LA COOPERAZIONE GIUDIZIARIA MULTILATERALE: DALLA CONVENZIONE DI BUDAPEST ALLA CONVENZIONE DELLE NAZIONI UNITE SUL *CYBERCRIME*(*)

di Concetta Locurto

1. Introduzione.

Lo sviluppo delle tecnologie dell'informazione e della comunicazione hanno profondamente cambiato le modalità delle connessioni personali e globali, incidendo sulla vita politica, economica e sociale delle comunità, al loro interno e nelle loro relazioni. Al contempo, hanno aperto nuovi e redditizi orizzonti alla criminalità.

Se si considera come e quanto la struttura e il funzionamento di fondamentali settori della vita economica e sociale siano mutati, a seguito della realizzazione e della diffusione capillare e globale delle reti *web* (negli anni Novanta dello scorso secolo) e poi del *web* 2.0 (nel primo decennio del Duemila) e a come e a quanto si sia contemporaneamente espansa la criminalità informatica, preoccupano le ulteriori opportunità che tale criminalità può trarre dalle nuove frontiere della tecnologia. Si pensi, ad esempio, alle potenzialità insite nel *web* 3.0, la terza fase dell'evoluzione di

(*) Il presente scritto rielabora e aggiorna il testo della relazione presentata al Corso «*La crisi della giurisdizione penale nella società digitalizzata. Sfide, ostacoli, nuovi modelli di investigazione e di cooperazione giudiziaria. Corso dedicato a Vittorio Occorsio*», organizzato dalla Scuola superiore della Magistratura e dalla Fondazione Occorsio, svoltosi a Firenze il 28 ottobre 2025. L'A., quale Consigliere giuridico della Rappresentanza Permanente di Italia presso le Organizzazioni Internazionali a Vienna e membro della delegazione italiana, ha partecipato ai negoziati per la elaborazione della Convenzione ONU sul crimine informatico, svoltisi a Vienna e a New York nel biennio 2022-2024.

Editore Associazione "Progetto giustizia penale" | via Festa del Perdono 7, 20122 Milano
c/o Università degli Studi di Milano, Dipartimento di Scienze Giuridiche "Cesare Beccaria"
redazione@sistemapenale.it

internet, caratterizzata da interconnettività, ubiquità e intelligenza artificiale, ma anche da indipendenza dagli intermediari e da resistenza alla censura.

Le sfide che originano dall'evoluzione della tecnologia impongono, nel settore della prevenzione e della repressione dei reati, di agire in plurime direzioni, al fine di:

- armonizzare gli ordinamenti penali degli Stati nazionali sotto il profilo sostanziale e processuale;
- sviluppare una politica condivisa di cooperazione giudiziaria;
- collaborare con le società e con gli imprenditori privati del settore;
- adottare tecniche e strumenti investigativi idonei a fronteggiare la rapidità e diffusività delle condotte dei cyber-criminali.

La partita si gioca non solo sul piano dell'ammodernamento e della condivisione dello strumentario tecnologico e investigativo, indispensabile per comprendere, intercettare e contrastare la diffusione delle condotte illecite, ma anche sul piano del diritto sostanziale, per la necessità di avvicinare gli ordinamenti giuridici e consentire il dialogo e lo scambio che solo la comunanza (di istituti giuridici, principi, linguaggio) può abilitare.

È quasi pleonastico, oggi, ricordare come il passaggio dal mondo analogico a quello digitale abbiano rivoluzionato la tradizionale dimensione spaziale e temporale. La rete internet non conosce frontiere; i suoi servizi possono essere prestati da qualsiasi luogo del mondo e non richiedono necessariamente un'infrastruttura fisica, né la presenza di un'azienda o di personale, tanto negli Stati in cui sono offerti, quanto nel mercato interno nel suo insieme. Anche la conservazione dei dati elettronici può avvenire in qualsiasi luogo del mondo, che il prestatore o amministratore di servizi internet (*internet service-provider* o *ISP)* sceglie in base alle più diverse ragioni, quali la sicurezza dei dati, le economie di scala, la rapidità di accesso, ma anche la normativa e il sistema processuale del Paese ospitante.

La diffusione del *web*, la creazione di un nuovo spazio de-materializzato in cui possono realizzarsi le più diverse condotte umane, lecite e illecite, svincolate da un necessario rapporto con il "territorio" degli Stati, ha messo in crisi il concetto tradizionale di sovranità territoriale degli Stati e la pretesa di regolare autonomamente gli accadimenti umani verificatisi sul proprio territorio. Nel *cyber*-spazio un'azione criminosa può essere ideata e concordata in uno Stato, eseguita attraverso dispositivi situati in uno o più Stati differenti e produrre i propri effetti in ancora altri Stati.

Analoghe considerazioni valgono per la prova dei reati, che sempre più spesso è una prova elettronica o digitale (la c.d. *e-evidence*), consistente in dati elaborati o trasmessi da un dispositivo elettronico, senza che conti dove sono conservati o generati (*content-data*, quali e-mail, sms o fotografie; *non-content data*, come l'abbonamento e il traffico dei dati, il *routing* e *timing* di un messaggio): una prova caratterizzata da altissima volatilità e rappresentata da dati che possono essere trasferiti, modificati o cancellati istantaneamente, con un comando (un semplice "*click*") impartito da qualsiasi parte del mondo, ovunque essi si trovino.

È evidente che per fronteggiare efficacemente una criminalità non legata al territorio di uno specifico Stato, ma che spesso esonda rispetto ai confini della sovranità nazionale, è indispensabile che i sistemi giuridici dei diversi Paesi "dialoghino" tra loro,

utilizzando un linguaggio comune. È anche necessario che le forze dell'ordine e le autorità giudiziarie siano poste in grado di tracciare e raccogliere tempestivamente la prova del reato, ovunque si trovi.

Da qui trae origine, specialmente negli anni più recenti (e nonostante la profonda crisi del multilateralismo nel contesto geopolitico contemporaneo), il rinnovato interesse per l'adozione di accordi internazionali che consentano di contrastare la criminalità informatica, sia a livello regionale, che sovranazionale, promuovendo l'armonizzazione dei quadri normativi di riferimento (la cui frammentazione rende spesso inane lo sforzo degli organi investigativi per ricostruire i fatti e raccogliere le prove) e rafforzando gli strumenti di cooperazione internazionale fra le forze di polizie e le autorità giudiziarie.

È così che, a quasi un quarto di secolo dal trattato antesignano in materia di criminalità informatica, la Convenzione sulla criminalità informatica del Consiglio d'Europa, hanno preso nuovo slancio gli strumenti di cooperazione internazionale.

Tra questi, nell'ambito del diritto dell'Unione europea, il regolamento (UE) 2023/1543 relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali.

Il regolamento, applicabile a partire dal 18 agosto 2026, è volto a:

- consentire alle autorità giudiziarie nazionali coinvolte in procedimenti penali di ordinare ai prestatori di servizi che offrono servizi nella UE[1] di produrre o conservare prove elettroniche ovunque possano essere localizzati i dati;
- agevolare e velocizzare l'accesso transfrontaliero alle prove elettroniche ed evitarne la cancellazione, assicurando al contempo garanzie giuridiche alle persone i cui dati sono stati richiesti.

Integra il quadro normativo sovranazionale, nello stesso ambito, la direttiva (UE) 2023/1544, del Parlamento europeo e del Consiglio, del 12 luglio 2023, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali, attuata nell'ordinamento interno con il decreto legislativo 30 dicembre 2025, n. 216 (Attuazione della direttiva (UE) 2023/1544 del Parlamento europeo e del Consiglio, del 12 luglio 2023, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali).

La direttiva, per agevolare la raccolta delle prove elettroniche da utilizzare nei procedimenti penali, impone che determinati prestatori di servizi che operano nell'Unione europea dispongano di stabilimenti designati o di rappresentanti legali nominati nell'Unione, in modo da poter ricevere e ottemperare agli ordini delle autorità nazionali.

---

[1] Il regolamento (UE) 2023/1543 si applica ai prestatori di servizi che forniscono una o più delle seguenti categorie di servizi nell'Unione: servizi di comunicazioni elettroniche; nomi di dominio internet e numerazione IP; servizi di comunicazione, archiviazione e trattamento.

Si tratta di strumenti che intendono accelerare l'accesso delle autorità ai dati digitali necessari per indagare e perseguire gli illeciti penali, indipendentemente dal luogo dove tali dati sono situati.

In questo contesto, con ambizioni maggiori (quanto all'ambito della regolamentazione e ai suoi destinatari), si colloca la Convenzione delle Nazioni Unite contro il crimine informatico *(United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*), adottata dall'Assemblea generale delle Nazioni Unite il 24 dicembre 2024 a New York, con la Risoluzione 79/243, aperta alla firma ad Hanoi (Vietnam) il 25 ottobre 2025.

2. Il quadro normativo a livello internazionale.

Prima di esaminare i contenuti della Convenzione ONU, è opportuno premettere alcuni cenni sul quadro normativo internazionale nel quale si inserisce il nuovo strumento pattizio, sia in ambito europeo (Convenzioni del Consiglio d'Europa, Direttive e Regolamenti dell'Unione europea), sia a livello più esteso (Convenzioni delle Nazioni Unite).

Particolare attenzione verrà dedicata alla Convenzione sulla criminalità informatica del Consiglio d'Europa, per lo speciale rilievo che essa riveste in materia, trattandosi dell'unico strumento di diritto internazionale pattizio, ad ampia base applicativa, attualmente in vigore.

2.1. La Convenzione di Budapest: inquadramento generale.

Adottata dal Consiglio d'Europa l'8 novembre 2001, entrata in vigore il 1° luglio 2004, la Convenzione sulla criminalità informatica (c.d. Convenzione di Budapest, dal luogo di apertura alla firma, il 23 novembre del 2001), rappresenta il più rilevante trattato internazionale in vigore in materia di *cybercrime* e di prova elettronica (*e-evidence*)[2].

Caratterizzata sin dalle origini da una vocazione tendenzialmente universale, non confinata alla *membership* del Consiglio d'Europa (pur non essendo membri del Consiglio d'Europa parteciparono ai negoziati anche il Canada, il Giappone, il Sudafrica e gli USA) la Convenzione di Budapest è aperta all'adesione di qualsiasi Stato disponibile ad attuare le sue previsioni e ad allacciare la cooperazione internazionale. Grazie all'ampia base di consenso che ha aggregato e al suo linguaggio neutrale,

[2] Utili indicazioni sulla storia, i contenuti, le prassi applicative della Convenzione di Budapest sono reperibili sul sito del Consiglio di Europa, al seguente *link*: https://www.coe.int/en/web/cybercrime/the-budapest-convention

adattabile all'evoluzione della tecnologia, da oltre venti anni essa rappresenta un efficace strumento di risposta al *cybercrime*, non solo in Europa, ma anche a livello globale.

Ad oggi vede l'adesione di 81 Stati[3], di cui 45 del Consiglio d'Europa (dei quali 26 membri della UE) e 37 esterni ad esso[4]; a questi si aggiungono 16 Stati "osservatori", firmatari o invitati ad aderirvi (tra questi l'Irlanda, unico Paese del Consiglio d'Europa e dell'Unione europea che ha firmato la Convenzione senza ancora ratificarla)[5].

Sono 11, inoltre, le organizzazioni e gli enti "osservatori" della Convenzione[6].

Il Consiglio d'Europa annota che alla data del mese di dicembre 2024:[7]

- circa il 95% degli Stati membri delle Nazioni Unite aveva attuato o era in procinto di attuare la riforma della propria legislazione in materia di criminalità informatica, con progressi significativi in Africa, nelle Americhe, in Asia, in Europa e in Oceania;
- molti Paesi presentavano ancora riforme incomplete, progetti di legge in sospeso da anni e difficoltà di applicazione delle nuove leggi, palesando la necessità di un sostegno per lo sviluppo delle proprie competenze (*capacity-building support*);
- il 68% degli Stati membri delle Nazioni Unite aveva adottato disposizioni di diritto penale sostanziale, per rendere punibili i reati compiuti contro e mediante i computer, conseguendo significativi progressi rispetto al 2013;
- il 52% degli Stati aveva la disponibilità di misure procedurali specifiche per assicurare la raccolta e la conservazione delle prove elettroniche; molti però, continuavano ad affidarsi a disposizioni di diritto procedurale generale, evidenziando la necessità di un ulteriore rafforzamento delle loro capacità;
- quasi il 50% degli Stati membri delle Nazioni Unite era parte o firmatario della Convenzione sulla criminalità informatica, con 95 Stati membri od osservatori del Comitato della Convenzione sulla criminalità informatica (T-CY);
- numerosi Paesi avevano avviato riforme volte ad attuare il Secondo protocollo alla Convenzione sulla criminalità informatica relativo al rafforzamento della cooperazione e alla divulgazione delle prove elettroniche.

La Convenzione è sostenuta dal Comitato della Convenzione sulla criminalità informatica (T-CY) che ne controlla l'attuazione, e dall'Ufficio per il programma sulla criminalità informatica di Bucarest, Romania, che sostiene i Paesi in tutto il mondo

---

[3] La lista integrale è reperibile al *link*: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

[4] Tra gli ultimi a ratificarla: il Ruanda, il 1.10.2025; la Nuova Zelanda, il 28.8.2025; São Tomé and Príncipe e Vanuatu, il 5.6.2025.

[5] Benin, Burkina Faso, Cameroon, Côte d'Ivoire, Ecuador, Fiji, Guatemala, Ireland, Korea, Mexico, New Zealand, Niger, Sierra Leone, South Africa, Timor-Leste, Trinidad and Tobago, Tunisia, Uruguay, Vanuatu.

[6] African Union Commission (AUC); Commonwealth Secretariat; European Union (European Commission and Council of the European Union, Eurojust, Europol, European Union Agency for Cybersecurity (ENISA)); G7 High-Tech Crime Subgroup; International Telecommunication Union (ITU); Interpol; Organisation for Economic Cooperation and Development (OECD); Organisation for Security and Co-operation in Europe (OSCE); Organisation of American States (OAS); Southeast European Law Enforcement Center (SELEC); United Nations Office on Drugs and Crime (UNODC).

[7] https://www.coe.int/en/web/cybercrime/-/the-global-state-of-cybercrime-legislation-2013-2024

attraverso programmi di formazione, come il progetto GLACY (*Global Action on Cybercrime*).

Si tratta di iniziative ed uffici poco conosciuti tra i non addetti ai lavori. Eppure, forniscono suggerimenti, materiale, approfondimenti molto utili ai fini applicativi, specie per la risoluzione dei problemi che possono insorgere nella cooperazione internazionale. Molto efficaci e puntuali, ad esempio, sono le guide (*Guidance Notes*) pubblicate dal Comitato della Convenzione sulla criminalità informatica a partire dal dicembre 2012: guide che hanno significativamente facilitato l'utilizzo e l'attuazione del trattato, anche alla luce delle modifiche del quadro giuridico, politico e degli sviluppi tecnologici. Sebbene non si tratti di strumenti giuridicamente vincolanti, esse rappresentano un substrato interpretativo condiviso tra i Paesi parte in ordine all'utilizzo della Convenzione[8].

