Una svolta nel dibattito sulla crittografia: la sentenza Podchasov c. Russia della Corte EDU. Verso *alcuni diritti* di cybersicurezza?

A Pivotal Moment in the Encryption Debate: the ECtHR Ruling in Podchasov v. Russia. Towards *Some* Cybersecurity Rights?

PIER GIORGIO **CHIARA**
Ricercatore a tempo determinato di tipo (a) in informatica giuridica (IUS/20), presso CIRSFID – Alma AI e Dipartimento di Scienze Giuridiche, Università di Bologna.
E-mail: piergiorgio.chiara2@unibo.it

ABSTRACT
La nostra società digitale, imperniata su reti, sistemi informativi e servizi informatici interconnessi, ha crescenti esigenze di cybersicurezza. All'inizio degli anni 2000 la cybersicurezza cessa di essere una questione puramente "tecnica" ed acquista progressivamente rilevanza strategica e giuridica. L'articolo evidenzia soprattutto questa seconda dimensione, analizzando le condizioni per le quali specifiche tecnologie di cybersicurezza, in particolare la crittografia, si pongano in una prospettiva di strumentalità sul piano del godimento e della tutela dei diritti e delle libertà fondamentali (ad es., il diritto alla riservatezza, alla protezione dei dati personali e libertà di espressione), prendendo in considerazione la recente pronuncia della Corte EDU nella causa *Podchasov c. Russia*. Partendo da questa sentenza, l'articolo sostiene la necessità di riconoscere nuovi ed autonomi "diritti di cybersicurezza"', mostrando come gli elementi basilari per il contesto di attuazione siano già stati predisposti nel diritto secondario dell'UE.

Our digital society is built on interconnected networks, information systems and IT services. As a consequence, it has increasing cybersecurity needs. In the early 2000s, cybersecurity ceased to be a purely "technical" issue and progressively acquired strategic and legal relevance. The article emphasises this second dimension by analysing the conditions under which specific cybersecurity technologies, in particular encryption, are placed in an instrumental perspective in terms of the protection of fundamental rights and freedoms (e.g. the right to privacy, protection of personal data and freedom of expression), taking into consideration the recent ruling of the European Court of Human Rights in the case of Podchasov v. Russia. Building on this ruling, the article argues for the necessity of recognising new and autonomous "cybersecurity rights"', showing how the basic elements for the implementation framework have already been laid down in EU secondary law.

KEYWORDS
cybersicurezza, crittografia, diritti

cybersecurity, encryption, rights

ISSN 1825-0173

Una svolta nel dibattito sulla crittografia: la sentenza Podchasov c. Russia della Corte EDU. Verso *alcuni diritti* di cybersicurezza?

PIER GIORGIO CHIARA

1. *Introduzione* – 2. *La crittografia: una prospettiva informatico-giuridica* – 3. *Crittografia e diritti fondamentali: tra conflitto e strumentalità* – 4. *Un diritto ad alcune tecnologie di cybersicurezza? Sfide e prospettive* – 5. *Conclusioni*.

1. *Introduzione*

Con l'inizio del nuovo millennio, la cybersicurezza acquista una crescente rilevanza strategica e politica. A livello europeo, si assiste ad una proliferazione di iniziative di regolamentazione di un settore che, fino agli anni '90, risultava frammentato tra diversi quadri normativi. In primo luogo, il quadro giuridico in materia di telecomunicazioni conteneva diverse misure e requisiti in tema di sicurezza delle operazioni di rete[1]; per altro verso, misure tecniche e organizzative di sicurezza per il trattamento di dati personali erano introdotte dalle normative nazionali, ancorché di matrice europea, in materia di protezione dei dati personali[2]; infine, l'aumento progressivo del fenomeno della criminalità informatica ha fatto sì che le iniziative legislative si concentrassero sulla definizione di obblighi e misure per il contrasto del cyber crimine, vale a dire reati informatici propri oppure reati comuni commessi con sistemi informatici o i cui indizi si rinvengono nei sistemi informatici[3].

A latere di questa frammentazione giuridica, sul finire degli anni '90 tre grandi fenomeni sul piano sociale, economico e politico iniziano a dispiegare i loro effetti anche con riguardo alla sicurezza delle reti e dell'informazione. Sono la liberalizzazione, la convergenza e la globalizzazione[4]. In primo luogo, la proprietà, e quindi la gestione, della maggior parte delle reti e dei sistemi informativi è nelle mani di attori privati; la sicurezza, pertanto, è un aspetto che fa parte dell'offerta di mercato. Connesso a ciò, queste reti e sistemi informativi sono sempre più interconnessi tra di loro e, in parte, condividono le stesse infrastrutture. Infine, la maggioranza delle

* Questo lavoro è stato sostenuto dal progetto SERICS (PE00000014) nell'ambito del Piano Nazionale di Ripresa e Resilienza del MUR finanziato dall'Unione Europea - NextGenerationEU.

[1] Direttiva 90/387/CEE del Consiglio, del 28 giugno 1990, sull'istituzione del mercato interno per i servizi delle telecomunicazioni mediante la realizzazione della fornitura di una rete aperta di telecomunicazioni; Direttiva 90/388/CEE della Commissione, del 28 giugno 1990, relativa alla concorrenza nei mercati dei servizi di telecomunicazioni. La sicurezza delle operazioni di rete, il mantenimento dell'integrità, la disponibilità in caso di incidente erano requisiti essenziali che potevano fondare il potere dello Stato membro di limitare l'accesso alla rete pubblica di telecomunicazioni o ai servizi pubblici di telecomunicazioni.

[2] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni.

[3] Legge 23 dicembre 1993, n. 547, Modificazioni ed integrazioni alle norme del Codice penale e del Codice di procedura penale in tema di criminalità informatica. A livello internazionale, si veda la Convenzione sulla criminalità informatica del Consiglio di Europa (c.d. Convenzione di Budapest) del 2001, ratificata in Italia dalla Legge n. 48 del 2008.

[4] COMMISSIONE EUROPEA 2001, 7-8.

reti e dei sistemi informativi sono detenuti da imprese o gruppi internazionali; inoltre, le comunicazioni di rete sono sempre più transfrontaliere.

Alla luce di questi fenomeni, che avrebbero limitato sempre di più l'efficacia delle politiche nazionali in materia, e della frammentazione del quadro giuridico di cui si è dato conto sopra, la Commissione europea inizia a considerare come necessaria una politica a livello di Unione europea completa ed unitaria in materia di sicurezza delle reti e dell'informazione, al fine di correggere il fallimento di mercato del settore della sicurezza[5] e per una più efficace applicazione del quadro normativo, in un'ottica di complementarietà alle più mature politiche di telecomunicazione, protezione dei dati e contrasto al cyber crimine.

Solo nel 2013, tuttavia, l'Unione si dota di una Strategia in materia di cybersicurezza[6] che delinea un quadro complesso di interventi strategici a livello normativo, d'investimento e politico, coinvolgendo tutti i portatori di interesse rilevanti (istituzioni UE; Stati membri; settore privato), secondo una logica di '*governance multi-stakeholder*' volta a chiarire i ruoli e le responsabilità sui diversi livelli[7]. Quattro anni più tardi, la Commissione e l'Alto Rappresentante dell'Unione propongono una nuova Strategia[8], con simili priorità strategiche, ribadite e rafforzate dall'ultima Strategia UE in materia di cybersicurezza del 2020[9]. L'implementazione degli interventi contenuti nelle tre strategie si concretizza *inter alia* nell'adozione di diversi atti giuridici, a cominciare dalla direttiva UE 2016/1148 (c.d. NIS), passando per il regolamento UE 2019/881 (c.d. *Cybersecurity Act*), per finire con la direttiva UE 2022/2555 (c.d. NIS2), il regolamento UE 2022/2554 (c.d. DORA), la direttiva UE 2022/2557 (c.d. CER), il regolamento UE 2024/2847 (c.d. *Cyber Resilience Act*).

L'elemento catalizzatore comune a queste tre strategie così ravvicinate è il rapido mutamento del panorama delle minacce, sia sul piano quantitativo che qualitativo[10]. Il crescente livello di rischio determinato dalle minacce su vasta scala ha portato necessariamente organizzazioni sovranazionali ed internazionali, governi ed aziende a sviluppare strategie di sicurezza sempre più complesse e sofisticate, basate su misure tecniche, operative ed organizzative di sicurezza allo stato dell'arte. In tal senso, la crittografia è diventata progressivamente uno strumento essenziale non solo come tecnologia di cybersicurezza fondamentale per garantire la riservatezza e l'integrità delle comunicazioni, ma anche per la tutela dei diritti e delle libertà fondamentali, con particolare riferimento alla riservatezza e alla protezione dei dati personali[11].

Questo articolo affronta la cybersicurezza e, in particolare, la crittografia, da un punto di vista metodologico, come un ambito di studio multidisciplinare adottando una prospettiva informatico-giuridica che permetta di affrontare le complesse sfide normative – vale a dire, giuridiche, etiche e sociali, i rischi ma anche i benefici posti da una particolare tecnologia, in questo caso la crittografia *end-to-end*, attraverso lo studio e la comprensione di quest'ultima.

I problemi sono infatti noti da tempo[12]: da un lato, l'adozione di questa tecnica crittografica rappresenta un vantaggio evidente per la protezione dei dati personali e per il rispetto della pri-

[5] Se, per le leggi del mercato, il meccanismo dei prezzi garantisce l'equilibrio tra costi di protezione delle reti e bisogni specifici di sicurezza, il fallimento è dato dall'assenza di soluzioni di sicurezza o dalla difficoltà nel portarle nel mercato. Vedi sul punto, BYGRAVE 2024, 2.

[6] COMMISSIONE EUROPEA, ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA 2013.

[7] BRUNI 2019, 258; in generale, sull'approccio multi-stakeholder, si veda LIAROPOULOS 2016.

[8] COMMISSIONE EUROPEA, ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA 2017.

[9] COMMISSIONE EUROPEA, ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA 2020.

[10] Si vedano, sul punto, i report annuali prodotti dall'Agenzia europea per la Cybersicurezza (ENISA); ad es., ENISA 2024.

[11] Art. 32, Reg. UE 2016/679.

[12] Cfr. *ex multis* ZICCARDI 2003; KOOPS 1999.

vacy dei cittadini; dall'altro, questa stessa tecnologia di sicurezza pone problemi complessi in termini di regolamentazione e controllo, poiché gli stessi strumenti che proteggono le comunicazioni private possono essere utilizzati anche per scopi illeciti o altrimenti dannosi per la collettività. Ciclicamente, infatti, taluni Stati – anche nell'Unione europea – esplorano diverse soluzioni, tecniche e giuridiche, per indebolire la crittografia[13]. L'approccio informatico, filosofico-giuridico qui proposto[14] non si limita pertanto a considerare le questioni legali, nonché gli aspetti tecnici di questa tecnologia, ma esplora anche gli impatti etici e sociali sottesi a questo dibattito, al fine di poter sostanziare meglio l'analisi normativa. È la sincronia tra tecnologia, rischio e risposta normativa a definire il metodo.

In tale contesto, questo articolo si concentra su come la crittografia, e più precisamente la crittografia *end-to-end*, sia centrale nella protezione dei diritti individuali e delle libertà in una società digitale ed interconnessa[15]. La sezione 2 fornirà un'analisi tecnica della tecnologia di cybersicurezza sotto indagine, su cui si baserà l'analisi normativa della sezione 3, che darà conto delle implicazioni sul piano dei diritti fondamentali e dei rischi per la sicurezza, cercando di bilanciare esigenze apparentemente contrapposte, anche alla luce della recente pronuncia della Corte Europea dei Diritti dell'Uomo nella causa *Podchasov contro Russia.* Alla luce di alcuni importanti principi di diritto emersi nel ragionamento della Corte nella ricerca del delicato equilibrio tra le esigenze di sicurezza nazionale e la salvaguardia dei diritti fondamentali, la sezione 4 metterà in luce la necessità del riconoscimento di alcuni nuovi "diritti di cybersicurezza". La sezione 5, infine, concluderà il contributo con alcune riflessioni finali.

2. *La crittografia: una prospettiva informatico-giuridica*

Prima di prendere in esame la crittografia *end-to-end*, è opportuno introdurre i concetti di fondo di questa tecnologia. Tra gli strumenti crittografici, sono possibili molte classificazioni. Ad un alto livello di astrazione, è possibile distinguere la crittografia simmetrica, o a chiave singola, dalla crittografia asimmetrica.

Attraverso complesse operazioni matematiche, la crittografia simmetrica nasconde il contenuto (il c.d. testo in chiaro, che al termine del processo diventa testo cifrato), rendendo l'informazione inintelligibile a chiunque non sia in possesso della chiave crittografica[16]. In tal senso, la crittografia è considerata una tecnologia di sicurezza avente una funzione bi-direzionale: ciò che viene criptato, tramite un algoritmo chiamato *cipher*, può essere decifrato con la chiave appropriata. Di conseguenza, senza la chiave crittografica, anche un attore con molte risorse (es., una grande azienda o addirittura uno Stato) non è in grado di decifrare un messaggio. Gli algoritmi di crittografia simmetrica più utilizzati sono quelli di "cifratura a blocchi" (*block ciphers*)[17].

La differenza principale tra crittografia simmetrica e asimmetrica è che quest'ultima, per le due fasi distinte di cifratura e decifratura, prevede l'uso di due chiavi separate, mentre la prima utilizza una sola chiave[18]. Con questo metodo, una delle chiavi (chiave pubblica) viene distribuita nella

[13] Ad es., ricordiamo il *Investigatory Powers Act* (IPA) adottato dal Regno Unito nel 2016; il Telecommunications and Other Legislation Amendment (Assistance and Access) Act australiano del 2018; e, a livello UE, si veda CONSIGLIO DELL'UNIONE EUROPEA 2020.

[14] GUIHOT 2019.

[15] FLORIDI 2018, 2133.

[16] SCHNEIER 1995, 21.

[17] STALLINGS, BROWN 2018, 55: «*a block cipher processes the plaintext input in fixed-size blocks and produces a blockof ciphertext of equal size for each plaintext block. The algorithm processes longer plaintext amounts as a series of fixed-size blocks. The most important symmetric algorithms, all of which are block ciphers, are the Data Encryption Standard (DES), triple DES, and the Advanced Encryption Standard (AES)*».

[18] È importante sottolineare come non vi siano elementi per ritenere l'una o l'altra forma di crittografia (a chiave

rete di comunicazione, mentre l'altra chiave (chiave segreta) non viene appunto rivelata[19]. Occorre sottolineare che i sistemi e i servizi moderni usano spesso i meccanismi crittografici descritti in modo integrato, atteso che nessuna delle due sia intrinsecamente più sicura dell'altra.

Infine, a differenza della crittografia, le funzioni di *hash* sono algoritmi crittografici unidirezionali, giacché consistono in un processo irreversibile che prende come input un dato di qualsiasi dimensione (può essere un messaggio, un file, una stringa di testo o anche una password) e lo trasforma in una sequenza di caratteri dalla lunghezza fissa, chiamata *hash* o *digest*[20], resistente alle collisioni – ossia agli attacchi, nonché indistinguibile da una sequenza randomica[21]. Negli ultimi anni, l'algoritmo SHA (*Secure Hash Algorithm*), sviluppato dall'agenzia federale statunitense NIST, è diventato la funzione di *hash* più popolare.[22] La logica della crittografia è quindi quella di proteggere potenzialmente informazioni di qualsiasi tipo, e in qualsiasi stato – dal momento che può interessare sia dati c.d. "a riposo" (crittografia di archiviazione, *storage encryption*) sia dati durante il "trasporto" (crittografia di trasmissione, *transmission encryption*)[23].

Queste tecnologie sono essenziali per garantire e preservare alcuni principi fondanti della sicurezza delle informazioni (*information security*), cioè, confidenzialità, integrità, autenticazione e non-repudiabilità[24]. Evidentemente, al fine di garantire la confidenzialità, sono adottati protocolli diversi in funzione del diverso contesto di applicazione: solitamente meccanismi di crittografia simmetrica sono applicati a devices che contengono i dati che l'utilizzatore vuole proteggere (es., laptop, smartphones, hard disk) impedendo pertanto l'accesso degli utenti non autorizzati; oppure, strumenti crittografici (a chiave pubblica) sono adottati nel contesto delle comunicazioni, al fine di escludere l'accesso al dato mentre avviene la trasmissione. In questo contesto, la crittografia c.d. *end-to-end* è un tipo di crittografia asimmetrica (cioè, a chiave pubblica) che è molto utilizzata nei servizi di comunicazione online (quali Whatsapp, Telegram – se si sceglie l'opzione "chat segreta" –, e Signal) per assicurare la confidenzialità del dato[25].

Del resto, altre tipologie di tecnologie crittografiche, sempre più diffuse nel mercato e su cui si fa ricerca al fine di perfezionare tecnologie volte a minimizzare gli impatti per la privacy e la protezione dei dati personali degli individui (c.d. *privacy enhancing technologies*), si basano su sistemi a chiave pubblica o privata. Ad esempio, la crittografia omomorfa è una variante della crittografia a chiave pubblica che si basa su algoritmi crittografici che permettono di trattare i dati crittografati senza doverli decifrare. In altre parole, si garantirebbe la possibilità di effettuare operazioni con il dato garantendo al tempo stesso la confidenzialità di quest'ultimo. Evidentemente, questa tecnica è particolarmente promettente in scenari dove più parti devono eseguire operazioni su dati criptati condivisi senza rivelare, però, i singoli input, ossia i dati in *plain text* (c.d. *secure multi-party computation*). Si pensi, ad esempio, alla gestione di trattamenti di dati personali particolari in contesti sanitari, dove sono diverse le parti coinvolte su una singola cartella: paziente, medico, struttura di ricerca, ecc[26].

segreta o pubblica) superiore all'altra da un punto di vista di sicurezza in senso tecnico (es., resilienza agli attacchi di forza bruta); come, del resto, sarebbe sbagliato ritenere la crittografia a chiave pubblica "un'evoluzione" di quella simmetrica e che quest'ultima, pertanto, possa essere abbandonata a vantaggio della crittografia asimmetrica.