Sempre in termini generali, va evidenziato che la Convenzione sulla criminalità informatica del Consiglio d'Europa non è esclusivamente un trattato sul *cybercrime*, ma consente l'adozione di *misure procedurali* e il ricorso alla cooperazione internazionale in relazione a qualsiasi reato per il quale assuma rilevanza la prova elettronica.

Si tratta, quindi, di uno strumento articolato, dagli obiettivi ambiziosi, che continua a guidare le riforme della legislazione in materia di criminalità informatica in tutto il mondo.

Come evidenziato nella *Explanation of Position of the United States on the Adoption of the Resolution on the UN Convention Against Cybercrime in UNGA's Third Committee* (l'illustrazione della posizione USA nella fase finale dei negoziati della nuova Convenzione ONU sul *cybercrime*), la Convenzione rappresenta tuttora «*the gold standard*» per la cooperazione internazionale in relazione al crimine informatico e alla prova elettronica. Essa, infatti, fornisce orientamenti a *qualsiasi* Paese che intenda sviluppare leggi nazionali in materia e funge da punto di riferimento, con modelli di intervento normativo e prassi operative, per una comunità larghissima di Stati, anche non (o non ancora) parti del trattato.

La Convenzione, infine, è corredata da due Protocolli addizionali:

1. un Protocollo sugli atti di natura razzista e xenofoba commessi a mezzo di sistemi informatici (2003), che punta a criminalizzare tanto la diffusione di materiale razzista e xenofobo tramite sistemi informatici, quanto le minacce e gli insulti di matrice razzista e xenofoba;

---

[8] Nel 2017, ad esempio, è stata adottata una guida molto utile per superare i dubbi e le difficoltà operative in materia di ordini di produzione di dati (*T-CY Guidance Note #10 - Production Orders for Subscriber Information*.). A fine novembre 2022, invece, è stata pubblicata una guida sull'attualissimo tema degli attacchi *ransomware*, sistemi informatici o virus "malevoli" che prendono il controllo del computer di un utente ed eseguono la crittografia dei dati; quindi, chiedono un riscatto (*ransom)* per ripristinare il normale funzionamento (*T-CY Guidance Note #12- Aspects of ransomware covered by the Budapest Convention).* L'ultima guida, pubblicata nel giugno 2025 riguarda invece le informazioni spontanee che, ai sensi dell'art. 26 della Convenzione, le Autorità possono fornire, senza preventiva richiesta, quando vengono in possesso di dati che ritengono utili per altre indagini e procedimenti penali, anche se l'Autorità destinataria non ne è ancora a conoscenza (*T-CY Guidance Note #14 - Spontaneous information*). Le Guide sono reperibili sul sito del Comitato, al link https://www.coe.int/en/web/cybercrime/guidance-notes

2. un Secondo Protocollo aggiuntivo (deliberato dal Consiglio d'Europa il 17 novembre 2021 e firmato dall'Italia il 12 maggio 2022) sul rafforzamento della cooperazione e della divulgazione delle prove elettroniche.

Il Secondo Protocollo addizionale entrerà in vigore quando almeno 5 Stati lo avranno ratificato. Al momento lo hanno firmato 52 Stati e solo 3 lo hanno ratificato[9].

2.1.1. Scopo e struttura della Convenzione.

La Convenzione nasce dall'esigenza di contrastare una forma di criminalità – quella "informatica" – connotata dal carattere transnazionale e dalle potenzialità dello strumento di cui si giova, connotato da facilità di accesso, efficacia e velocità. È noto, infatti, che, servendosi della connessione fra sistemi informatici distanti fra loro, l'autore di un reato è in grado di agire in un luogo e produrre effetti, in tempo reale, in uno o più luoghi diversi, soggetti a giurisdizioni distanti e differenti. In un simile contesto, è cruciale poter disporre di strumenti di cooperazione internazionale tempestivi ed efficaci per assicurare la raccolta delle prove, l'accertamento dei reati, la punizione dei loro autori, dovunque si trovino.

Il trattato, quindi, intende contribuire al contrasto tanto dei reati che possono essere commessi solo attraverso l'uso della tecnologia, in cui i dispositivi sono allo stesso tempo lo strumento per commettere il reato e l'obiettivo del reato (c.d. "*cyber-dependent crimes*"), quanto dei reati in cui la tecnologia è utilizzata per favorire la commissione di un altro reato, come avviene ad esempio nelle frodi (c.d. "*cyber-enabled crimes*"), mediante due piani di intervento concorrenti:

- l'armonizzazione dei quadri normativi vigenti nei diversi Paesi, per uniformare o, comunque, avvicinare il più possibile le legislazioni di carattere sostanziale e processuale;
- lo sviluppo e la regolamentazione della cooperazione internazionale: cooperazione che in tanto può essere efficace, in quanto sia fondata su un substrato comune di diritto armonizzato, che consenta agli Stati di intendersi e dialogare, condividendo nozioni, principi fondamentali, fattispecie penali e misure procedurali atte ad assicurare prontamente le prove.

Il perseguimento delle esigenze sopra richiamate è informato all'attenta considerazione del rispetto dei diritti umani e del principio di proporzionalità, in conformità delle indicazioni contenute:

- nel *preambolo* della Convenzione, che richiama la necessità di garantire un equo bilanciamento tra l'interesse per l'azione repressiva e il rispetto dei diritti umani fondamentali, quali previsti dalla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, adottata dal Consiglio d'Europa del 1950 (CEDU), nel Patto internazionale sui diritti civili e politici, adottato dalle Nazioni Unite del 1966 (PIDCP), e negli altri trattati a tutela dei diritti umani. Tali fonti

[9] Sul Secondo Protocollo si tornerà *infra,* al par. 2.2.

riaffermano il diritto di ciascuno di avere opinioni senza condizionamenti, il diritto alla libertà di espressione, comprensivo del diritto di cercare, ricevere, e trasmettere informazioni e idee di ogni tipo, senza limiti di frontiere, e del diritto al rispetto della *privacy*;

- nell'art. 15 (*Conditions and safeguards*) del trattato, che impone agli Stati parte di assoggettare l'introduzione e l'applicazione dei poteri e delle misure procedurali previste dalla Sezione II del Capitolo II a precise condizioni e salvaguardie, affinché sia assicurata un'adeguata tutela dei diritti umani e delle libertà; in particolare quelli discendenti dalla CEDU, dal PIDCP e dagli altri strumenti internazionali applicabili in materia di diritti umani. Tali condizioni e salvaguardie debbono includere il principio di proporzionalità e, quando appropriato in rapporto alla natura della procedura e del potere, il controllo giudiziario anche di altra autorità indipendente; un'adeguata base giuridica che giustifichi l'esercizio del potere; le limitazioni relative all'oggetto e alla durata di poteri e misure procedurali[10].

Quanto alla sua struttura, la Convenzione si articola in quattro capitoli, dedicati a: 1) Definizioni; 2) Misure da adottare a livello nazionale, in tema di diritto sostanziale e processuale; 3) Cooperazione internazionale; 4) Clausole finali.

2.1.2. Le misure di diritto sostanziale.

In materia di diritto penale sostanziale, la Convenzione estende l'obbligo di incriminazione a un ampio ventaglio di condotte dolose aventi a oggetto dati o sistemi informatici, attuate per il tramite di computer, internet o altre tecnologie informatiche di comunicazione.

L'inventario delle incriminazioni, contenuto nel Capitolo II, Sezione I (*Substantive criminal law*) comprende:

- le "classiche" fattispecie di c.d. "*cyber-dependent crimes*", ossia i reati commessi necessariamente con l'uso della tecnologia informatica, nei quali il dispositivo informatico integra sia lo strumento, sia l'oggetto della condotta illecita. Si tratta

[10] Article 15. Conditions and safeguards. 1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2- Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

di reati che offendono la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici (l'accesso illegale, l'intercettazione illegale, l'interferenza nei dati, l'interferenza in un sistema, l'uso improprio di dispositivi);

- i c.d. "*cyber-enabled crimes*", nei quali lo strumento informatico costituisce il mezzo di commissione del reato che intensifica l'offesa di beni e interessi molto spesso già tutelati dal diritto penale. Ne fanno parte la falsità informatica, la frode informatica, la pedopornografia e i reati in materia di diritto d'autore.

Più nel dettaglio, le incriminazioni sono raggruppate in quattro titoli:

1) Titolo I. Reati contro la riservatezza, l'integrità e la disponibilità dei dati *(Offences against the confidentiality, integrity and availability of computer data and systems)*:

- l'accesso illegale, intenzionale e senza diritto, a tutto o parte di un sistema informatico (art. 2. *Illegal access*);
- le intercettazioni illegali e, cioè, le intercettazioni di dati informatici, intenzionali e illecite, effettuate, mediante mezzi tecnici, durante trasmissioni non pubbliche (art. 3. *Illegal interception*);
- l'attentato all'integrità dei dati (danneggiamento, cancellazione, deterioramento, alterazione e soppressione dei dati informatici) compiuto intenzionalmente e senza averne diritto (art. 4. *Data interference*);
- l'attentato all'integrità dei sistemi, consistente nell'impedimento grave al funzionamento di un sistema informatico, effettuato intenzionalmente e senza averne diritto, mediante danneggiamento, cancellazione, deterioramento, alterazione o soppressione dei dati informatici (art. 5. *System interference*);
- la produzione, la vendita, l'ottenimento per l'uso, l'importazione, la diffusione o ogni altra forma di messa a disposizione, senza averne diritto, di dispositivi o programmi informatici realizzati specificamente per permettere la commissione dei delitti sopra indicati, nonché di *password*, di codici di accesso o di sistemi analoghi che consentano di accedere a tutto o in parte ad un sistema informatico (art. 6. *Misuse of devices*).

2) Titolo II. Reati connessi all'utilizzo del computer (*Computer-related offences*):

- la falsificazione informatica, ossia l'introduzione, l'alterazione, la cancellazione, la soppressione intenzionale e senza diritto di dati informatici, con l'intento di utilizzarli a fini legali come se fossero autentici (art. 7. *Computer-related forgery*);
- la frode informatica, ossia il fatto di causare intenzionalmente e senza diritto un pregiudizio patrimoniale ad altri, con l'intento di ottenere un indebito vantaggio patrimoniale per sé o altri, mediante l'introduzione, l'alterazione, la cancellazione, la soppressione intenzionale di dati informatici o mediante qualsiasi interferenza sul funzionamento di un sistema informatico (art. 8. *Computer-related fraud*).

3) Titolo III. Reati relativi ai contenuti (*Content-related offences*):

- la produzione, intenzionale e senza diritto, mediante un sistema informatico, di materiale pornografico minorile, nonché l'offerta o messa a disposizione,

diffusione, trasmissione o procacciamento per sé o per altri o il possesso dello stesso materiale (art. 9. *Offences related to child pornography*[11]).

4) Titolo IV. Reati contro la proprietà intellettuale e diritti collegati

- la violazione dei diritti sulla proprietà intellettuale e i diritti collegati, se commessi dolosamente, su scala commerciale e attraverso l'utilizzo di un sistema informatico (art. 10 *Offences related to infringements of copyright and related rights*).

Infine, per tutti i tipi di reati sopra indicati sono previste la punizione del concorso di persone (art. 11.1) e la responsabilità (penale, civile o amministrativa) delle persone giuridiche per le condotte commesse da persone fisiche che esercitino poteri direttivi nel loro ambito e nel loro interesse (art. 12). I reati previsti dagli artt. 3-5, 7, 8 e 9.1 lettere a) e c) sono perseguiti nella forma del tentativo (art. 11.2).

È altresì stabilito l'obbligo degli Stati parte di adottare sanzioni effettive, proporzionate, dissuasive anche in forma detentiva (art. 13).

2.1.3. Le misure procedurali.

Il Capitolo II, Sezione II (*Procedural law*), della Convenzione contiene disposizioni riguardanti l'ambito processuale. L'art. 14 impone agli Stati di adottare una serie di misure *procedurali,* per indagini o procedimenti penali specifici, in relazione:

a) ai reati previsti in conformità agli articoli da 2 a 11 della Convenzione;
b) a tutti gli altri reati commessi attraverso un sistema informatico;
c) alla raccolta delle prove elettroniche (*e-evidence)* di qualsiasi reato.

In particolare – fatte salve alcune riserve in relazione agli strumenti di indagine più intrusivi, quali la raccolta di dati in tempo reale o l'intercettazione di *content-data* – il trattato obbliga i Paesi parte ad adottare, all'interno dei rispettivi ordinamenti, le seguenti misure:

---

[11] Article 9 – Offences related to child pornography
1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
a) producing child pornography for the purpose of its distribution through a computer system;
b) offering or making available child pornography through a computer system;
c) distributing or transmitting child pornography through a computer system;
d) procuring child pornography through a computer system for oneself or for another person;
e) possessing child pornography in a computer system or on a computer-data storage medium.
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
a) a minor engaged in sexually explicit conduct;
b) a person appearing to be a minor engaged in sexually explicit conduct;
c) realistic images representing a minor engaged in sexually explicit conduct.
3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d and e, and 2, sub-paragraphs b and c.

- la conservazione e la divulgazione rapida dei dati archiviati e di traffico (artt. 16 e 17);
- l'ordine di produzione emesso dall'autorità giudiziaria nei confronti dei soggetti e dei fornitori di servizi situati sul territorio dello Stato che siano in possesso di dati informatici contenuti in un sistema o su supporti informatici (art. 18);
- le perquisizioni e i sequestri di sistemi e supporti informatici con possibilità di fare e trattenere copia dei dati, da mantenere integri o da rimuovere dal sistema informatico analizzato (art. 19);
- la raccolta o la registrazione in tempo reale, in regime di segretezza, di dati relativi al traffico concernenti specifiche comunicazioni, effettuate attraverso un sistema informatico, qualora ciò non contrasti con il diritto nazionale (art. 20). L'applicazione di tali misure può essere circoscritta a taluni specifici reati, da indicare espressamente nelle riserve eventualmente apposte all'atto della ratifica, purché il novero di tali reati comprenda quanto meno le fattispecie alle quali, nel diritto interno, sono applicabili le misure di cui al punto che segue (art. 14).
- la raccolta o la registrazione in tempo reale, in regime di segretezza, di dati relativi al *contenuto* di specifiche comunicazioni effettuate attraverso un sistema informatico, con riguardo a reati di particolare gravità previamente individuati, ove detto mezzo di ricerca della prova sia previsto dal sistema processuale nazionale (art. 21).

Come già si è detto sopra,[12] le misure in questione debbono essere oggetto di istituti di garanzia ai fini della salvaguardia dei diritti umani e delle libertà fondamentali, quali protetti, in particolare, alla CEDU e dal PDCP.