[19] Brooks 2014, 100.

[20] EDPS, AEPD 2019, 8-10; Dang 2012, 6-9.

[21] Stallings, Brown 2018, 65: questa proprietà riguarda l'impossibilità di trovare un messaggio alternativo con lo stesso valore di *hash* di un dato messaggio.

[22] Preneel 2010.

[23] Scarfone et al. 2017.

[24] Ad es., algoritmi di hash assicurano l'integrità dell'informazione dal momento che permettono a chi è autorizzato di verificare se i dati cifrati siano stati alterati.

[25] Per un approfondimento, si veda Ermoshina 2016.

[26] In questo contesto, si veda ad esempio il lavoro di Verheul 2016.

Come abbiamo visto, se l'algoritmo crittografico adottato è sufficientemente robusto[27] e se le politiche e procedure di gestione delle chiavi permettono la conservazione di queste nelle mani degli utenti, allora i dati cifrati non saranno accessibili da terzi rispetto ai proprietari delle chiavi. Al netto dei tentativi di accesso illecito da parte di terzi, il fatto che le chiavi siano conservate nei *device* degli utilizzatori o dai fornitori del servizio di cifratura (es., un fornitore di servizi di telecomunicazione), e quindi non nella disponibilità del soggetto, ha importanti risvolti sul piano politico e giuridico. Come anticipato sopra, anche soggetti potenti e con molte risorse come agenzie governative, servizi di intelligence e autorità di contrasto non hanno – teoricamente – possibilità di accesso ai dati crittografati senza la disponibilità delle chiavi necessarie per la decrittazione.

Pertanto, se da una parte la crittografia è una tecnologia che garantisce il godimento di alcuni diritti e libertà fondamentali, quali il diritto alla privacy, alla protezione dei dati personali e alla libertà di espressione, dall'altra il funzionamento stesso di questa tecnologia, in particolare per quanto attiene ai meccanismi di certificazione e alle politiche di gestione delle chiavi, crea necessariamente dei rapporti di dipendenza con terze parti: di conseguenza, la crittografia genera nuove vulnerabilità che richiedono ulteriori tecnologie di sicurezza digitali per individuare i comportamenti fraudolenti di queste terze parti o attacchi contro queste[28]. Questo è un altro esempio della complessità del rapporto intercorrente tra queste tecnologie di cybersicurezza e i diritti fondamentali: la crittografia può essere strumentale al godimento dei "diritti" e, allo stesso tempo, porsi in un'ottica di conflitto, richiedendo pertanto esercizi di bilanciamento, da distinguersi dalle istanze di *trade-offs*[29].

3. *Crittografia e diritti fondamentali: tra conflitto e strumentalità*

Il fatto che la crittografia *end-to-end* impedisca in linea teorica l'accesso ai dati "in chiaro" alle parti che non hanno disponibilità delle chiavi di cifratura, come visto nella sezione precedente, ha agitato nel corso degli ultimi tre decenni i governi di tutto il mondo. È infatti negli anni 90 che iniziano a dispiegarsi gli effetti della difficoltà di bilanciare, «a livello di regolamentazione statale, gli interessi confliggenti di *privacy* e di *information security* da un lato, e gli interessi di sicurezza nazionale e di applicazione delle leggi dall'altro»[30].

All'inizio degli anni 90, infatti, gli Stati Uniti d'America provarono per primi a far adottare una tecnologia software con una *backdoor* incorporata al fine di permettere l'accesso ai dati da parte delle autorità di contrasto, eludendo pertanto il meccanismo crittografico[31]. Allo stesso tempo, nel 1994 il Congresso statunitense promulgò una legge[32] per impedire ai fornitori dei servizi di telecomunicazioni di costruire una backdoor affinché le autorità di contrasto potessero decrittare le comunicazioni crittografate dagli utenti, nello scenario, pertanto, in cui i provider non avessero possibilità di con-

[27] La robustezza di un sistema crittografico è misurata in termini di attacchi (es., *brute force*) a cui riesce ad opporre resistenza con successo. I c.d. attacchi di "bruta forza" (*brute force*) consistono in molteplici tentativi ripetuti utilizzati da applicativi software per decodificare dati criptati e/o chiavi crittografiche, attraverso uno sforzo esaustivo.

[28] HILDEBRANDT 2019, 262.

[29] Da una parte, la prospettiva del bilanciamento implicherebbe una ricerca costante di (un nuovo) equilibrio. In altre parole, per ogni misura che viola i diritti e le libertà, si aumentano le garanzie; dall'altra, il trade-off suggerisce la compressione di un bene giuridico, di un diritto (es., diritto alla riservatezza), a fronte dell'introduzione di misure in contrasto con esso.

[30] ZICCARDI 2003, 22.

[31] È del 1993 il c.d. "chip Clipper"', un dispositivo sviluppato dall'Agenzia per la Sicurezza nazionale (NSA) statunitense per la crittografia telefonica con una backdoor incorporata per consentire l'accesso governativo. Si veda *ex multis* HOFFMAN 1995.

[32] Communications Assistance for Law Enforcement Act (CALEA).

trollo delle chiavi crittografiche[33]. Questi tentativi segnarono l'inizio della prima c.d. "*crypto war*".

Alla fine degli anni '90, i governi (non solo quello statunitense, ma anche diversi Stati europei furono coinvolti, tra cui la Gran Bretagna, l'Olanda, la Germania) abbandonarono sistemi con backdoor di accesso a causa della sfiducia del pubblico, dell'insicurezza tecnica e della consapevolezza che queste tecnologie non avrebbero comunque impedito ai criminali di utilizzare metodi di crittografia alternativi. Pertanto, invece di alterare l'infrastruttura del meccanismo crittografico attraverso backdoors, si iniziarono a preferire "ordini di decrittazione" rivolti ai singoli utenti indagati, qualora le autorità di contrasto si fossero imbattute in dati cifrati[34].

A seguito della crescente adozione di meccanismi di crittografia, quale la crittografia end-to-end, da parte dei privati (non solo fornitori di servizi Internet, ma anche e soprattutto produttori di dispositivi, che iniziano ad offrire sistemi di crittografia end-to-end di default per i loro prodotti e servizi di comunicazione associati) a tutela della privacy e della sicurezza degli utenti, viene rianimato un dibattito che sembrava sopito. La c.d. seconda *crypto war* fa così riferimento al difficile bilanciamento a cui vennero sottoposti le corti, soprattutto negli Stati Uniti[35], ma non solo, tra il dovere delle aziende di cooperare con le forze dell'ordine nelle attività di contrasto, da un lato, e l'interesse di evitare che l'assistenza obbligatoria di tali aziende con le autorità potesse mettere in pericolo la sicurezza e la privacy dei loro clienti, dall'altro[36].

Infatti, come abbiamo visto nella sezione precedente, in un servizio di comunicazione che adotta la crittografia end-to-end, poiché entrambe le fasi di cifratura e decrittazione dei messaggi inviati e ricevuti avvengono sui dispositivi degli utenti, solo i destinatari previsti, e non anche il fornitore di servizi di comunicazione, hanno accesso al contenuto dei messaggi. Un obbligo di decriptare le comunicazioni cifrate costringerebbe pertanto i fornitori di servizi di comunicazione a modificare i loro servizi esistenti creando delle backdoor che, una volta individuate, potrebbero peraltro essere facilmente sfruttate da soggetti sia legittimi che criminali. Non solo, una tale modifica del meccanismo crittografico – attraverso un aggiornamento del software – non potrebbe essere mirato a utenti specifici, bensì interesserebbe indiscriminatamente tutti gli utenti del servizio in questione[37]. Ne consegue che l'interferenza *inter alia* con i diritti alla riservatezza delle comunicazioni e al rispetto alla vita privata e familiare generato da un obbligo di questo genere risulterebbe sproporzionato rispetto ai fini perseguiti[38]. Nei paragrafi successivi si darà conto in misura esaustiva dello standard di "proporzionalità", che costituisce uno dei pilastri del diritto alla riservatezza, così come interpretato dalle corti europee.

Già nel 2016 un report congiunto di ENISA ed EUROPOL sottolineava delle alternative considerate proporzionate rispetto alle esigenze legittime di indagare su singoli sospettati, quali operazioni sotto copertura, infiltrazione in gruppi criminali e accesso ai dispositivi di comunicazione al di là dell'operazione crittografica, ad esempio mediante analisi forensi in tempo reale sui dispositivi sequestrati o mediante intercettazioni legali sui dispositivi mentre questi sono ancora utilizzati dai sospetti. Di converso, la rottura dei meccanismi crittografici potrebbe causare danni collaterali[39].

[33] Koops, Kosta 2018, 893.

[34] Koops, Kosta 2018, 895.

[35] Nel 2016, l'FBI cercò di accedere ad un telefono iPhone appartenuto ad un uomo dopo che questi aveva commesso un attacco terroristico a San Bernardino. Nonostante l'FBI potesse contare su un mandato per procedere all'ispezione, Apple non cooperò con l'agenzia che non poteva aggirare la crittografia del device. Tuttavia, il caso è stato archiviato e un tribunale non si è mai pronunciato sulle obiezioni sollevate da Apple. L'FBI, infatti, non avrebbe più avuto bisogno dell'aiuto di Apple: secondo quanto riportato dalla stampa, una società australiana, Azimuth Security, aveva trovato una falla di sicurezza che consentiva di aggirare il meccanismo crittografico dell'iPhone. Così l'FBI avrebbe acquistato questa vulnerabilità 'zero-day' per accedere al telefono. Vedi Kerr 2024, 187-188.

[36] Koops, Kosta 2018, 897.

[37] Privacy International 2022, 16.

[38] EDPB-GEPD 2022, 10.

[39] Enisa, Europol 2016.

L'obiettivo, infatti, dovrebbe essere quello di ottenere l'accesso alle informazioni, e non anche di rompere il meccanismo di protezione.

Su questa falsa riga, nel 2020 il Consiglio dell'Unione europea affermava la necessità di proteggere la privacy e la sicurezza delle comunicazioni attraverso la crittografia e allo stesso tempo sostenere la possibilità per le autorità competenti nel settore della sicurezza e della giustizia penale di accedere legittimamente ai dati pertinenti per scopi legittimi e chiaramente definiti nella lotta contro crimini gravi, nonché il crimine organizzato e il terrorismo[40].

In questo contesto, il 13 febbraio 2024, la Corte europea dei diritti dell'uomo (Corte EDU) ha emesso una sentenza nella causa *Podchasov c. Russia*[41]. Questa sentenza merita un'attenzione particolare perché è il primo riconoscimento espresso, da parte di una corte europea, del fatto che la crittografia end-to-end non possa essere indebolita per un utente senza recare un pregiudizio decisivo alla sicurezza del meccanismo stesso, recando quindi un grave rischio alla sicurezza e riservatezza delle comunicazioni per tutti gli utenti indiscriminatamente.

In breve, il caso riguarda la compatibilità con l'Articolo 8 della Convenzione europea dei diritti dell'uomo (CEDU) di requisiti legali per i fornitori di servizi di comunicazione elettronica relativi alla conservazione dei dati e dei metadati delle comunicazioni, alla sorveglianza segreta e, in particolare, agli ordini di decrittazione. La legge russa[42], infatti, prevede che gli "organizzatori di comunicazioni online" (i) conservino obbligatoriamente i dati di comunicazione per un anno e il contenuto di tutte le comunicazioni per sei mesi; (ii) esibiscano tali dati alle autorità di contrasto e servizi di intelligence nelle circostanze specificate dalla legge; (iii) forniscano le informazioni necessarie per decifrare i messaggi elettronici, ove criptati[43].

Nel 2017, i servizi d'intelligence russi del FSB ordinarono a Telegram – inclusa nella lista degli organizzatori di comunicazioni online – di fornire supporto per la decrittazione delle comunicazioni di sei individui sospettati di attività terroristiche, nonché fornire dati tecnici, tra cui indirizzi IP, numeri di porta TCP/UDP e, soprattutto, le chiavi di cifratura. Telegram si rifiutò, obiettando che gli individui in questione avevano optato per l'opzione "chat segreta", che si poggia sulla crittografia end-to-end: la decrittazione delle sei chat, come richiesto dalle autorità di sicurezza russe, non sarebbe stata possibile senza compromettere la sicurezza di tutti gli utenti[44]. La mancanza di cooperazione con le autorità costò a Telegram due diverse sanzioni amministrative e anche un ordine di blocco su territorio russo, ancorché rimanga tuttora accessibile in Russia[45].

Il ricorrente e 34 altri utenti contestarono quindi in tribunale l'obbligo posto dalla legge in questione adducendo che se Telegram avesse obbedito a tale ordine avrebbe consentito alle autorità un accesso illimitato a tutte le comunicazioni (e non solo quelle per cui si richiedeva accesso)[46]: secondo i ricorrenti, un simile obbligo costituirebbe una seria interferenza con il diritto al rispetto della vita privata e alla confidenzialità delle comunicazioni di tutti gli utenti, aprendo quindi la strada ad un sistema di sorveglianza arbitraria. Le corti adite tuttavia rigettarono i ricorsi. Dopo aver esaurito i rimedi giudiziali interni, il ricorrente ha presentato ricorso dinanzi alla Corte EDU.

Dopo essersi pronunciata sulla giurisdizione[47] e sull'ammissibilità[48] del ricorso, la Corte ha valutato se e in che misura vi sia stata un'interferenza con i diritti di cui all'articolo 8 della CE-

[40] Consiglio dell'Unione europea 2020, 4.

[41] Corte E.D.U., 13 febbraio 2024, caso Podchasov c. Russia, n. 33696/19. Ci sia concesso richiamare Chiara 2024a; si veda inoltre van't Schip, Borgesius 2024.

[42] Federal Law no. 149-FZ of 27 July 2006 «on Information, Information Technologies and Protection of Information» (c.d. "the Information Act").

[43] *Podchasov c. Russia*, §§16-20.

[44] *Ibid.*, §8.

[45] *Ibid.*, §14.

[46] *Ibid.*, §9.

[47] *Ibid.*, §35.

[48] *Ibid.*, §37.

DU. Il governo russo ha sostenuto che i diritti del ricorrente non erano stati violati perché questi non era riuscito a provare che l'FSB detenesse informazioni private su di lui, e comunque qualsiasi interferenza aveva una chiara base legale, con garanzie procedurali previste volte ad evitare gli abusi (es., l'autorizzazione preventiva di un tribunale), e queste misure sono state ritenute necessarie in una società democratica per il fine legittimo di combattere il terrorismo. Inoltre, le chiavi di crittografia sarebbero state richieste solo per casi specifici di sospette attività terroristiche con un accesso limitato ad una parte selezionata del personale dell'FSB[49].

In merito all'esistenza dell'interferenza e al suo ambito di applicazione, la Corte ha innanzitutto ritenuto che la mera memorizzazione da parte degli "organizzatori" di tutti i contenuti delle comunicazioni e dei metadati di un individuo costituisse un'interferenza ai sensi dell'articolo 8 della CEDU, a prescindere dal fatto che le autorità avessero effettivamente effettuato un accesso a tali informazioni[50]. Pertanto, la Corte ha richiamato l'ampia analisi della legislazione russa in materia di sorveglianza segreta in *Roman Zakharov*[51]. Non stupisce, quindi, che la Corte abbia (nuovamente) ritenuto che gli obblighi scaturenti da tale normativa costituissero un'interferenza con i diritti di cui all'articolo 8 del ricorrente, ritenendo provato, in particolare, l'assunto del ricorrente circa l'impossibilità *tecnica* di fornire alle autorità chiavi di cifratura associate ad utenti specifici, sicché sarebbe stato necessario modificare il meccanismo crittografico adottato con impatti indiscriminati per gli utenti del servizio[52].

La Corte ha poi considerato congiuntamente se l'interferenza fosse conforme alla legge e perseguisse uno o più obiettivi legittimi pertinenti, e quindi se fosse necessaria in una società democratica. Non ci soffermeremo troppo sull'applicazione dei principi al tema della conservazione delle comunicazioni e – conseguentemente – all'accesso ai relativi dati da parte delle autorità per due motivi: in primo luogo, ai fini del presente articolo, è di maggiore interesse il ragionamento della Corte circa l'obbligo di decriptare le comunicazioni; in secondo luogo, come già rilevato nel caso *Roman Zacharov*, il quadro normativo russo in specie non soddisfa il requisito della "qualità della legge"[53], dal momento che 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»[54]. Infatti, la Corte ha evidenziato che le misure e le garanzie impugnate coinvolgevano indiscriminatamente i dati delle comunicazioni online di tutti gli utenti, anche in assenza di un ragionevole sospetto di coinvolgimento in attività criminali o che mettessero in pericolo la sicurezza nazionale, ancorché queste avessero una base giuridica e perseguissero obiettivi legittimi[55].