Gli istituti di garanzia devono comprendere, fra l'altro, compatibilmente e coerentemente con la natura di ciascun tipo di misura, forme di controllo giudiziario sulla sussistenza dei presupposti per l'adozione delle misure, nonché limitazioni del campo di applicazione e della durata delle stesse (art. 15).

2.1.4. La cooperazione internazionale.

Il Capitolo III, relativo alla cooperazione internazionale, contiene le disposizioni relative a: estradizione (art. 24); assistenza giudiziaria (art. 25); informazioni spontanee (art. 26); procedura relativa alla domanda di assistenza in assenza di accordi internazionali applicabili (art. 27); riservatezza delle informazioni e restrizioni nella loro utilizzazione (art. 28); assistenza in materia di misure di conservazione rapida (art. 29) e divulgazione rapida dei dati conservati (art. 30); assistenza concernente l'accesso ai dati (art. 31), l'accesso tranfrontaliero ai dati con il consenso dell'avente diritto o ai dati accessibili al pubblico (art. 32); assistenza nella raccolta in tempo reale dei dati relativi al traffico (art. 33) e nell'intercettazione dei dati relativi al contenuto (art. 34); rete 24/7 (art. 35).

[12] Par. 2.1.1.

In estrema sintesi, le disposizioni regolano la raccolta transnazionale delle prove elettroniche, secondo meccanismi di cooperazione internazionale volti a costituire, nella misura più ampia possibile, un sistema efficace, rapido e ispirato ai principi generali dell'obbligo di cooperazione (art. 23), sia ai fini sia estradizionali (art. 24), sia ai fini della mutua assistenza (art. 25). Le norme mirano a favorire lo scambio spontaneo e veloce di informazioni potenzialmente utili per l'inizio o lo svolgimento di indagini o di procedimenti relativi a reati previsti dalla Convenzione, senza obbligo di previa ricezione di richiesta (art. 26) e con assicurazione di assistenza immediata mediante l'individuazione di un "punto di contatto" in ciascuno Stato, sempre disponibile 24 ore su 24 e 7 giorni su 7 (art. 35).

In particolare, si segnalano i tre principi fondamentali relativi alla cooperazione internazionale, fissati dall'art. 23:

- le parti devono cooperare reciprocamente nella misura più ampia possibile;
- la cooperazione non riguarda solo i reati oggetto di armonizzazione, ma si estende a tutti i reati connessi a sistemi o dati informatici (*criminal offences related to computer systems and data*), così come alla raccolta delle prove in forma elettronica di qualsiasi reato;
- la cooperazione deve svolgersi in conformità alle previsioni della Convenzione, facendo applicazione dei pertinenti strumenti di cooperazione internazionale in materia penale, degli accordi stretti sulla base delle legislazioni uniformi e reciproche e del diritto nazionale degli Stati parte.

2.1.5. La ratifica della Convenzione: a) le ricadute sul versante del diritto penale sostanziale (cenni).

Il Parlamento italiano ha ratificato e ordinato l'esecuzione della Convenzione con la legge 18 marzo 2008, n. 48 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno)[13].

La Relazione introduttiva del disegno di legge originario, presentato dal Governo il 19 giugno 2007 (A.C. n. 2807, XV Legislatura),[14] spiegava che l'adeguamento normativo richiesto, ai fini della ratifica della Convenzione, nel settore del diritto penale sostanziale era risultato «modesto, essendo, in molti casi, già in vigore una disciplina esaustiva, addirittura più incisiva di quella richiesta dalle disposizioni della Convenzione medesima».

---

[13] Sulla legge di ratifica della Convenzione di Budapest, *ex plurimis,* Aa.Vv. (a cura di LUPARIA), *Sistema penale e criminalità informatica,* Milano, 2009; AA.VV., (a cura di CORASANITI G., CORRIAS LUCENTE), Cybercrime, *responsabilità degli enti, prova digitale. Commento alla legge 18 marzo 2008, n. 48,* Padova, 2009; CAJANI, *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono...,* in *Cyberspazio e dir.*, 2010.

[14] Il ddl A.C. e i lavori preparatori sono reperibili al *link* https://leg15.camera.it/_dati/lavori/schedela/trovaschedacamera_wai.asp?Pdl=2807.

L'Italia, infatti, era stato «uno dei primi Paesi europei ad introdurre una legge organica, la legge 23 dicembre 1993, n. 547, in tema di delitti informatici».

Successivamente erano «entrate in vigore altre leggi, relative a specifici settori, volte a reprimere i comportamenti illeciti di pirateria informatica (legge 18 agosto 2000, n. 248, che ha modificato le disposizioni in materia della legge 22 aprile 1941, n. 633, introdotte dal decreto legislativo 29 dicembre 1992, n. 518), a garantire la protezione dei dati personali (legge 31 dicembre 1996, n. 675, e successive modificazioni), a contrastare la detenzione, lo scambio e il commercio di materiale pedopornografico in rete (legge 3 agosto 1998, n. 269) e ad estendere ai fenomeni di pedopornografia virtuale l'ambito di applicazione delle norme incriminatici introdotte dalla legge n. 269 del 1998 (legge 6 febbraio 2006, n. 38)».

Ciò nonostante, si ritenne «opportuno procedere all'integrazione o alla modifica di alcune disposizioni del codice penale, per considerazioni legate, da un lato, alla esigenza di una migliore collocazione sistematica, dall'altro, all'insorgere di nuove problematiche che avevano determinato l'inadeguatezza delle originarie forme di tutela».

Di fatto, le modifiche di diritto penale sostanziale apportate in conseguenza degli obblighi derivanti dalla Convenzione si ridussero a quelle dettate dagli artt. 4 e 5 della legge di ratifica[15]:

- l'art. 4 sostituì l'originaria formulazione dell'art 615-*quinquies* cod. pen. con una nuova tipizzazione della fattispecie incriminatrice, che puniva il c.d. abuso di dispositivi, ossia la «diffusione di apparecchiature, dispositivi e programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico»;
- l'art. 5, invece, riscrisse l'intero "sistema" delle fattispecie di danneggiamento informatico (ossia delitti contro la sicurezza e l'integrità di dati e sistemi), modificando la previgente incriminazione del delitto di «Danneggiamento di informazioni, dati e programmi informatici» (art. 635-*bis* cod. pen.) e introducendo tre nuove ipotesi delittuose: il delitto di «Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità» (nuovo art. 635-*ter* cod. pen.); il delitto di «Danneggiamento di sistemi informatici o telematici» (nuovo art. 635-*quater* cod. pen.); il delitto di «Danneggiamento di sistemi informatici o telematici di pubblica utilità» (nuovo art. 635-*quinquies* cod. pen.).

Di rilievo, inoltre, con il d.lgs. 8 giugno 2001, n. 231 (Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300), l'aggiunta di un nuovo art. 24-*bis*, che estese la responsabilità amministrativa da reato delle persone giuridiche e degli enti a tutte le nuove fattispecie delittuose in materia di criminalità informatica introdotte nel codice penale sia dalla

---

[15] Così V. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. e proc.*, n. 6/2008, p. 700 e ss., cui si rinvia per una più ampia disamina delle innovazioni in materia penale sostanziale.

legge di ratifica n. 48 del 2008 (con esclusione del solo art. 495-*bis* cod. pen., concernente la falsa attestazione al certificatore di firma elettronica), sia dalla precedente l. n. 547 del 1993, salva l'esclusione del delitto di frode informatica, di cui all'art. 640-*ter* cod. pen., se non «commesso in danno dello Stato o di altro ente pubblico».

2.1.6. (*continua)*: b) le ricadute sul versante processuale (cenni).

Quanto alle innovazioni sul versante processuale[16], la legge n. 48 del 2008 intervenne sul codice di procedura penale lungo una duplice direttrice:

- attraverso l'integrazione di talune disposizioni del codice di procedura penale (che già disciplinavano misure di indagine corrispondenti a quelle previste dalla Convenzione) o l'adeguamento "lessicale" delle stesse, finalizzato a renderne esplicite le potenzialità applicative in campo informatico;
- mediante l'inserimento di *nuove* disposizioni procedurali, volte a disciplinare misure richieste dalla Convenzione non presenti nell'ordinamento interno.

Esempi del primo tipo di intervento sono le modifiche apportate agli articoli relativi alle ispezioni e alle perquisizioni, incidenti tanto sulla dimensione "statica" dei due mezzi di ricerca della prova descritti nel Libro terzo del codice di rito (artt. 244, 247 e 258 cod. proc. pen.), quanto sulla loro portata "dinamica" così come delineata nel Libro quinto (artt. 352 e 354 cod. proc. pen.)[17].

In particolare, sia per le attività disposte dall'autorità giudiziaria, sia per quelle di iniziativa della polizia giudiziaria, fu previsto un preciso *modus operandi*, a garanzia della genuinità delle acquisizioni: l'adozione di «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». Nell'art. 354 cod. proc. pen., dedicato agli accertamenti urgenti della polizia giudiziaria sui luoghi o sulle cose, fu altresì previsto l'obbligo degli ufficiali di polizia giudiziaria, in relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, oltre che di adottare le misure tecniche per salvaguardarne l'integrità, di provvedere, «ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità».

Senza voler entrare nel noto dibattito relativo al sequestro probatorio di materiale informatico conservato all'interno di dispositivi di archiviazione digitale[18], merita

---

[16] Sulle ricadute in materia processuale della legge di ratifica v, diffusamente L. LUPARIA, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. I profili processuali*, in *Dir. pen. e proc*., n. 6/2008, p. 717 e ss.

[17] La distinzione è di L. LUPARIA, *op. cit*., p. 719

[18] Il tema è caratterizzato da un ampio dibattito dottrinale e giurisprudenziale, che interessa il diritto interno e quello dell'Unione europea, come interpretato dalla Corte di giustizia. Si evidenzia, in generale, l'invasività di tale atto investigativo e la necessità della garanzia del vaglio giurisdizionale (pur con diverse modulazioni, tra chi ritiene sufficiente un decreto motivato del pubblico ministero e chi reputa, invece, necessario un atto di autorizzazione del giudice autorizzativo del giudice), nonché il rispetto del principio di proporzionalità. La materia è oggetto del disegno di legge C. 1822 – approvato dal Senato nel mese aprile 2024 e ancora all'esame della 2^ Commissione Giustizia della Camera dei Deputati (Modifiche al codice di procedura penale in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali).

ricordare anche le importanti modifiche apportate all'art. 254 cod. proc. pen. (Sequestro di corrispondenza), che hanno comportato l'ampliamento della nozione di "corrispondenza" alle forme di comunicazione elettronica.

Infatti, in conseguenza della sostituzione del comma 1 dell'art. 254 cod. proc. pen. e dell'interpolazione del suo comma 2, fu ampliato l'ambito applicativo della norma, consentendone l'operatività anche in relazione alla figura del c.d. *service provider*, vale a dire il fornitore di servizi telematici, assoggettabile all'attività di *adprehensio* dei dati da parte dell'autorità giudiziaria. Le modifiche legislative estesero, poi, l'oggetto del sequestro di corrispondenza a ogni corrispondenza, anche se inoltrata per via telematica, così fugando ogni dubbio sul fatto che la posta elettronica e le altre forme di comunicazione elettronica rientrino nel concetto di "corrispondenza". Il che, ovviamente, ha comportato l'estensione a tutte le forme di corrispondenze, così come nuovamente intese, dell'intero corredo di garanzie costituzionali e codicistiche che assistono il sequestro di "corrispondenza", tra le quali va ricordato il divieto per la polizia giudiziaria di procedere all'apertura e alla presa di conoscenza del relativo contenuto (la novella del 2008 aggiunse al riguardo anche l'ulteriore proibizione di "alterare" i dati trasmessi in via telematica).

Fu introdotto *ex novo*, invece, all'interno delle disposizioni sul sequestro probatorio, l'art. 254-*bis* cod. proc. pen., che disciplina il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni, con modalità tali da evitare turbative alla regolare fornitura di detti servizi.

Altro innesto innovativo fu quello in materia di "*data retention*", con l'introduzione dei commi 4-t*er*, 4-*quater* e 4-*quinquies* dell'art. 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196 ("*Codice privacy*").

Tali disposizioni disciplinano una misura che, conformemente a quanto richiesto dalla Convenzione (art. 16, *Expedited preservation of stored computer data*), permette il «congelamento» temporaneo e urgente di dati relativi al traffico telematico (esclusi comunque i contenuti delle comunicazioni), «anche in relazione alle eventuali richieste avanzate da autorità investigative straniere» (cfr. art. 29 Convenzione di Budapest).

La legge n. 48 del 2008 dispose che i fornitori di servizi fossero obbligati a conservare e proteggere i dati per un periodo di novanta giorni, prorogabile fino a sei mesi, su ordine di un ampio novero di soggetti (il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della

---

In giurisprudenza, la Corte di cassazione, sezione sesta penale, sentenza 1 aprile 2025 - 8 aprile 2025, n. 13585, discostandosi da una precedente pronuncia di altra sezione (sezione quinta penale, sentenza 28 gennaio 2025 – 28 febbraio 2025 , n. 8376) ha ritenuto che il sequestro dei dati contenuti in un dispositivo informatico a fini di indagine penale eseguito dal pubblico ministero senza la preventiva autorizzazione del giudice contrasti con la direttiva UE 2016/680, come interpretata dalla sentenza della Corte di Giustizia dell'Unione europea, Grande Camera, del 4 ottobre 2024, in causa C-548/21, che richiede un pronuncia autorizzatoria, in via preventiva, da parte di un giudice o un organo amministrativo indipendente. Tale non può essere ritenuto, secondo il Supremo Collegio, il pubblico ministero, il quale non ha il compito di dirimere in piena indipendenza una controversia, ma dirige il procedimento di indagine ed esercita, se del caso, l'azione penale.

Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nell'art. 226, comma 1, disp. att. cod. proc. pen.), per finalità essenzialmente preventive (comma 4-*ter*).

Inoltre, le nuove disposizioni assoggettarono il *service provider* al segreto sull'ordine ricevuto, con esplicito rinvio, in caso di violazione, al reato previsto dall'art. 326 c.p. (comma 4-*quater*) e disciplinarono la procedura di convalida da parte del pubblico ministero (comma 4-*quinquies*).

Da ultimo, merita ricordare l'aggiunta, all'art. 51 cod. proc. pen., di un comma 3-*quinquies*, con il quale le indagini sui reati informatici e i reati di pornografia minorile furono devolute all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.

2.1.7. La questione delle riserve.

Nel diritto internazionale, la riserva indica la volontà dello Stato di non accettare una o più clausole di un trattato o di accettarle con alcune modifiche, oppure secondo una determinata interpretazione. Apponendo la riserva, lo Stato *limita* l'efficacia vincolante del trattato, nei rapporti con gli altri Stati contraenti, alla sola parte non investita dalla riserva[19].

La Convenzione di Budapest, all'art. 42, consente agli Stati di apporre alcune riserve al momento della firma o del deposito dello strumento di ratifica, accettazione, approvazione o adesione.