[49] *Ibid.*, §§40-43.

[50] *Ibid.*, §§ 50-52, 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. Sebbene la Corte solitamente non esamini le leggi *in astratto*, è giurisprudenza consolidata (cfr. *Ekimdzhiev e altri c. Bulgaria*, §376) che nei casi di sorveglianza segreta, date le sue caratteristiche intrinseche che non consentono agli individui di sapere se i loro dati siano stati consultati, la mera esistenza dei requisiti di legge contestati equivale di per sé a un'interferenza dei diritti di cui all'articolo 8. Sul punto, si veda JANSEN 2022, 139.

[51] *Roman Zakharov v Russia* [GC] n. 47143/06, 4 dicembre 2015.

[52] *Podchasov v Russia,* §58.

[53] La legge deve indicare la portata di qualsiasi potere discrezionale conferito alle autorità competenti e le modalità del suo esercizio con sufficiente chiarezza per dare all'individuo un'adeguata protezione contro le interferenze arbitrarie.

[54] *Podchasov c. Russia,* §64; *Roman Zakharov*, §§ 231-234. Peraltro, in *Kogan e altri v. Russia,* n. 54003/20, 7 marzo 2023, la terza sezione della Corte ha ribadito che il requisito della "previsione della legge"' non si limita a richiedere che la misura contestata abbia una base nel diritto interno, bensì si riferisce anche alla "qualità" della legge in questione, che deve prevedere, tra le altre cose, un certo grado di tutela legale contro interferenze arbitrarie o abusi da parte delle autorità pubbliche (*Kogan e altri v. Russia,* §58). Inoltre, per quanto riguarda il requisito dello "scopo legittimo", soprattutto nell'ambito della tutela della sicurezza nazionale, i concetti di legalità e Stato di diritto in una società democratica impongono che le misure che incidono sui diritti fondamentali siano soggette a una qualche forma di procedimento contraddittorio davanti a un organo indipendente, competente a riesaminare le ragioni della decisione e le prove pertinenti, se necessario, con adeguate limitazioni procedurali all'uso di informazioni classificate, affinché l'individuo possa contestare l'assunto dell'esecutivo (*Kogan e altri v. Russia,* §58). Cfr. con *Juszczyszyn v. Polonia*, n. 35599/20, 6 ottobre 2022, §§261-280.

[55] *Podchasov c. Russia,* §70.

La Corte ha ritenuto che l'obbligo di fornire alle autorità i mezzi per decrittare le comunicazioni criptate end-to-end non fosse proporzionato agli obiettivi legittimi perseguiti[56]. Sul punto, la Corte ha chiarito che alcune tecnologie di cybersicurezza, come la crittografia end-to-end, contribuiscono a garantire il godimento dei diritti fondamentali, come il diritto al rispetto della vita privata e della corrispondenza online e la libertà di espressione. Accogliendo le osservazioni di esperti del settore, la Corte ha affermato che nel contesto della crittografia end-to-end non esistono ordini di decrittazione mirati per utenti specifici: una volta che il meccanismo di crittografia end-to-end è "rotto", è "rotto" per tutti gli utenti, aprendo pertanto la strada ad una sorveglianza generale e indiscriminata[57]. E, peggio ancora, le reti criminali potrebbero approfittare di questo indebolimento.

Infine, per quanto riguarda l'argomento secondo cui una crittografia forte protegge i criminali, sollevato, come abbiamo visto, anche da governi occidentali ciclicamente nel corso degli ultimi decenni, la Corte ha rilevato come siano state indicate soluzioni alternative alla decrittazione, che non indebolissero i meccanismi di protezione, sia sul piano legislativo che sul piano tecnico (es., accesso ai dispositivi di comunicazione eludendo il meccanismo crittografico mediante analisi forense in tempo reale su dispositivi sequestrati o mediante intercettazione legale di tali dispositivi mentre sono ancora utilizzati dai sospettati)[58]. La Corte ha pertanto concluso che la legislazione contestata non poteva essere considerata necessaria in una società democratica, poiché consentiva alle autorità pubbliche di accedere, su base generalizzata e senza sufficienti garanzie, al contenuto delle comunicazioni elettroniche. Di conseguenza, le misure contestate hanno compromesso l'essenza stessa dell'articolo 8 della Convenzione, che è risultato essere stato violato[59].

Questa pronuncia, ancorché ribadisca alcuni principi fondamentali già consolidati nella giurisprudenza della stessa Corte (vedi *Roman Zacharov* e *Ekimdzhiev*), è importante anche per gli effetti che potenzialmente può dispiegare al di là del quadro di tutela della CEDU. Sullo sfondo della frequente interazione ed allineamento della giurisprudenza delle due corti europee (Corte EDU e Corte di giustizia dell'UE), soprattutto in relazione alla tutela del diritto alla riservatezza (e alla protezione dei dati personali)[60], la difesa da parte della Corte di Strasburgo del meccanismo crittografico in ragione della sua strumentalità nella tutela e godimento di alcuni diritti umani può aprire la strada ad un simile riconoscimento dell'importanza per i diritti fondamentali della crittografia (end-to-end) da parte della Corte di Lussemburgo nel diritto dell'Unione europea. Connesso a ciò, la CGUE aveva già associato l'essenza del diritto fondamentale alla protezione dei dati personali ex art. 8 della Carta dei diritti fondamentali dell'UE ai principi e alle misure dell'*information security*[61]. Una prospettiva, quella strumentale, che peraltro è da sempre stata sostenuta con forza dal Garante europeo della protezione dei dati personali[62] e dal Comitato europeo per la protezione dei dati personali[63].

Alla luce di quanto è emerso, la sezione che segue analizza se e fino a che punto questa pronuncia in particolare legittima una riflessione circa l'emersione, o, meglio, la necessità di riconoscere in Europa degli autonomi diritti ad alcune tecnologie di cybersicurezza.

[56] *Ibid.*, §79.

[57] *Ibid.*, §77.

[58] *Ibid.*, §78; la Corte fa espresso riferimento al report congiunto di Europol ed ENISA del 2016; nonché del rapporto di Privacy International.

[59] *Podchasov c. Russia*, §§ 80-81.

[60] Si veda COLE, VANDENDRIESSCHE 2016, 123. Ad esempio, la giurisprudenza della CGUE in materia di sorveglianza e conservazione dei dati fa riferimento alla giurisprudenza della Corte EDU: vedi Cause riunite C-511/18, C-512/18 e C-520/18 *La Quadrature du Net e altri* [2020] ECLI:EU:C:2020:791, § 128. D'altra parte, la Corte EDU, in *Szabò e Vissy c. Ungheria* (no. 37138/14), rimanda alla decisione della CGUE in *Digital Rights Ireland c. Minister for Communciations & Others* del 2014 (cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238).

[61] Si veda la già citata *Digital Rights Ireland*, §40; Parere 1/15 della Corte [Grande Sezione], 26 luglio 2017 §150.

[62] Cfr. BUTTARELLI 2016; WIEWIÓROWSKI 2020, 3; WIEWIÓROWSKI 2023.

[63] EDPB 2021.

4. *Un diritto ad alcune tecnologie di cybersicurezza? Sfide e prospettive*

La mancanza, allo stato dell'arte, di soluzioni *tecniche* di modifica del meccanismo crittografico accettabili per risolvere la tensione sottesa al dibattito intorno alla crittografia end-to-end è ancora più evidente nel contesto di alcune controverse iniziative legislative in Europa, sia a livello UE che in UK. Nel 2018, infatti, la Commissione ha proposto un regolamento che stabilisce misure per prevenire e combattere gli abusi sessuali nei confronti dei minori[64]. Senza entrare nel merito specifico della proposta di regolamento (c.d. "regolamento CSAM")[65], è sufficiente qui richiamare la previsione di obblighi per i fornitori di servizi di hosting e di comunicazione interpersonale di adottare tecnologie per accedere alle comunicazioni degli utenti e rilevare materiali relativi ad abusi sessuali di bambini noti e sconosciuti o l'adescamento di minori, a seguito della ricezione di ordini di rilevazione da parte delle autorità nazionali competenti[66].

Secondo l'EDPB e l'EDPS, queste misure infatti potrebbero comportare «una scansione di fatto generalizzata e indiscriminata dei contenuti praticamente di tutti i tipi di comunicazioni elettroniche di tutti gli utenti nell'UE»[67]. Infatti, l'uso di strumenti per l'intercettazione e l'analisi delle comunicazioni è intrinsecamente incompatibile con la crittografia end-to-end. Sebbene la proposta non preveda un obbligo sistematico di intercettazione, la mera possibilità dell'emissione di ordini di rilevazione potrebbe influenzare le scelte tecniche dei fornitori, inducendoli a rinunciare a questi meccanismi crittografici per poter rispettare tali obblighi. Peraltro, l'EDPB e l'EDPS ricordano come le misure tecniche suggerite nella valutazione d'impatto che accompagna la proposta per eludere la crittografia end-to-end comporterebbero trattamenti indiscriminati e generalizzati di contenuti non (ancora) cifrati sui dispositivi degli utenti (scansione lato *client*) oppure sui server dei prestatori (scansione lato *server*)[68]. In ragione dell'invasività delle misure mirate al contrasto di materiale pedopornografico sconosciuto e all'adescamento di minori, nonché della loro natura probabilistica (basata su tecniche automatizzate di IA) e quindi esposta a significativi tassi di falsi positivi, l'EDPB e il Garante europeo per la protezione dei dati personali considerano che tale ingerenza vada oltre quanto strettamente necessario e proporzionato[69].