In particolare, per quel che più interessa nella prospettiva dell'ordinamento italiano, la Convenzione consente di apporre riserve in relazione:

- ad alcune ipotesi di pornografia minorile (art. 9, par. 4: ogni Parte può riservarsi il diritto di non applicare in tutto o in parte le disposizioni di cui al paragrafo 1, lettere *d* ed *e* – riguardanti le condotte di acquisizione o possesso di materiale pedopornografico – e al paragrafo 2, lettere *b* e *c*, relative alla c.d. pedopornografia "putativa", cioè alle rappresentazioni visuali di una persona che *appare* come un minore dedito ad un comportamento sessualmente esplicito, anche se in realtà è un maggiorenne);
- al requisito della doppia incriminabilità ai fini dell'assistenza per la conservazione rapida dei dati immagazzinati (art. 29, par. 4), in materia di cooperazione internazionale in relazione a violazioni diverse da quello indicate negli articoli da 2 ad 11 della Convenzione.

[19] La materia delle riserve è disciplinata dagli artt. 19-23 della Convenzione di Vienna sul diritto dei trattati, del 22 maggio 1969. L'art. 19, in particolare, dispone che le riserve sono generalmente ammesse (lo Stato può formularle al momento della firma, della ratifica, dell'accettazione, dell'approvazione di un trattato o al momento dell'adesione), a meno che: *a)* la riserva non sia vietata dal trattato; *b)* il trattato disponga che si possono fare solo determinate riserve, tra le quali non figura la riserva in questione; o *c)*, nei casi diversi dai precedenti, la riserva sia incompatibile con l'oggetto e lo scopo del trattato.

Sotto il primo profilo, va rilevato che l'art. 600-*quater*.1 cod. pen. puniva (e punisce) la pedopornografia "virtuale", avente a oggetto *immagini virtuali di minori*, ossia immagini «realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali»[20], ma non la pedopornografia "putativa", riguardante materiale pornografico che ritrae o rappresenta persone con *sembianze* di minori, come soggetti efebici o comunque di aspetto adolescenziale, ma in realtà maggiorenni[21]. Tuttavia, nonostante tale divergenza tra il diritto interno in materia di "pornografia minorile" e gli obblighi di incriminazione internazionali (che, come si è detto, impongono l'incriminazione anche della pornografia minorile "putativa"), nessuna riserva fu apposta con la legge n. 48 del 2008, o notificata al Segretariato generale della Consiglio d'Europa, ai sensi dell'art. 48 del trattato.

Ciò vale anche per il requisito della doppia incriminabilità, cui l'ordinamento interno subordina l'esecuzione dell'assistenza giudiziaria (quando non risulti che l'imputato abbia liberamente espresso il suo consenso alla domanda di assistenza giudiziaria: art. 724, comma 7, lett. *b*, cod. proc. pen.). Nonostante che, in questo caso, nella relazione al disegno di legge presentato dal Governo fosse stata segnalata la necessità di apporre una riserva in relazione all'art. 29 della Convenzione, «poiché l'art.

---

[20] Nel senso che il concetto di pedopornografia virtuale, rilevante ai fini della integrazione del reato di pornografia virtuale, di cui all'art. 600-*quater*.1 cod. pen., comprende la realizzazione di immagini senza l'impiego di bambini reali, utilizzando la tecnologia digitale per lo sviluppo di immagini tratte da soggetti reali, compresa la rappresentazione fumettistica di attività sessuali coinvolgenti bambini nel caso in cui sia di qualità tale da far apparire come accadute o realizzabili nella realtà, e quindi vere o verosimili, le situazioni non reali, cfr., da ultimo, Cass. Sez. 3 -, Sentenza n. 22579 del 18/03/2025 Ud. (dep. 16/06/2025) Rv. 288257 – 01.

In motivazione, la S. C. ricorda che «[è] stata anche richiamata da Sez. 3, n. 22265 del 13/01/2017, cit. la Convenzione sulla criminalità informatica che ha spiegato la ragione della severità con la quale deve essere perseguita ogni condotta di "pedopornografia telematica" in considerazione dell'incremento dell'uso dello scambio di files e del commercio elettronico, chiarendo il significato del termine "materiale pedopornografico" che può comprendere in alternativa: a) la rappresentazione di un abuso sessuale di un minore reale, ovvero b) l'immagine pornografica rappresentante una persona che appaia essere un minore impegnato in attività sessuali esplicite, ovvero c) le immagini che, sebbene realistiche non coinvolgono un minore realmente impegnato in attività sessuali esplicite. In tali ipotesi, prosegue Sez. 3, n. 22265 del 13/01/2017, l'interesse tutelato dalle tre situazioni è diverso: nella prima, si tratta di protezione contro l'abuso di minore; nella seconda e nella terza, il *focus* afferisce più direttamente alla protezione contro un comportamento che, seppure non abbia necessariamente offeso uno specifico minore (quello riprodotto nel materiale pedopornografico, che potrebbe anche essere "non reale") potrebbe essere usato per favorire l'abuso sui minori».

[21] Una fattispecie incriminatrice della pornografia minorile "putativa" (per le ipotesi di cessione o diffusione di materiale pornografico prodotto utilizzando persone che *sembrano* essere minori) era prevista sia nella bozza della Commissione Interministeriale, incaricata nel 2003 di redigere uno schema di legge di ratifica della Convenzione, sia nel contemporaneo disegno di legge A.C. 4599 ("Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo INTERNET"), presentato alla Camera nel corso della XIV Legislatura, il 13 gennaio 2004, dall'allora Ministra per le Pari Opportunità. La disposizione, tuttavia, scomparve nel testo definitivamente approvato all'esito *dell'iter* legislativo (sfociato nella Legge 6 febbraio 2006, n. 38) e non fu neppure ripreso nel disegno di legge di ratifica della Convenzione di Budapest presentato dal Governo nella successiva Legislatura (AC 2807 della XV Legislatura).

724, comma 4 b) c.p.p. prevede appunto il requisito della doppia incriminabilità come condizione generale per l'esecuzione delle rogatorie», nessuna riserva risulta essere stata prevista nella legge di ratifica o essere stata altrimenti apposta dallo Stato italiano all'atto del deposito dello strumento di ratifica.

Al Segretariato generale del Consiglio d'Europa sono state notificate solo due "dichiarazioni":

- la designazione del punto di contatto per gli scopi indicati nell'art. 35 (network 24/7, ossia la rete di assistenza disponibile 24 ore su 24, 7 giorni su 7), individuato nel "Servizio Polizia Postale e delle Comunicazioni" del Ministero dell'Interno.
- la designazione del Ministero della Giustizia, Dipartimento Affari di Giustizia, quale Autorità centrale, ai fini dell'art. 24, par. 7 e 27, par. 2 (in materia di estradizione e assistenza giudiziaria).

2.2. Il secondo Protocollo addizionale alla Convenzione di Budapest.

Il «*Secondo Protocollo aggiuntivo alla Convenzione sulla criminalità informatica sul rafforzamento della cooperazione e della divulgazione delle prove elettroniche"* è stato approvato dal Consiglio d'Europa il 17 novembre 2021 e aperto alla firma a Strasburgo il 12 maggio 2022. Alla data del 21 marzo 2026 risulta sottoscritto da 52 Paesi, di cui 35 membri del Consiglio d'Europa e 17 non membri[22].

I Paesi che hanno aperto la strada alla firma sono stati inizialmente 22 (Austria, Belgio, Bulgaria, Estonia, Finlandia, Islanda, Italia, Lituania, Lussemburgo, Macedonia del Nord, Montenegro, Paesi Bassi, Portogallo, Romania, Serbia, Spagna e Svezia, oltre ad altri Stati non membri quali Cile, Colombia, Giappone, Marocco e Stati Uniti). Gli stessi hanno firmato il protocollo il 12 maggio 2022, in occasione di una conferenza internazionale organizzata sotto la Presidenza Italiana del Comitato dei Ministri del Consiglio d'Europa.

L'accordo entrerà in vigore solo quando almeno cinque Paesi lo avranno ratificato. Sinora, tre soli Paesi lo hanno fatto (la Serbia, il Giappone e, da ultimo, nel febbraio del 2026, l'Ungheria).

Lo strumento addizionale mira a fornire norme comuni a livello internazionale per rafforzare la cooperazione nella lotta alla criminalità informatica e nella raccolta e "divulgazione" (*disclosure*) di prove in formato elettronico nell'ambito dei procedimenti penali. Intende, in particolare, superare alcuni limiti insiti nella Convenzione di Budapest[23], dati dalla insufficienza dei tradizionali poteri di contrasto, confinati

[22] Lo stato delle firme e delle ratifiche del secondo Protocollo aggiuntivo è disponibile sul sito del Consiglio d'Europa, al *link* https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224

[23] L'importanza della firma della Convenzione è ben rappresentata nelle parole dell'allora Ministra della Giustizia italiana, Marta Cartabia, che insieme con la Segretaria generale del Consiglio d'Europa, Marija Pejčinović Burić, aprì la Cerimonia per la firma del Protocollo addizionale a Budapest: «*l'utilizzo delle ICT (tecnologie dell'informazione e della comunicazione) da parte della criminalità organizzata in tutti i "settori" (sfruttamento sessuale, traffico di sostanze stupefacenti, contrabbando, terrorismo) rappresenta un'ulteriore sfida per*

all'interno dei territori nazionali, al fine di acquisire prove elettroniche nella disponibilità dei prestatori di servizi sottoposti a giurisdizioni straniere.

Va considerato, al riguardo, che la Convenzione di Budapest consente di estendere la cooperazione a qualsiasi misura procedurale. Con la domanda di assistenza si può richiedere la rapida conservazione dei dati presenti in un sistema informatico situato nel territorio dello Stato destinatario della richiesta (art. 29), ma anche lo svolgimento di attività di indagine (artt. 31-34). La concreta operatività di tali misure e l'instaurazione di un'utile cooperazione transnazionale, tuttavia, implica la necessità di una previa localizzazione geografica dell'informazione da acquisire. Ed è sotto questo profilo che, a causa della sempre più frequente delocalizzazione delle informazioni digitali, la Convenzione del 2001 ha mostrato la sua inadeguatezza.

I problemi hanno trovato una soluzione solo parziale nella disposizione dell'art. 32 della Convenzione, che prevede la possibilità per lo Stato parte di accedere a qualsiasi dato elettronico disponibile al pubblico *(open-source)*, ovunque esso si trovi, nonché di accedere a e/o ricevere, mediante un sistema informatico nel proprio territorio, dati situati in altro Stato parte, previo consenso della persona autorizzata a divulgarli.

Il Secondo Protocollo addizionale intende rafforzare ulteriormente, in tal senso, la cooperazione *diretta* con i prestatori di servizi privati che si trovano in altri Stati (come *internet service-provider* o società fornitrici dei servizi di telecomunicazione) e agevolare la possibilità di ottenere informazioni dettagliate su abbonati, dati di traffico e registrazione dei nomi di dominio.

Lo strumento, inoltre, fornisce la base giuridica per nuove forme di cooperazione accelerata in caso di emergenza – compreso l'uso di squadre investigative comuni e lo svolgimento di indagini congiunte – e di mutua assistenza, come l'utilizzo della videoconferenza per l'esame di testimoni o consulenti e il ricorso a indagini congiunte.

In un quadro di sintesi, le previsioni del testo convenzionale possono ricondursi alle misure di seguito indicate.

(1) Procedure volte a rafforzare la cooperazione diretta con i prestatori di servizi e i soggetti presenti nel territorio di un'altra parte (*Sezione II)*:

- Richiesta di informazioni sulla registrazione di nomi di dominio

  Art. 6.1: Ciascuna parte adotta le misure legislative e di altra natura necessarie per autorizzare le proprie autorità competenti, ai fini di indagini o procedimenti penali specifici, a inviare a un soggetto che fornisce servizi di registrazione di nomi di dominio sul territorio di un'altra parte una richiesta relativa a informazioni in suo possesso o sotto il suo controllo, allo scopo di identificare o contattare il titolare di un nome di dominio.
- Divulgazione delle informazioni relative agli abbonati

---

le nostre autorità giudiziarie e istituzioni. I nostri governi devono rispondere in modo adeguato ed efficace a tutti questi reati, in linea con l'evoluzione tecnologica. Il secondo protocollo addizionale, pertanto, risponde alla necessità di una cooperazione maggiore e più efficace tra gli Stati e tra gli Stati e il settore privato, chiarendo i casi in cui i "fornitori di servizi" potranno fornire i dati in loro possesso direttamente alle autorità competenti di altri Paesi. La pertinenza di questo Protocollo è una speranza per le vittime della criminalità informatica».

Art. 7.1: Ciascuna parte adotta le misure legislative e di altra natura necessarie per autorizzare le proprie autorità competenti a emettere un ordine da impartire direttamente a un prestatore di servizi sul territorio di un'altra parte, al fine di ottenere la divulgazione di specifiche informazioni memorizzate relative agli abbonati, in suo possesso o sotto il suo controllo, qualora tali informazioni siano necessarie ai fini di indagini o in procedimenti penali specifici della parte emittente.

(2) Procedure volte a rafforzare la cooperazione internazionale tra le autorità ai fini della divulgazione di dati informatici memorizzati (*Sezione III)*:

- Esecuzione degli ordini emessi da un'altra parte finalizzati alla presentazione accelerata di informazioni sugli abbonati e dati relativi al traffico

  Art. 8.1.: Ciascuna parte adotta le misure legislative e di altra natura necessarie per autorizzare le proprie autorità competenti a emettere un ordine da presentare nell'ambito di una richiesta rivolta a un'altra parte al fine di imporre a un prestatore di servizi sul territorio della parte richiesta di divulgare *a)* informazioni relative agli abbonati; *b)* dati relativi al traffico, specificati e memorizzati, in possesso o sotto il controllo del prestatore di servizi, necessari ai fini di indagini o in procedimenti penali specifici della parte.
- Divulgazione accelerata di dati informatici memorizzati in caso di emergenza

  Art. 9: Ciascuna parte adotta le misure legislative e di altra natura necessarie a far sì che, in caso di emergenza, il proprio punto di contatto della rete reperibile 24 ore su 24, sette giorni su sette, di cui all'articolo 35 della Convenzione («punto di contatto») possa trasmettere una richiesta di assistenza immediata al punto di contatto di un'altra parte, e possa ricevere tale richiesta da quest'ultimo, al fine di ottenere da un prestatore di servizi sul territorio di tale parte la divulgazione accelerata di specifici dati informatici memorizzati, in possesso o sotto il controllo di tale prestatore di servizi, in assenza di una richiesta di mutua assistenza giudiziaria […].

(3) Procedure relative alla mutua assistenza giudiziaria di emergenza (*Sezione IV*)

(4) Procedure relative alla cooperazione internazionale in assenza di accordi internazionali applicabili (*Sezione V)*

- Videoconferenze per l'audizione di testimoni ed esperti (art. 11)
- Squadre investigative comuni e indagini congiunte (art. 12).

2.3. Le altre convenzioni del Consiglio d'Europa.

In seno al Consiglio d'Europa sono stati elaborati anche altri strumenti di diritto internazionale per affrontare le minacce associate alla rete internet, quali:

- la Convenzione sulla prevenzione del terrorismo (2005), che contiene disposizioni penali che puniscono il reclutamento e l'addestramento di terroristi tramite internet;
- la Convenzione di Lanzarote (2007), che affronta lo sfruttamento sessuale e l'abuso di minori, anche *on-line*;

- la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, nota anche come "Convenzione 108" (1981): pur se risalente, essa rappresenta il primo trattato internazionale vincolante sulla protezione dei dati personali e ha posto le basi per lo sviluppo delle garanzie contro la raccolta e l'utilizzo illeciti di dati personali, successivamente recepite e ampliate anche nelle normative dell'Unione europea.

Di recente adozione è il terzo Protocollo addizionale alla Convenzione europea di assistenza giudiziaria in materia penale (CETS No. 227, adottata dal Comitato dei Ministri del Consiglio d'Europa il 4 giugno 2025).

Aperto alla firma nel mese di settembre 2025 a La Valletta (Malta), il nuovo protocollo mira a rafforzare la capacità degli Stati membri e degli Stati partner di rispondere efficacemente alla criminalità, in particolare in un contesto di rapidi cambiamenti politici, sociali e *tecnologici*. Tale fonte pattizia integra e aggiorna la Convenzione adottata nel 1959 e i suoi primi due Protocolli aggiuntivi.

Le principali novità includono la semplificazione e l'accelerazione delle procedure di assistenza reciproca, l'ampliamento della gamma di situazioni in cui può essere richiesta l'assistenza reciproca, l'estensione dell'uso dei canali di comunicazione elettronica e delle videoconferenze, la possibilità di utilizzare strumenti di sorveglianza tecnica come i localizzatori GPS e (con una serie di cautele) l'intercettazione delle telecomunicazioni anche nel territorio di altri Stati, nonché l'introduzione di limiti temporali per l'esecuzione delle richieste.

2.4. La normativa in ambito UE.

Le fonti rilevanti, all'interno dell'Unione europea, sono settoriali e intersecano parzialmente i contenuti della nuova Convenzione delle Nazioni Unite. Ciò non di meno, si tratta di strumenti giuridici di particolare rilievo, per vincolatività e livello di garanzie assicurate al rispetto dei diritti e delle libertà fondamentali, dai quali i Paesi membri dell'Unione non hanno potuto prescindere nel prendere posizione comune[24] nei negoziati intrapresi, in sede onusiana, con i Paesi terzi.

Fino al varo del c.d. pacchetto *e-evidence* (di cui si dirà fra più sotto), venivano in rilievo, in particolare:

- la direttiva 2013/40/EU sugli attacchi ai sistemi di informazione, che mira a contrastare tale fenomeno su larga scala, richiedendo agli Stati membri di rafforzare le leggi nazionali;[25]

[24] La DG Home della Commissione dell'Unione europea ha ricevuto mandato dal Consiglio dell'Unione europea di negoziare la Convenzione ONU sul *cybercrime* per conto dei 27 Paesi membri. La posizione comune europea è stata definita nel corso dei periodici incontri del gruppo di lavoro sulla cooperazione giudiziaria in materia penale (COPEN).

[25] A dimostrazione del rilievo "formante" che sempre più spesso le fonti unionali hanno sul diritto penale interno, è utile ricordare che, proprio per rispondere a una procedura di infrazione avviata dalla Commissione dell'Unione europea nei confronti dell'Italia, per la mancata o parziale attuazione di tale direttiva, l'art. 19 della L. 23 dicembre 2021, n. 238 (Legge europea 2019-2020) ha apportato alcune

- la direttiva 2011/93/EU contro l'abuso sessuale e lo sfruttamento dei minori e la pornografia minorile[26], che ha costituito un importante strumento di rafforzamento della tutela dei minori, anche rispetto ai nuovi e preoccupanti sviluppi del crimine nell'ambiente *online* (come per la diffusa pratica di presentarsi come minori per attirare minori a fini di abuso sessuale);[27]
- il regolamento generale per la protezione dei dati personali 2016/679 (*General Data Protection Regulation* o GDPR);
- la direttiva (UE) 2016/680 del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali;
- la direttiva 2019/713/UE, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, che vincola gli Stati membri ad adattare la disciplina interna in materia di mezzi di pagamento diversi dai contanti. Il d. lgs. 8 novembre 2021, n. 184 ha dato attuazione alla direttiva nell'ordinamento interno e ha apportato rilevanti innovazioni introducendo, tra l'altro, la nuova fattispecie incriminatrice di «*Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti*» (art. 493-*quater* cod. pen.).

Il quadro normativo si è recentemente arricchito del c.d. pacchetto *e-evidence*[28], contenente nuove norme per accelerare l'accesso ai dati digitali utilizzati per le indagini

---

significative integrazioni e modifiche a diverse disposizioni incriminatrici del codice penale in materia di: *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici* (art. 615-*quater*); *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico* (art. 615-*quinquies*); *Cognizione, interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche* (art. 617); *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche* (art. 617-*bis*); *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche* (art. 617-*quater*); *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche* (art. 617-*quinquies*).

[26] La direttiva si è rivelata utile nei negoziati per l'elaborazione della nuova Convenzione delle Nazioni Unite, in quanto fornisce ai Paesi membri dell'Unione europea un'importante base giuridica nell'individuazione di una posizione comune per la soluzione delle questioni emerse in ordine all'estensione degli obblighi di incriminazione in caso di materiale auto-prodotto dai minorenni stessi.

[27] Anche in questo caso, per rispondere a una procedura di infrazione avviata dalla Commissione dell'Unione europea nei confronti dell'Italia, per la mancata o parziale attuazione di tale direttiva, è dovuta intervenire la già citata L. 238/2021, con l'art. 20, che ha apportato alcune integrazioni e modifiche ad alcuni articoli del codice penale in materia di abuso sui minori e pedopornografia, tra le quali l'innesto nell'art. 600-*quater* della nuova fattispecie di accesso intenzionale e senza giustificato motivo, mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione, a materiale pornografico realizzato utilizzando minori degli anni diciotto.

[28] Le prove elettroniche (*e-evidence*) consistono in dati digitali utilizzati per lo svolgimento delle indagini e l'acquisizione della prova dei reati. Includono, tra l'altro: e-mail, SMS o contenuti provenienti dalle applicazioni di messaggistica, contenuti audiovisivi, informazioni sull'account *online* degli utenti. S^per una panoramica sull'*e-evidence package* di recente attuazione, v. C. DE LAZZARO, *L'acquisizione delle prove elettroniche nello spazio di libertà, sicurezza e giustizia: una prima implementazione dell'e-evidence package*, in *Sist.*

e l'accertamento dei reati, indipendentemente dall'ubicazione dei dati e della sede principale (in Paesi terzi) dei *service-provider* che operino nell'ambito dell'Unione europea.

È noto, infatti, che l'accesso alle prove elettroniche può rivelarsi un processo lungo e complicato, perché i prestatori di servizi *online* conservano i dati degli utenti in *server* situati anche in diversi Paesi, sia all'interno che all'esterno dell'Unione europea. Per superarte le difficoltà operative, sono stati adottati due nuovi strumenti unionali.

Il primo è il regolamento (UE) 2023/1543 relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali (applicabile a partire dal 18 agosto 2026) volto a:

- consentire alle autorità giudiziarie nazionali coinvolte in procedimenti penali di ordinare ai prestatori di servizi che offrono servizi nell'Unione europea[29] di produrre o conservare prove elettroniche ovunque siano localizzati i dati;
- agevolare e velocizzare l'accesso transfrontaliero alle prove elettroniche ed evitarne la cancellazione, garantendo al contempo garanzie giuridiche alle persone i cui dati sono stati richiesti.

Per adeguare l'ordinamento interno al regolamento, il decreto legislativo 30 dicembre 2025, n. 215 ha individuato nel Ministero dell'interno (e segnatamente nell'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155) l'autorità centrale alla quale notificare la designazione dello stabilimento designato o la nomina del rappresentante legale ai fini dell'acquisizione della *e-evidence* nei procedimenti penali.

Il secondo stgrumento è la direttiva (UE) 2023/1544 recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali.

La direttiva – recentemente recepita nell'ordinamento interno, con il decreto legislativo 30 dicembre 2025, n. 216 - è volta ad assicurare che i *service provider* che offrono servizi nell'Unione dispongano di stabilimenti designati o rappresentanti legali nominati nell'Unione stessa, in modo da poter ricevere e ottemperare agli ordini delle autorità nazionali al fine di raccogliere prove elettroniche nell'ambito dei procedimenti penali.

2.5. Le Convenzioni ONU.

Nel contesto delle Nazioni Unite, tra le convenzioni in vigore viene innanzi tutto in rilievo, per duttilità di impiego e numero di adesioni, la Convenzione contro il crimine

---

Pen., 2 febbraio 2026.

[29] Il regolamento (UE) 2023/1543 si applica ai prestatori di servizi che forniscono una o più delle seguenti categorie di servizi nell'Unione: servizi di comunicazioni elettroniche; nomi di dominio Internet e numerazione IP; servizi di comunicazione, archiviazione e trattamento.

organizzato transnazionale, firmata a Palermo nel 2000 (detta anche "Convenzione di Palermo" o UNTOC, acronimo della denominazione inglese *United Nations Convention against Transnational Organized Crime*).

Il trattato costituisce il principale strumento internazionale di riferimento contro tutte le forme di criminalità, giovandosi di una vastissima base di consenso (attualmente conta 194 Parti, a fronte di 193 Stati membri delle Nazioni Unite. Dopo la ratifica della Repubblica islamica dell'Iran, nell'agosto del 2025, soltanto il Congo, fra i firmatari, non l'ha ancora ratificata[30].

La Convenzione contiene norme innovative in materia di indagini, sorveglianza elettronica, cooperazione giudiziaria e responsabilità da reato degli enti, con disposizioni applicabili anche ai fornitori e intermediari dei servizi internet. Si caratterizza, inoltre, per l'ampia nozione di "reato grave di natura transnazionale" e di "gruppo organizzato".

Proprio questa notevole ampiezza e flessibilità dell'ambito applicativo della Convenzione di Palermo ne ha consentito l'utilizzo anche nel contrasto delle emergenti forme di criminalità informatica, supplendo alla più limitata adesione registrata dalla Convenzione di Budapest[31].

Nel corso dei negoziati per la costruzione della nuova Convenzione ONU sul *cybercrime,* hanno costituito un fertile terreno dal quale attingere nozioni e principi condivisi anche *altre* Convenzioni delle Nazioni Unite, quali:

- le Convenzioni in materia di diritti umani o sui diritti dell'infanzia (*International Covenant on Civil and Political Rights* del 1966 e *Convention on the Rights of the Child - CRC* del 1989, con il Protocollo opzionale alla Convenzione, riguardante la vendita di bambini, la prostituzione dei bambini e la pornografia rappresentante bambini), che hanno fornito un'importante leva per estendere anche ai negoziati per la nuova Convenzione ONU sul *cybercrime* un forte e incondizionato richiamo alla necessità del rispetto dei diritti umani e per fornire utili indicazioni sul superamento delle divisioni fra gli Stati in materia di sfruttamento o abuso di minori e di età del consenso;
- la Convenzione delle Nazioni Unite contro la corruzione, firmata a Mérida nel 2003 (Convenzione di Mérida o UNCAC, *United Nations Convention against Corruption*): convenzione che, anche per la vasta platea di Paesi che ne sono parte, (192, su 193 delle Nazioni unite) insieme alla Convenzione di Palermo si è rivelata di grande utilità per la ricerca di soluzioni condivise durante i nuovi negoziati sul *cybercrime,* specie in materia di condizioni e salvaguardie ("*conditions and safeguards*"), di delimitazione dell'ambito applicativo delle nuove disposizioni, di formulazione delle regole sulla giurisdizione e per una migliore e coerente messa a fuoco di fattispecie quali il riciclaggio.

---

[30] Lo stato delle ratifiche è reperibile sul sito delle Nazioni unite, al link https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en

[31] Cfr. l'accurato contributo di. A. MATTARELLA *La futura convenzione ONU sul* cybercrime *e il contrasto alle nuove forme di criminalità informatica*, in *Sist. pen.*, fasc. 3, 2022, p. 41 e ss..

Alle disposizioni delle convenzioni UNTOC e UNCAC, inoltre, il Comitato *ad hoc* per l'elaborazione della nuova Convenzione ONU sulla criminalità informatica ha ampiamente attinto per le proposte in materia di cooperazione giudiziaria (*MLA – Mutual Legal Assistance)* e di recupero e confisca dei profitti illeciti (il c.d. *asset recovery).*

3. La nuova Convenzione ONU contro il crimine informatico.

Ultima (in ordine di tempo) e significativa tappa del processo di internazionalizzazione del contrasto penale alla criminalità informatica è, a livello globale, la Convenzione delle Nazioni unite contro il crimine informatico, adottata dall'Assemblea Generale delle Nazioni Unite il 24 dicembre 2024, aperta alla firma nell'autunno del 2025.

Prima di tratteggiarne i contenuti essenziali, sembra utile ripercorrere il lungo e tortuoso cammino che ha portato alla sua adozione, nel corso di anni di negoziati e confronti diplomatici. Si esamineranno, quindi, la struttura e i nodi più problematici della Convenzione, confrontandone i contenuti con quelli della Convenzione di Budapest.

3.1. I lavori preparatori e lo stato di avanzamento della Convenzione.

Il progetto per la costruzione di una convenzione delle Nazioni Unite in materia di criminalità informatica affonda le sue radici nello scorso decennio[32].

Già durante il 12° Congresso delle Nazioni Unite sulla Prevenzione della criminalità e la Giustizia penale, tenutosi in Brasile nel 2010, alcuni Paesi, tra i quali la Russia, avevano proposto un nuovo trattato sulla criminalità informatica all'interno del sistema delle Nazioni Unite.

A seguito dell'iniziativa, era stato creato un gruppo intergovernativo di esperti (IEG) per condurre uno studio completo sulla criminalità informatica. Il gruppo operò fino al 2021 nell'ambito della Commissione delle Nazioni Unite per la Prevenzione della Criminalità e la Giustizia Penale (CCPCJ).