È similmente controversa la sezione 121 della legge britannica sulla sicurezza online (*Online Safety Act*, OSA) del 2023. Questa disposizione conferisce ad Ofcom – l'autorità compente per l'applicazione dell'OSA – il potere di inviare un avviso ad un fornitore di «servizi regolamentati di comunicazione tra utenti» richiedendo l'uso di una «tecnologia accreditata» per identificare contenuti legati allo sfruttamento o abuso sessuale di minori, sia nelle comunicazioni pubbliche che private[70]. In altre parole, i fornitori di servizi regolamentati, per essere conformi a tale disposizione, devono poter monitorare i messaggi privati scambiati attraverso le loro piattaforme. Dal momento che la legge non prevede alcuna eccezione né stabilisce delle garanzie in caso un fornitore di servizi di comunicazione regolamentato adotti una tecnologia di crittografia end-to-end, i fornitori si ritroverebbero nella condizione di dover (eventualmente) rimuovere tale meccanismo crittografico oppure eluderlo con sistemi di *scanning* a livello di dispositivo utente parimenti invasivi per adempiere agli obblighi imposti dalla normativa[71].

Ancorché le misure di cui sopra non obblighino *esplicitamente*, come nel caso della legislazione russa visto nella sezione precedente, i prestatori di servizi di comunicazione a fornire mezzi per

[64] COMMISSIONE EUROPEA, Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori, COM (2022) 209 final.
[65] Sul punto si veda *ex multis* NERONI REZENDE 2024.
[66] Art. 7 e 10, proposta di regolamento CSAM.
[67] EDPB-GEPD 2022, 20.
[68] EDPB-GEPD 2022, 28.
[69] EDPB-GEPD 2022, 23.
[70] Online Safety Act, §121(2)(a)(iii).
[71] SHURSON 2024, 4. Vedi anche TRENGOVE et al. 2022.

la decrittazione di contenuti cifrati (anche e soprattutto con il meccanismo della crittografia end-to-end), né obblighino detti operatori economici a creare delle backdoors al fine di consentire alle autorità amministrative e di contrasto di esaminare contenuti potenzialmente illeciti, i prestatori, per rispettare gli ordini di rilevazione, si troverebbero comunque innanzi ad un bivio: volendo escludere la strada che porta alla creazione delle backdoor, la scelta sarà tra l'abbandono dell'utilizzo della crittografia end-to-end e l'adozione di tecnologie di scansione sui device degli utenti prima che i contenuti vengano crittografati end-to-end. Ed entrambe le opzioni minano alla radice la *ratio* ultima del meccanismo della crittografia end-to-end.

A tal proposito, la Corte EDU in *Podchasov*, pur limitando il ragionamento alla situazione in cui l'indebolimento della tecnologia in indagine è dovuta alla creazione di backdoors, applicando il principio di proporzionalità, considera non proporzionate misure che indeboliscano la crittografia end-to-end nella misura in cui abbiano la capacità di interessare tutti gli utilizzatori del dato servizio indiscriminatamente[72]. *Mutatis mutandis*, questo principio può essere applicato anche al caso degli ordini di rilevazione europei, i quali, pur non obbligando il *provider* a fornire chiavi di decrittazione o a rompere il meccanismo crittografico, renderebbero tecnicamente possibile un sistema di «sorveglianza di routine, generale e indiscriminata delle comunicazioni elettroniche personali»[73]. Pertanto, è molto probabile che anche questi obblighi costituiscano una violazione dell'Articolo 8 CEDU e, nel contesto del diritto UE, dell'essenza dei diritti fondamentali ex Art. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

Il 20 giugno 2024, il Consiglio dell'UE avrebbe dovuto adottare la sua posizione sulla proposta regolamento CSAM. Tuttavia, il voto è stato rinviato dalla presidenza belga a causa delle forti pressioni contrarie di diversi paesi, tra cui Germania, Austria, Polonia, Paesi Bassi e Repubblica Ceca, che hanno ascoltato gli appelli degli esperti di privacy e sicurezza[74].

In questo contesto, alcuni commentatori hanno iniziato a domandarsi se nella sentenza della Corte EDU si nasconda un implicito riconoscimento ad un "diritto alla crittografia"[75]. In questo senso, sarebbe possibile pensare ad un "diritto alla crittografia" come una particolarizzazione del più ampio diritto alla "privacy", enucleato nell'Articolo 8 della CEDU e nell'Articolo 7 della Carta dei Diritti Fondamentali dell'UE.[76] A tal proposito, Bygrave sottolinea che la cybersicurezza, da un punto di vista normativo, ha progressivamente trovato un radicamento nel quadro costituzionale dell'UE per quanto concerne la protezione dei diritti fondamentali (con riguardo alla dimensione della sicurezza dei dati personali), in particolare grazie alla giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo[77]. Con ciò, non si vuole suggerire che l'insieme delle tecnologie crittografiche debba vedersi riconosciuto *tout court* uno speciale status costituzionale, bensì che una restrizione generalizzata e indiscriminata di queste tecnologie sia passibile di violare l'essenza di determinati diritti (come ad esempio la privacy), come esplicitamente riconosciuto dalla Corte EDU nel caso *Podchasov*.

Invero, già da qualche tempo si riflette sull'opportunità di riconoscere un "diritto alla cybersicurezza"[78]. L'emersione di un simile diritto impone alcune considerazioni politiche e giuridiche fondamentali: i) perché un simile diritto è necessario, soprattutto alla luce degli esistenti diritti fondamentali alla privacy e alla protezione dei dati personali? ii) fino a che punto è possibile considerare la cybersicurezza una mera trasposizione del concetto di sicurezza nella dimensione

[72] *Podchasov c. Russia*, §77.
[73] *Ibid*.
[74] GOUJARD 2024.
[75] SHURSON 2024; cfr. VAN DAALEN 2023.
[76] Si veda DAVIES 2024.
[77] BYGRAVE 2024, 4-5.
[78] CERRINA FERONI, MORBIDELLI 2008; PAPAKONSTANTINOU 2022; FRATTASI, POLLICINO, SCARPELLINI 2024. *Contra* vedi LONGO 2024, 322.

digitale? iii) quale dovrebbe essere il suo contenuto? La sua formulazione dovrebbe basarsi su un approccio "dichiarativo"' – tradizionale dei diritti umani, o, piuttosto, prescrittivo mediante una precisa identificazione di obblighi positivi o negativi (od entrambi)? Quali dovrebbero essere i beneficiari di questo diritto e chi dovrebbe attuarlo?

In altra sede[79], ho cercato di rispondere a queste domande; ai fini del presente articolo, è importante richiamare alcuni aspetti inerenti, soprattutto, all'oggetto di questo diritto. Ho infatti sostenuto che un eventuale nuovo diritto fondamentale alla cybersicurezza dovrebbe prendere come modello la «Dichiarazione europea sui diritti e i principi generali per il decennio digitale» (da qui in avanti, "Dichiarazione")[80]. In particolare, il principio 16 afferma che

> «Ogni persona dovrebbe avere accesso a tecnologie, prodotti e servizi digitali che siano sicuri e protetti e tutelino la vita privata fin dalla progettazione, traducendosi in un elevato livello di riservatezza, integrità, disponibilità e autenticità delle informazioni trattate».

La Dichiarazione elabora ulteriormente tale principio attraverso tre impegni politici, che dovrebbero guidare le istituzioni responsabili nell'attuazione di questo "principio alla cybersicurezza":

> «a) adottare ulteriori misure per promuovere la tracciabilità dei prodotti e assicurare che nel mercato unico digitale siano offerti solo prodotti sicuri e conformi alla legislazione dell'UE; b) proteggere gli interessi delle persone, delle imprese e delle istituzioni pubbliche dai rischi di cibersicurezza e dalla criminalità informatica [...], il che comprende requisiti di cibersicurezza per i prodotti connessi immessi sul mercato unico; c) contrastare coloro che cercano di compromettere, all'interno dell'UE, la sicurezza online e l'integrità dell'ambiente digitale o che promuovono la violenza e l'odio attraverso strumenti digitali, e chiamarli a rispondere delle loro azioni».