---

[32] Per un'introduzione al progetto di nuova Convenzione delle Nazioni Unite e un'accurata analisi del contesto generale di riferimento si rinvia a A. MATTARELLA *La futura convenzione ONU sul* cybercrime *e il contrasto alle nuove forme di criminalità informatica,* cit. p. 41 e ss. Un'analisi più recente delle diverse posizioni in campo, con ampio corredo di richiami, è fornita da I. TENNANT, *Endgames. The final phase of the cybercrime negotiotions?* GI-TOC, January 2024, pp 2 e ss., in https://globalinitiative.net/analysis/united-nations-cybercrime-negotiations-final-phase/. Per gli ultimi sviluppi e l'esito del negoziato si rinvia a S. WALKER-A.P. OLIVEIRA, *The final call UN member states adopt a new cybercrime-treaty*, GI-TOC, September 2024, in *https://globalinitiative.net/analysis/the-final-call-un-member-states-adopt-a-new-cybercrime-treaty/*
Sul testo approvato dall'Assemblea generale delle Nazioni Unite, da ultimo, A. BALSAMO, *Spazio virtuale e processo penale: la nuova Convenzione ONU sul cybercrime,* in *Dir. pen. e proc.*, 2/2025, p. 240 ss., nonché A. MATTARELLA, *Diritto penale e nuove tecnologie: dalla Convenzione Onu contro i reati informatici alle sfide dell'intelligenza artificiale*, *ivi,* p. 250 e ss.

Nel 2017, la Russia presentò nuovamente al Segretario generale delle Nazioni Unite una bozza di convenzione sulla criminalità informatica, anche per conto di altri Paesi (Bielorussia, Cambogia, Cina, Repubblica democratica popolare della Corea, Myanmar, Nicaragua e Venezuela), dal titolo "*Countering the use of information and communications technologies for criminal purposes*". In contrasto con i Paesi "occidentali", la Russia non riteneva la Convenzione di Budapest in linea con le proprie esigenze e insisteva per l'adozione di una Convenzione universale che coprisse non solo il *cybercrime* in senso stretto, ma, più in generale, l'utilizzo delle nuove tecnologie dell'informazione e della comunicazione a scopi criminali.

Il progetto assunse concretezza con la Risoluzione n. 74/247 dell'Assemblea Generale delle Nazioni Unite, adottata il 27 dicembre 2019, intitolata «Lotta all'uso delle tecnologie dell'informazione e della comunicazione a fini criminali» («*Countering the use of information and communications technologies for criminal purposes*»), istitutiva di un Comitato intergovernativo di esperti (Comitato *ad hoc*), rappresentativo di tutti i Paesi, per elaborare una Convenzione globale sul contrasto all'uso delle tecnologie dell'informazione e della comunicazione per scopi criminali.

Rinviati a causa della pandemia, i lavori del Comitato *ad hoc* furono oggetto di una successiva risoluzione dell'Assemblea generale (n. 75/282, anche questa intitolata: «Lotta all'uso delle tecnologie dell'informazione e della comunicazione a fini criminali»), con la quale fu deciso, tra l'altro, che il Comitato *ad hoc* convocasse almeno sei sessioni, di 10 giorni ciascuna, seguite da una sessione conclusiva a New York, al fine di elaborare una bozza di convenzione da sottoporre all'Assemblea Generale nel corso della sua settantottesima sessione; fu inoltre deciso che il Comitato tenesse la prima, terza e sesta sessione negoziale a New York e la seconda, quarta e quinta sessione a Vienna.

Alla sessione organizzativa del 10-12 maggio 2021, a New York, il Comitato elesse quale proprio presidente la rappresentante dell'Algeria, ambasciatrice Faouzia Boumaiza Mebarki.

A distanza di oltre quattro anni dal suo insediamento, dopo due sessioni organizzative, otto sessioni negoziali e cinque consultazioni intersessionali con la società civile (oltre a numerose consultazioni informali), il Comitato *ad hoc* – all'esito dell'ultima sessione negoziale, svoltasi a New York dal 29 luglio al 9 agosto 2024 – ha portato a termine il suo compito, adottando una bozza di Convenzione dal titolo "*Draft United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*". Unitamente alla Convenzione, il Comitato *ad hoc* ha approvato la bozza di Risoluzione alla quale è stata allegata per l'approvazione la Convenzione stessa e le Note interpretative su specifici articoli[33].

Nonostante il voto contrario della maggioranza dei Paesi presenti su sette richieste di emendamento al testo da parte della Repubblica Islamica dell'Iran, il

[33] I lavori preparatori sono reperibili alla pagina *web* del Comitato *Ad Hoc*: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_reconvened_concluding_session/main.

Comitato ha adottato all'unanimità i testi finali della Convenzione, la Risoluzione e le Note interpretative.[34]

Gli atti sono quindi passati all'esame dell'Assemblea Generale delle Nazioni Unite, che il 24 dicembre 2024, a New York, con la risoluzione n. 79/243 ha adottato la Convenzione delle Nazioni Unite contro il crimine informatico *(United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*).

La Convenzione è stata aperta alla firma ad Hanoi (Vietnam), il 25 ottobre 2025. Esaurita la cerimonia inaugurale, durante la quale è stata acquisita la sottoscrizione di 72 partecipanti, le firme continuano tuttora ad essere raccolte presso il quartiere generale delle Nazioni Unite a New York, ove il trattato continuerà ad essere aperto alla firma fino al 31 dicembre 2026.

Alla data del 21 marzo 2026, sono state acquisite 75 firme. Tra i firmatari, solo uno (il Qatar) ha anche ratificato la Convenzione.[35] Seguirà la fase delle ratifiche o delle accessioni degli Stati.

L'entrata in vigore è prevista il novantesimo giorno successivo al raggiungimento della soglia di quaranta ratifiche, accettazioni, approvazioni o accessioni al trattato.

3.2. L'esito dei lavori: una valutazione complessiva.

L'adozione della Convenzione da parte dell'Assemblea generale delle Nazioni unite, nel dicembre 2024, è il punto di arrivo di un lungo e travagliato percorso negoziale, con il conseguimento di un risultato niente affatto scontato, considerata la distanza di approccio e di obiettivi dei principali protagonisti del negoziato.

---

[34] Le regole di funzionamento del Comitato *ad Hoc* sono state stabilite con la Risoluzione n. 75/282 dell'Assemblea Generale delle Nazioni Unite, adottata il 26 maggio 2021, e prevedono che le decisioni sulle questioni di merito, se non adottate "*by consensus*" (ossia all'unanimità), devono essere sostenute dalla maggioranza di almeno i 2/3 dei rappresentanti dei Paesi presenti e votanti. Il *report* della sessione conclusiva è reperibile al link: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Documents/A_78_986-A_AC.291_28_Advance_120924.pdf. Nello stesso si dà atto che, dopo la votazione sui singoli emendamenti, il testo finale della Convenzione è stato approvato all'unanimità, senza necessità di ricorrere al voto.

[35] Il testo della Convenzione e tutte le informazioni relative ad essa sono reperibili al *link* https://www.unodc.org/unodc/cybercrime/convention/home.html. Dal sito risulta che tra i firmatari figurano 13 Paesi dell'Unione europea: Austria, Belgio, Repubblica Ceca, Francia, Grecia, Irlanda, Lussemburgo, Polonia, Portogallo, Slovacchia, Slovenia, Spagna, Svezia, oltre alla stessa Unione europea. L'Italia, ad oggi, non risulta avere firmato il trattato. La lista aggiornata delle firme e delle ratifiche è reperibile al link https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en

Si aprono ora nuovi scenari per la cooperazione giudiziaria internazionale, essendosi compiuto un passaggio di grande rilievo, sul piano giuridico e politico.

La Convenzione sarà il primo strumento giuridicamente vincolante in materia di criminalità informatica elaborato in seno alle Nazioni Unite e, quindi, a vocazione universale; per alcuni aspetti, inoltre, essa è più aggiornata della Convenzione del Consiglio d'Europa del 2001 (c.d. Convenzione di Budapest). Al tempo stesso, la Convenzione costituisce uno strumento che segna la difficile sintesi, probabilmente la migliore concretamente realizzabile nel contesto geopolitico attuale, tra le diverse visioni che hanno diviso i negoziatori nel corso degli anni. Essa rappresenta un bilanciamento equilibrato tra le seguenti fondamentali esigenze in gioco:

- dotare gli Stati di uno strumentario che consenta, a livello nazionale e internazionale, un'efficace attività di prevenzione e contrasto della criminalità informatica, abilitandoli all'utilizzo delle più avanzate e penetranti tecniche investigative e rafforzando la cooperazione internazionale;
- assicurare, al contempo, il rispetto dei diritti umani e delle libertà fondamentali, impedendo che i poteri assegnati agli Stati siano utilizzati strumentalmente, con finalità discriminatorie o repressive del dissenso politico, della libertà di manifestazione del pensiero, di ricerca scientifica, di impresa e delle altre libertà fondamentali.

La partita, sul piano politico, si è sempre giocata intorno alla ricerca di un punto di equilibrio tra questi due poli, che attingono, a ben vedere, alle diverse concezioni del rapporto tra il singolo e lo Stato, tra i diritti individuali e diritti collettivi[36]:

- da un lato, la tutela della collettività e della sicurezza della società, assunta dai Paesi più autoritari (se non propriamente illiberali) a giustificazione della concessione dei più ampi e penetranti poteri alle autorità pubbliche per finalità di prevenzione e repressione dei reati, anche a scapito dei diritti e delle libertà individuali;

---

[36] Accade spesso, in ambito 'onusiano', che a quanti invocano il rispetto dei diritti umani si contrappongono Stati che enfatizzano la necessità di rispettare non solo i diritti umani "individuali" (quali, tradizionalmente, i diritti civili e politici o i diritti sociali, economici e culturali dei singoli), ma anche i diritti "collettivi" di società o popoli (come il diritto allo sviluppo sostenibile, alla pace o a un ambiente sano). Quella dei diritti umani "collettivi" è una categoria non universalmente accettata, emersa negli anni '70 dello scorso secolo e applicata, ad esempio, per l'affermazione dei diritti delle popolazioni indigene nella *Human and Peoples' Rights and the Declaration on the Rights of Indigenous Peoples*. La stessa Dichiarazione Universale dei Diritti Umani include il diritto all'autodeterminazione e un diritto umano allo sviluppo è stato "codificato" nella 1986 *UN General Assembly Declaration*. Il timore è che tale assimilazione concettuale, trapiantata in altri contesti, possa essere utilizzata strumentalmente da alcuni regimi repressivi per giustificare la negazione di diritti umani (individuali) in nome di quelli collettivi: per esempio, limitando in diversi modi i diritti civili al fine di assicurare lo "sviluppo economico" del Paese.
Sul tema, v. A. BADGER, *Collective v. individual human rights in membership governance for indigenous peoples, in* https://www.corteidh.or.cr/tablas/r29305.pdf. La *UN Declarations on the Rights of Indigenous people* (UN Re. 13.6.2007) è reperibile all'indirizzo: https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf.
Per un rapido sguardo sulla evoluzione dei diritti umani, v. *L'evoluzione dei diritti umani* in COMPASS, ed. 2012, cap. IV in https://www.coe.int/it/web/compass/the-evolution-of-human-rights

- dall'altro, la necessità di mantenere l'esercizio dei poteri pubblici nel perimetro rigoroso della *rule of law*, sottoponendolo a regole certe e a controlli indipendenti che impediscano abusi e arbitri, imponendo il rispetto dei diritti umani e dei diritti processuali delle parti, garantendo un trattamento uguale e non discriminatorio di tutte le persone.

Il compito del Comitato *ad hoc*, in tale contesto, si è rivelato molto difficile:

- per l'ampiezza del progetto convenzionale, che spazia dal diritto sostanziale (incriminazioni) al diritto processuale (misure procedurali); dalla cooperazione internazionale alla prevenzione, sino all'assistenza tecnica e agli scambi informativi;
- per la difficoltà dei profili tecnici coinvolti, che incidono su materie molto divisive (talvolta, come per i reati in materia di abuso sui minori, fortemente condizionate da impostazioni etico-religiose irrinunciabili per taluni Paesi confessionali e, tuttavia, totalmente inconciliabili con gli ordinamenti di altri Paesi, specialmente quelli europei e *like-minded*), sulle quali era necessario muoversi con accortezza, per evitare risultati incompatibili con gli assetti ordinamentali interni: esigenza particolarmente sentita dai Paesi membri dell'Unione europea, che dovevano (e devono) tener conto della cornice giuridica unionale, ma anche per i Paesi membri del Consiglio d'Europa, che devono evitare frizioni con la Convenzione di Budapest e, ad alcuni effetti, con la Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e gli abusi sessuali (c.d. Convenzione di Lanzarote);
- per la polarizzazione del dibattito su molte materie sensibili, quali il rispetto dei diritti umani e delle libertà fondamentali, nel contesto della contrapposizione tra il blocco dei Paesi occidentali e alcuni altri Paesi (in particolare Russia e Iran) che ha fortemente risentito di un quadro politico deterioratosi all'immediata vigilia dell'avvio del processo negoziale, a causa dei conflitti in Ucraina e in Medio-Oriente.

Per quanto complesso e ambizioso, si è trattato di un compito necessario da svolgere, per un duplice ordine di ragioni.

Sul piano politico, l'aver portato a termine un negoziato così complesso, in una stagione storica segnata dalla riapertura di tragici conflitti e da una rinnovata polarizzazione, restituisce una *barlume di fiducia nel multilateralismo:* nonostante i segni evidenti del compromesso che reca in sé il testo finale della Convenzione, e forse proprio *grazie* a quella capacità di compromesso che ne ha reso possibile l'approvazione, il risultato raggiunto è la conferma della forza del dialogo in un mondo diviso.

Sul piano giuridico, il trattato fornisce opportunità straordinarie, se ben coltivate, di armonizzazione degli ordinamenti e di cooperazione a livello globale, rispondendo a un bisogno da tempo avvertito dagli investigatori, segnalato dalla comunità scientifica e ampiamente dibattuto negli stessi fori onusiani[37].

---

[37] *Ex aliis*, G. MELILLO, *Prolusione del P.N.A. per il trentennale della istituzione del servizio centrale di investigazione sulla criminalità organizzata*, in *Sistema penale*, 13.9.2024, p. 2: «La realtà ci mostra ogni giorno che le nuove tecnologie sono sempre più un moltiplicatore della pericolosità delle reti criminali, determinando profondi

3.3. I nodi più critici del negoziato.

Su alcuni punti cruciali del testo negoziale (quali l'ambito di applicazione della Convenzione, le incriminazioni, le condizioni e le salvaguardie cui subordinare la cooperazione internazionale) le posizioni dei diversi Paesi sono sempre state molto distanti, difficilissime da conciliare.

Uno dei motivi di maggiore tensione, durante i negoziati, è stata la tendenza, specialmente da parte di alcuni Paesi con tradizioni giuridiche e culturali diverse da quelle dei Paesi del *Group of Western European and Other States* (anche noto come *Western European and Other States Group* o WEOG[38]), a estendere il novero delle incriminazioni (e della cooperazione internazionale) oltre il limitato ambito dei *cyber-dependent crimes* e di pochi altri, selezionati *cyber-enabled crimes*.

Da parte di molti Paesi, infatti, vi è sempre stata una fortissima insistenza per includere nello *scope of application* numerosi altri reati, alcuni dei quali legati al "contenuto" delle comunicazioni digitali (discriminazione, razzismo e xenofobia, terrorismo, riabilitazione e giustificazione del genocidio o di altri crimini contro la pace

---

cambiamenti degli scenari investigativi, sui quali ormai si stagliano anche i delicatissimi problemi correlati all'impiego a fini criminosi dell'intelligenza artificiale.

L'era digitale vede dunque realizzarsi rapide trasformazioni della struttura e dello stesso codice genetico dei gruppi criminali» e p. 4: «Nonostante il tempo della guerra e le logiche della polarizzazione restringano inevitabilmente lo spazio della cooperazione fra gli Stati, non vi è alternativa al riconoscere che la cooperazione internazionale è l'unica strada praticabile per contrastare efficacemente fenomeni criminali transnazionali retti di logiche e ruoli di governo che rischiano di risultare indecifrabili se considerati negli angusti limiti delle giurisdizioni nazionali e nello stesso tempo per riconoscere che la cooperazione è possibile soltanto all'interno del perimetro dello Stato di diritto.»

V. anche le segnalazioni di EUROPOL, nei suoi report annuali IOCTA ("*Internet Organised Crime Threat Assessment*"), reperibili al *link* https://www.europol.europa.eu/publications-events/main-reports/iocta-report.

Già nel *report* annuale del 2017, «*Serious Organised Crime Threat Assessment*» (SOCTA), dedicato al "*Crime in the Age of Technology*", Europol segnalava: «*Criminals quickly adopt and integrate new technologies into their modi operandi or build brand-new business models around them. The use of new technologies by OCGs has an impact on criminal activities across the spectrum of serious and organised crime. This includes developments online, such as the expansion of online trade and widespread availability of encrypted communication channels, as well as other aspects of technological innovation such as more accessible and cheaper highperformance drone technology. Technology has a fundamental and lasting impact on the nature of crime*."

Innumerevoli gli allarmi anche in ambito ONU, in cui il contrasto al *cybercrime* rientra, tra l'altro, negli obiettivi di sviluppo sostenibile concordati dai 193 Membri delle Nazioni Unite nell'Agenda 2030 (SDG 16 e 17). Per la promozione della capacità degli Stati (*capacity-building*) nel contrasto al *cybercrime* lavorano anche gli speciali programmi di UNODC (l'Ufficio delle Nazioni Unite per il contrasto alla droga e al crimine).

[38] Il *Western European and Other States Group* (o WEOG) è uno dei cinque gruppi regionali delle Nazioni Unite, composto da 28 Stati membri, per lo più dell'Europa occidentale, ma anche Oceania, Nord America e Asia occidentale; gli altri quattro gruppi sono: *Latin American and Caribbean Group; African Group, Eastern European Group, Asia* e il *Pacific Group*. A questi si aggiungono il Kiribati, che è membro delle NU non compreso in alcun gruppo regionale e gli Stati "osservatori", ossia la Santa sede e la Palestina.

e l'umanità), con il rischio di uno slittamento verso spazi di incriminazione che avrebbero potuto offrire la base giuridica per un utilizzo strumentale della Convenzione, volto a reprimere diritti e libertà fondamentali, quale la libertà di manifestazione del pensiero.

Tutto ciò, peraltro, con deboli salvaguardie procedurali e di rispetto dei diritti umani. Alcuni Paesi addirittura si opponevano in maniera intransigente a ogni riferimento esplicito alla salvaguardia dei diritti umani. Altri sembravano avere come obiettivo principale l'inclusione del maggior numero possibile di fattispecie di reato, mostrando un minore interesse per gli aspetti di cooperazione internazionale.

In tale quadro composito – come è ovvio che sia, in un contesto geo-politico frastagliato – i Paesi "*like-minded*" del gruppo occidentale (Paesi europei, ma anche USA, Canada, Giappone e Australia), aderenti alla Convenzione di Budapest, tendevano a rimanere quanto più allineati possibile all'impianto adottato in seno al Consiglio d'Europa, sia con riferimento all'ambito applicativo della nuova convenzione, sia con riferimento al "linguaggio" del testo da adottare. La posizione comune, in tal senso, tendeva a circoscrivere gli obblighi di incriminazione ai soli reati c.d. *cyber-dependent*, ovvero a quelli che possono essere commessi unicamente attraverso l'uso di tecnologie informatiche, con l'inclusione di pochi reati c.d. *cyber-enabled*, ovvero quelli che possono essere commessi anche al di fuori del cyberspazio e senza il ricorso a tecnologia informatica, ma che con l'utilizzo di tale tecnologia diventano significativamente insidiosi, per diffusività, capacità offensiva e per l'attitudine ad assicurare l'anonimato dell'autore.

Un capitolo a se stante, in questa divaricazione di vedute, è rappresentato dai reati di sfruttamento o abuso di minori *on-line* (la terminologia onusiana tende ad affrancarsi dal tradizionale linguaggio delle convenzioni esistenti, che fanno riferimento a pedopornografia *on-line*, e preferisce utilizzare la formula di *child sexual abuse and exploitation material*, c.d. CSAM). Pur a fronte di un unanime consenso rispetto all'inclusione di tali reati nell'ambito di applicazione della Convenzione, molto distanti si sono rivelate le posizioni dei negoziatori sulla definizione dei *contenuti* delle incriminazioni, in una contrapposizione fortemente segnata, per alcuni Stati, da pregiudiziali politiche, culturali e religiose e, per altri Stati, dall'esigenza di adottare formulazioni delle clausole convenzionali che fossero compatibili con gli assetti normativi nazionali e sovranazionali, coerenti – in particolare – con le Convenzioni di Budapest e di Lanzarote e (per gli Stati dell'Unione europea) con la direttiva 2011/93/UE.

Riguardo alle misure procedurali e di cooperazione internazionale, poi, era trasversale nei Paesi del WEOG la volontà di mantenere le stringenti clausole di salvaguardia (inclusa la garanzia del rispetto dei principi della CEDU) previste dalla Convenzione di Budapest per i mezzi di indagine e per lo scambio di informazioni particolarmente avanzate ed invasive.

All'interno del "blocco" occidentale, tuttavia, esistevano differenze di vedute sulla lista dei reati da includere nel capitolo sulla criminalizzazione, con l'Unione europea in posizione molto conservativa, e USA, Canada, Regno Unito, Australia e Nuova Zelanda più aperti, almeno su alcune fattispecie (quali, ad esempio, la diffusione non consensuale di immagini intime o la violazione del diritto d'autore).

Si è rivelato molto problematico, poi, il nodo della protezione dei dati personali e del c.d. *data-retention*, con posizioni divergenti tra gli USA e i Paesi dell'Unione europea, vincolati dalla stringente normativa dell'Unione europea in materia.

Arduo, divisivo, e sottoposto a numerose consultazioni informali all'interno di appositi gruppi di "co-facilitazione" è stato anche il delicato profilo delle misure procedurali più intrusive, quali la raccolta in tempo reale dei dati relativi al traffico informatico (*real time collection of traffic data*) e l'intercettazione dei dati relativi al contenuto di comunicazioni effettuate attraverso un sistema informatico (*interception of content data*). Su tale fronte si sono contrapposte la posizione di iniziale chiusura dei Paesi dell'Unione europea – che avrebbero voluto escludere tali misure dal trattato (posizione alla quale, agli esordi del negoziato, si erano associati la Norvegia, Singapore, la Svizzera e il Liechtenstein) – e la volontà di quanti, all'opposto, ne chiedevano l'inclusione, pur con diverse formulazioni e subordinatamente a particolari condizioni e salvaguardie (Iran, Brasile, Australia, USA, Russia, Egitto, Nigeria, Nuova Zelanda, Trinidad e Tobago per conto del CARICOM – ossia dei 14 Paesi della Comunità Caraibica –, Eritrea, Algeria, Colombia, Cina, Pakistan, Namibia, Venezuela, Cile, Argentina, Indonesia, India, Tailandia, Perù, Filippine, Regno Unito, Kenya).

3.4. Struttura e contenuto della Convenzione delle Nazioni Unite: una visione d'insieme.

La struttura della Convenzione e la formulazione di gran parte delle sue disposizioni attingono in larga parte ad altri strumenti di diritto internazionale vincolanti (in particolare, come già si è detto, la UNTOC, la UNCAC e la Convenzione di Budapest).

Analogamente a quei modelli, la nuova Convenzione ONU si articola in separati capitoli, dedicati a: Disposizioni generali (I); Incriminazioni (II); Giurisdizione (III); Misure procedurali e di polizia (IV); Cooperazione internazionale (V); Misure di prevenzione (VI); Assistenza tecnica e scambio di informazioni (VII); Meccanismo di attuazione (VIII); Disposizioni finali (IX).

In una sintetica visione d'insieme (a fronte di un trattato di ben nove capitoli e sessantotto articoli), può rilevarsi che il nuovo strumento pattizio, allo scopo di promuovere e rafforzare la prevenzione e il contrasto della criminalità informatica (art. 1), si muove lungo sei direttrici fondamentali:

1. sul piano del diritto sostanziale, impone l'obbligo di incriminazione di alcune specifiche condotte (Cap. II), sostanzialmente riconducibili ai tipici e più diffusi reati "*cyber-dependent*", ovvero quei reati strettamente dipendenti dal mezzo informatico (accesso illegale, intercettazione illegale, interferenza con dati elettronici, interferenza con un sistema informatico, uso improprio di dispositivi), cui si aggiungono limitate ipotesi di reati "*cyber-enabled* "o "*cyber-related*", scelti tra quelli di maggiore gravità e diffusività (furto e frode informatica; reati connessi all'abuso o allo sfruttamento sessuale o all'adescamento di minori attraverso il sistema informatico; diffusione non consensuale di immagini intime; riciclaggio). In tal modo, la Convenzione

costruisce un nucleo di armonizzazione delle fattispecie penali, funzionale al contrasto più efficace della criminalità informatica "domestica" e globale e alla concreta realizzazione della cooperazione internazionale (che presuppone, il più delle volte, la doppia incriminazione). Inoltre, in relazione alle fattispecie di reato "armonizzate", la Convenzione prevede l'obbligo dell'istituzione della responsabilità (penale, civile o amministrativa) delle persone giuridiche;

2. sul piano degli strumenti procedurali, impone l'obbligo di adozione di una serie di misure processuali e di polizia, per lo svolgimento di specifiche indagini e procedimenti penali aventi a oggetto i reati previsti dalla Convenzione, nonché altri reati commessi attraverso i sistemi tecnologici di informazione e comunicazione e altresì per la raccolta delle prove elettroniche di qualsiasi reato (Cap. IV). L'intervento mira ad armonizzare, anche in ambito processuale, gli ordinamenti interni, grazie alla previsione di un ampio spettro di misure: da quelle classiche e meno invasive (quali la conservazione e l'esibizione rapida di dati archiviati, gli ordini di produzione, le perquisizioni e i sequestri di dati archiviati) a quelle più intrusive (quali la raccolta in tempo reale di dati di traffico e l'intercettazione di dati relativi al contenuto di comunicazioni). In questo modo, il trattato prosegue sulla strada inaugurata da altre grandi convenzioni in materia penale, al chiaro fine di consentire l'efficace azione di contrasto dei reati "domestici" , al tempo stesso funzionale al potenziamento della cooperazione internazionale;
3. sul piano della cooperazione internazionale (Cap. V), disegna una politica condivisa che non si limita ai tradizionali strumenti di cooperazione giudiziale (estradizione, trasferimento di persone condannate e di procedimenti penali, reciproca assistenza giudiziaria), ma si estende a nuove forme più idonee a fronteggiare la rapidità e la diffusività delle condotte dei *cyber*-criminali; come la cooperazione rapida in caso di emergenza, la collaborazione diretta tra forze di polizie e le indagini congiunte (peraltro già previste anch'esse nella Convenzione di Budapest). L'obbligo di cooperazione internazionale, in relazione alla raccolta, conservazione e condivisione di *e-evidence* di reati *diversi* da quelli oggetto di armonizzazione riguarda, tuttavia, i soli reati "gravi";
4. sul piano della prevenzione (Cap.VI), promuove l'adozione di un robusto e articolato apparato di misure preventive, con il coinvolgimento attivo della società civile e degli imprenditori privati del settore, prestando una particolare attenzione ai soggetti vulnerabili;
5. completa, poi, la cornice di collaborazione a livello internazionale con la previsione di misure di assistenza tecnica e scambio informativo tra gli Stati (Cap. VII), secondo un modello collaborativo consueto negli strumenti onusiani, volto a rafforzare la capacità degli Stati di dare attuazione alla Convenzione e a perseguirne efficacemente gli scopi;
6. disciplina, infine, il meccanismo di attuazione della Convenzione (Cap. VIII), attraverso l'istituzione di un organo di governo del trattato (la Conferenza degli Stati parte), assistito da un Segretariato.

3.5. Focus sui punti più problematici.

I temi più sensibili e divisivi, nel corso dei negoziati, sono stati tre: l'ambito di applicazione della Convenzione; le disposizioni a salvaguardia del rispetto dei diritti umani e delle libertà fondamentali; la formulazione delle fattispecie incriminatrici in materia di abuso o sfruttamento sessuale di minori attraverso il sistema informatico.

Su tali punti, all'esito di un paziente e complesso lavorio diplomatico, il Comitato *ad hoc* ha raggiunto, ma soltanto *in extremis*, una soluzione di compromesso che rispetta le linee invalicabili (*red-lines)* che l'Unione Europea, per conto dei 27 Paesi membri, aveva tracciato, d'intesa con i Paesi *like-minded.*

Non sfugge, a un occhio attento, il prezzo pagato al compromesso: l'impegno a lavorare in vista di un protocollo addizionale, contenuto nella risoluzione n. 79/243 del 24 dicembre 2024. Con tale risoluzione, l'Assemblea delle Nazioni Unite, nell'adottare il testo della Convenzione, ha incaricato il Comitato *ad hoc* di «proseguire i propri lavori, *mutatis mutandis*, in conformità con le risoluzioni 74/247 e 75/282 dell'Assemblea Generale, al fine di negoziare un progetto di protocollo supplementare alla Convenzione che affronti, tra l'altro, ulteriori reati penali, se del caso». La stessa risoluzione prevede lo svolgimento di due sessioni della durata di 10 giorni ciascuna, la prima delle quali si terrà due anni dopo l'adozione della Convenzione da parte dell'Assemblea Generale e la seconda nell'anno successivo, rispettivamente a Vienna e a New York, al fine di presentare i risultati alla Conferenza delle Parti della Convenzione, affinché siano esaminati e siano intraprese ulteriori azioni, in conformità con gli articoli 57, paragrafo 5 (g), 61 e 62 della Convenzione.