Un "diritto alla cybersicurezza", come già sostenuto altrove[81], dovrebbe essere volto a garantire solamente la dimensione della resilienza[82], o robustezza[83], ricomprendendo ad esempio i principi della sicurezza *by design* e *by default*, cioè unicamente quegli aspetti della cybersicurezza che si pongono in un'ottica di complementarietà – o in taluni casi di strumentalità – rispetto al godimento di altri beni fondamentali (es., il diritto alla riservatezza), e non quindi in un'ottica di conflitto, come nel caso di altre dimensioni della cybersicurezza (ad esempio, le fasi di rilevazione e risposta)[84].

Peraltro, se è vero che la cybersicurezza ha progressivamente visto riconoscersi uno speciale riconoscimento sul piano costituzionale per il tramite della tutela dei diritti alla privacy e alla protezione dei dati, come ricordato sopra, d'altra parte occorre anche riflettere sull'opportunità

[79] Chiara 2024b.

[80] Dichiarazione comune del Parlamento europeo, Consiglio e Commissione europea, Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, 2023/C 23/01. La Dichiarazione non è giuridicamente vincolante per gli Stati membri o per gli attori privati, né stabilisce alcun nuovo diritto che possa essere esercitato dai cittadini dell'Unione, e neanche influisce sul contenuto delle norme giuridiche rilevanti o sulla loro applicazione. Si veda sul punto, Papakonstantinou, De Hert 2024, 121. Allo stesso tempo, come osservato da Cocito e De Hert, la Dichiarazione dimostra la volontà dei responsabili politici dell'UE di partecipare alla conversazione su nuovi diritti digitali: si veda Cocito, De Hert 2023. Inoltre, secondo De Gregorio 2022, «*it cannot be excluded that courts, particularly the European Court of Justice, will refer to this instrument as a creative source of constitutional interpretation of the Charter, also considering the judicial activism shown by the CJEU in these years*».

[81] Chiara 2024b.

[82] Per un quadro analitico del concetto di "resilienza" nel contesto del diritto europeo della cybersicurezza si veda: Bygrave 2022; cfr. Chiara, Brighi 2024.

[83] Taddeo 2019, 350.

[84] Porcedda 2023.

di mantenere questo legame, soprattutto se analizzassimo taluni risvolti operativi sul piano del c.d. diritto secondario. Infatti, il diritto europeo alla protezione dei dati personali[85] non qualifica giuridicamente le violazioni di cybersicurezza *per se*. Le violazioni di sicurezza acquistano valore giuridico nel Regolamento (UE) 2016/679 (GDPR) nella misura in cui comportano «la distruzione, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o altrimenti trattati»[86]. Tuttavia, una violazione di misure tecniche ed organizzative[87] di cybersicurezza può causare danni alle persone fisiche, anche gravi (si pensi ad esempio ad ingenti danni materiali in termini di perdite finanziarie o immateriali in termini di ansia e disagio psicologico), senza il coinvolgimento di dati personali nell'incidente o nell'attacco. Se però la violazione di sicurezza non è qualificabile come violazione di dati personali, tali danni non costituiscono una violazione del diritto alla protezione dei dati personali.

Un nuovo diritto fondamentale alla cybersicurezza colmerebbe questa lacuna unificando un quadro normativo finora incompleto, tutelando una legittima aspettativa degli individui di godere di una "vita digitale sicura". In tal senso, il riconoscimento di "un diritto", o "diritti di cybersicurezza" non potrebbe prescindere da un percorso di emancipazione dai diritti alla privacy e alla protezione dei dati personali. Un nuovo diritto fondamentale alla cybersicurezza, che riconosca un'autonoma posizione di garanzia per la persona costituita da diversi diritti, quali un diritto di accesso a tecnologie (reti, servizi informativi, prodotti, processi informatici) sicure ed un diritto alla crittografia, troverebbe già una sua attuazione nel quadro normativo di matrice euro unitaria sviluppatosi negli ultimi anni. In questa direzione, l'espressione legislativa del principio di assicurare un accesso a tecnologie sicure trova spazio, per quanto concerne i prodotti con elementi digitali (sia hardware che software) nel Regolamento UE 2024/2847 (c.d. Cyber Resilience Act)[88] e, per quanto riguarda i servizi, nella direttiva UE 2022/2555 (c.d. Direttiva NIS2).[89]

5. *Conclusioni*

L'evoluzione della cybersicurezza da questione prevalentemente tecnica a problema strategico, sociale, politico e giuridico, il cui governo non interessa solo gli attori statali – prerogativa tradizionale nella dimensione "analogica" – ma anche attori privati, che detengono parti considerevoli dell'infrastruttura tecnica su cui si basa la società digitale, sottolinea la sua crescente centralità nel dibattito giuridico. La sentenza *Podchasov v Russia* della Corte EDU evidenzia chiaramente il ruolo cruciale di alcune tecnologie di cybersicurezza, come la crittografia end-to-end, nella tutela di alcuni diritti umani quali il rispetto alla vita privata, alla corrispondenza e la libertà di espressione. Questo articolo ha sostenuto come tale sentenza legittimi una lettura "possibilista" per un riconoscimento autonomo, sul piano dei diritti fondamentali, slegato quindi dal pur "vicino"

[85] Art. 8della Carta dei diritti fondamentali dell'UE e art. 16 del Trattato sul funzionamento dell'Unione europea, ed attuato dal Regolamento generale sulla protezione dei dati personali, c.d. GDPR (Regolamento (UE) 2016/679).

[86] Art. 4 (12), Regolamento (UE) 2016/679.

[87] Articolo 32, Regolamento (UE) 2016/679. Si vedano le Conclusioni dell'avvocato generale G. Pitruzzella, presentate il 27 aprile 2023 (ECLI:EU:C:2023:353), nella causa della Corte di Giustizia dell'UE C-340/21, *VB contro Natsionalna agentsia za prihodite*: «la mera esistenza di una "violazione dei dati personali", come definita all'articolo 4, paragrafo 12, non sia di per sé sufficiente per concludere che le misure tecniche e organizzative attuate dal titolare del trattamento non erano "adeguate" a garantire la protezione dei dati in questione» [para. 84].

[88] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciber-resilienza).

[89] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), recepita in Italia con il decreto legislativo 4 settembre 2024, n. 138.

diritto alla privacy (e alla protezione dei dati, nel contesto del diritto dell'Unione europea), della cybersicurezza.

La strada che porta all'emersione di un "diritto alla cybersicurezza" nell'UE, che racchiuda diversi "diritti di cybersicurezza", è lastricata di ostacoli, di natura sia politica che giuridica, ancorché il diritto secondario dell'UE in materia di cybersicurezza adottato recentemente ponga già una solida base per la sua implementazione. In tal senso, la traiettoria che potrebbe seguire questo diritto sarebbe simile a quella percorsa dal diritto fondamentale alla protezione dei dati personali: introdotto nel diritto primario dell'Unione successivamente all'adozione della direttiva sulla protezione dei dati personali del 1995, quest'ultima è stata interpretata retroattivamente dalla Corte di Giustizia dell'UE alla luce del nuovo diritto di cui all'Art. 8 della Carta di Nizza e all'Art. 16 del TFUE[90]. In questo senso, il riconoscimento di nuovi "diritti di cybersicurezza" rappresenta non solo una risposta alle sfide attuali, ma anche una necessaria transizione verso una società digitale più resiliente e rispettosa delle libertà fondamentali.

[90] Gonzalez Fuster, Gellert 2012, 78; van der Sloot 2017, 11. Cfr. CGUE Caso C-543/09, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, ECLI:EU:C:2011:279 §50.

Riferimenti bibliografici

BROOKS R.R. 2014. *Introduction to Computer and Network Security: Navigating Shades of Gray*, CRC Press.

BRUNI A. 2019. *Promoting Coherence in the EU Cybersecurity Strategy,* in VEDDER A, SCHROERS J., DUCUING C., VALCKE P. (eds.), *Security and Law,* Intersentia, 253 ss.

BUTTARELLI G. 2016. *Encryption protects security and privacy*, Keynote speech at Assemblée nationale française, 21 novembre 2016.

BYGRAVE L.A. 2024. *The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes,* in «Computer Law & Security Review», 56, 2024, 1 ss.

BYGRAVE L.A. 2022. *Cyber Resilience versus Cybersecurity as Legal Aspiration,* in JANČÁRKOVÁ T. et al. (eds.), *14th International Conference on Cyber Conflict, CYCON,* NATO – CCDCOE.

CERRINA FERONI G., MORBIDELLI G. 2008. *La sicurezza: un valore superprimario,* in «Percorsi costituzionali», 1, 2008, 31 ss.

CHIARA P.G. 2024a. *Statutory Requirements for Communications Service Providers to Decrypt Online Communications Impair the Essence of Article 8 ECHR,* in «European Data Protection Law Review», 10, 2024, 312 ss.

CHIARA P.G. 2024b. *Towards a Right to Cybersecurity in EU Law? The Challenges Ahead,* in «Computer Law & Security Review», 53, 2023, 1 ss.

CHIARA P.G., BRIGHI R. 2024. *La dimensione della "resilienza" nel diritto UE della cybersicurezza,* in «Ragion Pratica», 63, 2024, 405 ss.

COCITO C., DE HERT P. 2023. *The Transformative Nature of the EU Declaration on Digital Rights and Principles: Replacing the Old Paradigm (Normative Equivalency of Rights),* in «Computer Law & Security Review», 50, 2023, 1 ss.

COLE M., VANDENDRIESSCHE A. 2016. *From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabo/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance*, in «European Data Protection Law Review», 2, 2016, 121 ss.

COMMISSIONE EUROPEA 2001. *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo,* COM(2001) 298 definitivo.

COMMISSIONE EUROPEA, ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA 2013. *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro,* JOIN(2013) 1 definitivo.

COMMISSIONE EUROPEA, ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA 2017. *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE,* JOIN(2017) 450 definitivo.

COMMISSIONE EUROPEA, ALTO RAPPRESENTANTE DELL'UNIONE PER GLI AFFARI ESTERI E LA POLITICA DI SICUREZZA 2020. *La strategia dell'UE in materia di cibersicurezza per il decennio digitale,* JOIN(2020) 18 definitivo.

CONSIGLIO DELL'UNIONE EUROPEA 2020. *La sicurezza attraverso la crittografia e nonostante la crittografia*, 12863/20.

DANG Q. 2012. *Recommendation for Applications Using Approved Hash Algorithms*, in *NIST Special Publication 800-107*.

DAVIES P. A. E. 2024. *A Right to Encryption in the European Union's Charter of Fundamental Rights,* in «Columbia Journal of European Law», 30, 2024, 52 ss.

DE GREGORIO G. 2022. *The Declaration on European Digital Rights and Principles: A First Analysis*

from Digital Constitutionalism, in «The Digital Constitutionalist», 2 febbraio 2022, disponibile in: https://digi-con.org/the-declaration-on-european-digital-rights-and-principles-a-first-analysis-from-digital- constitutionalism/ (consultato il 24 novembre 2024).

EDPB-GEPD 2022. *Parere congiunto n. 4/2022 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori*, disponibile in: https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf (consultato il 18 novembre 2024).

EDPB 2021. *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.*

EDPS, AEPD 2019. *Introduction to the Hash Function as a Personal Data Pseudonymisation Technique*.

ENISA, EUROPOL 2016. *On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA Joint Statement*, disponibile in: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection (consultato il 16 novembre 2024).

ENISA 2024. *Threat Landscape 2024*, disponibile in: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (consultato il 29 ottobre 2024).

ERMOSHINA K. et al. 2016. *End-to-End Encrypted Messaging Protocols: An Overview*, in BAGNOLI F. *et al.* (eds.), *INSCI 2016, LNCS 9934*, Springer International Publishing, 244 ss.

FLORIDI L. 2018. *Soft ethics, the governance of the digital and the General Data Protection Regulation*, in «Philosophical Transactions of the Royal Society A», 376, 2018, 1 ss.

FRATTASI B., POLLICINO O., SCARPELLINI F. 2024. *La cybersecurity è strategica per i diritti del cittadino e per la difesa del Paese: il ruolo dell'Agenzia per la cybersicurezza*, in «Il Sole 24 Ore», 22 novembre 2024.

GONZALEZ FUSTER G., GELLERT R. 2012. *The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right*, in «International Review of Law, Computers and Technology», 26, 2012, 73 ss.

GOUJARD C. 2024, *EU cancels vote on child sexual abuse law amid encryption concerns*, in Politico, 20 giugno 2024, disponibile in: https://www.politico.eu/article/eu-council-cancels-vote-on-encryption-breakingchild-sexual-abuse-law (consultato il 19 novembre 2024).

GUIHOT M. 2019. *Coherence in technology law*, in «Law, Innovation and Technology», 11, 2019, 311 ss.

HILDEBRANDT M. 2019. *Digital security and human rights: A plea for counter-infringement measures*, in SUSI M. (eds.), *Human Rights, Digital Society and the Law*, Routledge, 259 ss.

HOFFMAN L.J. 1995. *Building in Big Brother. The Cryptographic Policy Debate*, Springer.

JANSEN R. 2022. *Flaws in Legal Safeguards and Oversight Procedures Around Secret Surveillance in Bulgaria*, in «European Data Protection Law Review», 8, 2022, 137 ss.

KERR O. 2024. *The Digital Fourth Amendment: Privacy and Policing in Our Online World*, Oxford University Press.

KOOPS B.-J. 1999. *The Crypto Controversy – A Key Conflict in the Information Society*, Kluwer Law International.

KOOPS B.-J., KOSTA E. 2018. *Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark*, in «Computer Law & Security Review», 34, 2018, 1 ss.

LIAROPOULOS A. 2016. *Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-Stakeholderism, and Power Politics*, in «Journal of Information Warfare», 15, 2016, 14 ss.

LONGO E. 2024. *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in

«Rassegna Parlamentare», 2, 2024, 313 ss.

NERONI REZENDE I. 2024. *The Proposed Regulation to Fight Online Child Sexual Abuse: An Appraisal of Privacy, Data Protection and Criminal Justice Issues*, in «International Review of Law, Computers & Technology», 38, 2024, 369 ss.

PAPAKONSTANTINOU V. 2022. *Cybersecurity as Praxis and as a State: The EU Law Path Towards Acknowledgement of a New Right to Cybersecurity?*, in «Computer Law & Security Review», 44, 2022, 1 ss.

PAPAKONSTANTINOU V., DE HERT P. 2024. *The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis and EU Law Brutality at Play*, Routledge.

PORCEDDA M.G. 2023. *Cybersecurity, Privacy and Data Protection in EU Law: Law, Policy and Technology Analysis*, Hart Studies in Information Law and Regulation (serie), Bloomsbury Publishing.

PRENEEL B. 2010. *The First 30 Years of Cryptographic Hash Functionsand the NIST SHA-3 Competition*, in «CT-RSA 2010: Topics in Cryptology», Springer.

PRIVACY INTERNATIONAL 2022. *Securing Privacy: Privacy International on End-to-End Encryption*, report disponibile in: *https://privacyinternational.org/sites/default/files/2022-09/SECURING%20PRIVACY%20-%20PI%20on%20End-to-End%20Encryption.pdf* (consultato il 10 novembre 2024).

SCARFONE K. et al. 2017. *Guide to Storage Encryption Technologies for End User Devices*, in *NIST Special Publication 800-111*.

SCHNEIER B. 1995. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley.

SHURSON J. 2024. *A European right to end-to-end encryption?*, in «Computer Law & Security Review», 55, 2024, 1 ss.

STALLINGS W., BROWN L. 2018. *Computer Security: Principles and Practice*, Pearson.

TADDEO M. 2019. *Is cybersecurity a public good?*, in «Minds and Machines», 29, 2019, 349 ss.

TRENGOVE M. et al. 2022. *A critical review of the Online Safety Bill*, in «Patterns», 3, 2022, 1 ss.

VAN DAALEN O. 2023. *The right to encryption: Privacy as preventing unlawful access*, in «Computer Law & Security Review», 49, 2023, 1 ss.

VAN DER SLOOT B. 2017. *Legal Fundamentalism: Is Data Protection Really a Fundamental Right?*, in LEENES R. et al. (eds.), *Data protection and privacy: (in)visibilities and infrastructures*, Springer.

VAN 'T SCHIP M., BORGESIUS F.Z. 2024. *Podchasov v. Russia: the European Court of Human Rights emphasizes the importance of encryption*, in «EU Law Analysis» (online blog), disponibile in: *https://eulawanalysis.blogspot.com/2024/04/podchasov-v-russia-european-court-of.html* (consultato il 10 novembre 2024).

VERHEUL E. et al. 2016. *Polymorphic Encryption and Pseudonymisation for Personalised Healthcare*, Whitepaper, Institute for Computing and Information Sciences Radboud University Nijmegen, The Netherlands, disponibile in: *https://eprint.iacr.org/2016/411.pdf* (consultato il 5 novembre 2024).

WIEWIÓROWSKI W. 2020. *The Future of Encryption in the EU*, ISOC 2020 Webinar Keynote Speech.

WIEWIÓROWSKI W. 2023. *Cybersecurity and Data Protection: a necessary and powerful duo*, 28 settembre 2023, disponibile in: *https://www.edps.europa.eu/press-publications/press-news/blog/ cybersecurity-and-data-protection-necessary-and-powerful-duo_en* (consultato il 22 novembre 2024).

ZICCARDI G. 2003. *Crittografia e diritto*, Giappichelli.