3.5.1. Ambito di applicazione e misure di armonizzazione sostanziale e processuale.

Quanto all'ambito di applicazione, il testo finale dell'art. 3, frutto di una soluzione faticosamente mediata tra le delegazioni, ne traccia un doppio livello:

a) uno più ampio per i reati previsti nella Convenzione (ossia i reati per i quali la Convenzione impone l'obbligo di incriminazione, descritti agli artt. 7-17). Le disposizioni della Convenzione trovano integrale applicazione relativamente alla prevenzione, alle indagini e all'esercizio dell'azione penale in ordine a tali reati, ivi comprese le disposizioni riguardanti il sequestro, la confisca e la restituzione dei proventi e del profitto dei medesimi reati;
b) uno più ristretto per la raccolta, la conservazione e la condivisione della prova in formato elettronico: a questi fini, negli ordinamenti interni è prevista l'applicazione delle misure procedurali di cui al capitolo IV (art. 23), con importanti *caveat* per le misure più intrusive (che ciascuno Stato può riservarsi di applicare solo a determinate categorie di reati gravi: artt. 23.3.a e 30.1). Invece, la cooperazione internazionale è limitata ai soli reati "gravi" (art. 35.1.c), ossia a quelli puniti con una pena detentiva massima di almeno 4 anni (art. 2.1.h).

Tale ambito applicativo è *più ristretto* di quello contenuto nella Convenzione di Budapest, che non prevede limiti edittali per i reati in relazione ai quali è ammessa la collaborazione per lo scambio di prova elettronica (art. 25 della Convenzione di Budapest).

Sostanzialmente *coincidente* con il dettato della Convenzione di Budapest, invece, è l'area di applicazione delle misure procedurali più intrusive (la raccolta in tempo reale di dati di traffico e l'intercettazione di dati relativi al contenuto di comunicazioni), in ordine alle quali anche la Convenzione del Consiglio d'Europa consente agli Stati limitazioni rimesse al diritto interno (artt. 14.3.a e 21.1 della Convenzione di Budapest).

Venendo alle misure di armonizzazione minima, con riguardo al diritto penale sostanziale si registra una parziale *difformità* tra il novero dei reati per cui la Convenzione prevede l'incriminazione e quelli contemplati dalla Convenzione di Budapest.

Infatti, la nuova Convenzione

- negli artt. 7-11 replica il nucleo tradizionale dei reati "*cyber-dependent*" contenuti nella Convenzione di Budapest (artt. 2-6): accesso illegale, intercettazione illegale, interferenza con i dati elettronici, interferenza in un sistema, uso improprio di dispositivi;
- agli artt. 12 e 13 aggiunge i due reati "*computer-related*" previsti dalla stessa Convenzione del Consiglio di Europa (artt. 7 e 8): falsità informatica e frode informatica
- e tuttavia amplia la descrizione del reato di "furto o frode" informatica (art. 13), estendendola a qualsiasi truffa commessa per il tramite dello strumento informatico.

Ulteriori *novità*, rispetto alla Convenzione di Budapest, poi, è costituita dalla previsione:

- dell'autonomo reato di adescamento dei minori *on-line* allo scopo di commettere reati sessuali (art. 15)
- del reato di diffusione non consensuale di immagini intime (art. 16);
- del reato di riciclaggio (art. 17).

Il reato relativo agli abusi sessuali in rete sui minori (art. 14), pur se diversamente formulato rispetto all'omologo della Convenzione di Budapest (art. 9), vi corrisponde nella sostanza, anche nei margini di flessibilità concessi agli Stati per temperare l'obbligo di incriminazione dei minorenni in caso di auto-produzione e scambio di immagini intime (art. 14.4.b).

Ulteriore elemento differenziale, infine, è la mancanza, nella Convenzione ONU, di un'incriminazione per le violazioni dei diritti di autore analoga a quella prevista dall'art. 10 della Convenzione di Budapest.

Quanto alle misure processuali, il catalogo comprende il medesimo strumentario della Convenzione di Budapest:

- conservazione rapida di dati elettronici immagazzinati (art. 25);
- conservazione e parziale divulgazione rapide di dati relativi al traffico (art. 26);
- ordine di produzione (art. 27);
- perquisizione e sequestro di dati informatici immagazzinati (art. 28);
- raccolta in tempo reale di dati relativi al traffico (art. 29);

- intercettazione di dati relativi al contenuto, limitato a una serie di gravi reati, da definire nelle legislazioni dei singoli Paesi (art. 30).

A tali misure (disciplinate in modo analogo a quelle corrispondenti della Convenzione di Budapest, anche per quanto attiene alla riservatezza delle operazioni), la nuova Convenzione ONU aggiunge, per i soli reati previsti dalla Convenzione (quelli oggetto di "armonizzazione" obbligatoria), l'obbligo di adottare ulteriori misure per assicurare il "congelamento", il sequestro e la confisca dei proventi del reato (art. 31), la protezione dei testimoni (art. 33), l'assistenza e la protezione delle vittime (art. 34).

3.5.2. Clausole di salvaguardia.

Venendo al secondo punto, relativo alle garanzie del rispetto dei diritti umani e delle libertà fondamentali, il testo convenzionale vede l'inserimento di esplicite e robuste clausole di salvaguardia, inedite rispetto ai precedenti trattati, volte a bilanciare le misure che gli Stati sono chiamati ad attivare sul piano nazionale e internazionale con l'imprescindibile tutela dei diritti umani e delle libertà fondamentali.

Questa finalità si esprime attraverso:

- l'inserimento, tra le disposizioni generali, di un'importante clausola di protezione dei diritti umani (art. 6), con l'espressa menzione dei diritti e delle libertà fondamentali a più alto rischio, a fronte dei penetranti poteri attribuiti ad autorità giudiziarie e forze di polizia (art. 6.2: «*Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law*»);
- la chiara affermazione del dovere di rispettare il diritto dei singoli al giusto processo e il diritto di difesa (art. 21.4);
- l'articolazione specifica degli obblighi di rispetto dei diritti umani in relazione alle misure processuali e di polizia, sia a livello domestico, sia in sede di cooperazione internazionale, con l'espresso richiamo di principi e diritti fondamentali che nel nostro ordinamento costituiscono parte integrante del giusto processo, quali il principio di proporzionalità, il diritto al controllo da parte di autorità giurisdizionali o altre autorità indipendenti, il diritto a rimedi effettivi, la giustificazione e la limitazione delle misure procedurali (art. 24, paragrafi 1, 2 e 4);
- la previsione di un robusto apparato di garanzia anche sul fronte della cooperazione internazionale, con l'indicazione di una serie di motivi di rifiuto che assicurino un alto standard di protezione dei dati personali (art. 36) e dei diritti umani, neutralizzando la possibilità dell'utilizzo strumentale della Convenzione per motivi di persecuzione e discriminazione (art. 37.15, in riferimento all'estradizione: «*Nothing in this Convention shall be interpreted as imposing an obligation to extradite if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing*

a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions, or that compliance with the request would cause prejudice to that person's position for any one of these reasons.» Identica clausola è prevista dall'art. 40.22 per l'assistenza giudiziaria reciproca).

3.5.3. Reati connessi all'abuso o allo sfruttamento sessuale di minori attraverso il sistema informatico.

Gli artt. 14, 15 e 16 apprestano la tutela penale contro gli abusi sessuali in rete ai danni di minori.

Nell'art. 14, innanzi tutto, viene stabilito l'obbligo di incriminazione dei reati connessi all'abuso o allo sfruttamento sessuale *on-line* di minori (*Offences related to online child sexual abuse or child sexual exploitation material*), attraverso la sostanziale riproduzione delle fattispecie incriminatrici già descritte nell'art. 9 della Convenzione di Budapest (produzione, offerta, vendita, distribuzione, invio, trasmissione, visualizzazione, pubblicazione, o di attribuzione in altro modo della disponibilità di materiale relativo ad abusi o sfruttamento sessuale attraverso un sistema tecnologico di informazione e comunicazione; ma anche sollecitazione e accesso a detto materiale *on-line* e possesso dello stesso).

Vengono poi introdotte due fattispecie innovative rispetto alla Convenzione di Budapest: il reato di adescamento dei minori *on-line* allo scopo di commettere reati sessuali (art. 15: *Solicitation or grooming for the purpose of committing a sexual offence against a child*) e il reato di diffusione non consensuale di immagini intime (art. 16: *Non-consensual dissemination of intimate images*);

Al pari di quanto previsto dalla Convenzione di Budapest, la punibilità richiede l'intenzionalità e abusività ("*without right*") della condotta.

Il paragrafo 2 dell'art. 14 definisce cosa si intenda per "materiale relativo ad abusi o sfruttamento sessuale di minori". Esso *deve* includere il materiale visivo e *può* includere anche i contenuti scritti o audio che – in ambedue i casi – raffigurano, descrivono o rappresentano un minore: (a) che è impegnato in attività sessuali reali o simulate; (b) in presenza di una persona impegnata in qualsiasi attività sessuale; (c) le cui parti sessuali ("*sexual parts"*) vengono mostrate per scopi principalmente sessuali; (d) sottoposto a tortura o trattamenti o punizioni crudeli, inumani o degradanti, quando tale materiale sia di natura sessuale ("*serxual in nature"*).

Il richiamato paragrafo 2 contiene tre profili di novità rispetto alla Convenzione di Budapest:

- l'inclusione opzionale (con una "*may provision*") di contenuti scritti o audio tra il materiale relativo ad abusi o sfruttamento sessuale di minori";
- l'inclusione del materiale che rappresenta il minore sottoposto a tortura o trattamenti o punizioni crudeli, inumani o degradanti, quando tale materiale sia di natura sessuale;
- l'estensione delle "attività sessuali" a quelle "simulate".

A fronte dell'esteso perimetro applicativo della fattispecie, all'esito di un faticosissimo negoziato è stato ottenuto un temperamento dell'obbligo di incriminazione, tale da rendere la formulazione del testo compatibile con gli assetti normativi interni di molti Paesi (tra i quali l'Italia) e coerente con gli altri obblighi di fonte sovranazionale, derivanti dalla Convenzione di Budapest (art. 9.4), dalla Convenzione di Lanzarote (art. 20.3) e dalla direttiva 2011/93/UE (art. 5.8 e art. 8.3).

Una prima "*may provision*" è stata inserita nel paragrafo 3, che consente di limitare la nozione di materiale rilevante alla pedopornografia reale.

La seconda eccezione all'obbligo di criminalizzazione, inserita nel paragrafo 4, riguarda il materiale autoprodotto dal minore e le condotte tenute nell'ambito di un rapporto consensuale, limitatamente ai minori che hanno raggiunto l'età legale per svolgere attività sessuale secondo l'ordinamento interno, sempre che tale materiale sia conservato esclusivamente per l'uso privato delle persone raffigurate.[39]

Si tratta di un'area di liceità penale che molti Stati hanno voluto mantenere per non incorrere nel rischio di *over-criminalization* degli stessi minorenni. Al tempo stesso, questo spazio di tutela della libertà sessuale dei minorenni è stata fortemente osteggiato da parte di una serie di Paesi che ne rivendicano l'incompatibilità con i propri principi etici e tradizioni religiose[40].

Merita ricordare, al riguardo, gli analoghi margini di flessibilità concessi:

- dalla Convenzione di Budapest (art. 9, comma 4: «*Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d and e, and 2, sub-paragraphs b and c*»);
- dalla Convenzione di Lanzarote (art. 20, comma 3: «*Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material:*
    - *consisting exclusively of simulated representations or realistic images of a non-existent child;*

---

[39] «4. *In accordance with their domestic law and consistent with applicable international obligations, States Parties may take steps to exclude the criminalization of:*

(a) Conduct by children for self-generated material depicting them; or

(b) The consensual production, transmission, or possession of material described in paragraph 2 (a) to (c) of this article, where the underlying conduct depicted is legal as determined by domestic law, and where such material is maintained exclusively for the private and consensual use of the persons involved.»

[40] Ne sono prova le quattro richieste di emendamento al testo degli artt. 14 e 16 poste al voto, nella sessione finale del Comitato *ad hoc*, su richiesta della Repubblica islamica dell'Iran (e sostenute da diversi altri Paesi, per motivi connessi alle tradizioni culturali e religiose islamiche), ma anche la riserva espressa dall'unico Stato che finora ha ratificato il trattato, il Qatar, proprio rispetto agli obblighi derivanti dagli artt. 14, 15, 16 della Convenzione, che esso considera contrari alla legge islamica della Sharia, al proprio diritto interno e ai valori sociali e culturali dello Stato («*The State of Qatar does not consider itself bound by the provisions of Articles (16), (15), and (14) of the Convention, as they contradict the provisions of Islamic Sharia, national legislation, and the social and cultural values of the State of Qatar*»: la riserva è reperibile al *link*: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=_en)

  - *involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use*»);
- dalla direttiva 2011/93/EU, che consente la deroga all'obbligo di incriminazione:
  - *in caso di immagini realistiche ritraenti minori nel compimento di atti sessuali o organi sessuali di un minore, prevalentemente a scopo sessuale, le quali siano state prodotte e siano possedute solo dall'autore, per suo uso personale, e sempre che non vi sia stato abuso alcuno e non vi sia rischio di divulgazione del materiale (art. 5, comma 8, «It shall be within the discretion of Member States to decide whether paragraphs 2 and 6 of this Article apply to cases where it is established that pornographic material as referred to in Article 2(c)(iv) is produced and possessed by the producer solely for his or her private use in so far as no pornographic material as referred to in Article 2(c)(i), (ii) or (iii) has been used for the purpose of its production and provided that the act involves no risk of dissemination of the material»);*
  - *in caso di attività di produzione, acquisto o possesso di materiale pedopornografico in cui sono coinvolti minori che abbiano raggiunto l'età del consenso sessuale, nei casi in cui tale materiale è prodotto e posseduto con il consenso di tali minori e unicamente per l'uso privato delle persone coinvolte (Art. 8, comma 3: «It shall be within the discretion of Member States to decide whether Article 5(2) and (6) apply to the production, acquisition or possession of material involving children who have reached the age of sexual consent where that material is produced and possessed with the consent of those children and only for the private use of the persons involved, in so far as the acts did not involve any abuse»).*

Del resto, proprio grazie a tali margini di elasticità, nella legislazione nazionale e nell'interpretazione che ne ha fornito la Corte di cassazione[41] si è ritagliato uno spazio di *liceità*, rispetto al reato di pornografia minorile di cui all'art. 600-*ter*, comma primo, cod. pen., ma soltanto nel caso in cui la produzione di materiale pornografico sia realizzata senza l'"utilizzazione" del minore e con il consenso espresso di colui che abbia raggiunto l'età per manifestarlo; con l'ulteriore precisazione che «[s]i ha "utilizzazione" del minore allorquando, all'esito di un accertamento complessivo che tenga conto del contesto di riferimento, dell'età, maturità, esperienza, stato di dipendenza del minore, si appalesino

[41] Corte di cssazione, sezioni unite penali, sentenza n. 4616 del 28 ottobre 2021 – 9 febbraio 2022, Rv. 282718. A commento della sentenza, in dottrina, N. RECCHIA, *Pregevoli approdi e persistenti criticità nella sentenza delle Sezioni unite sul sexting. (Pornografia minorile).*in *Giur. it*., 2022, fasc. 6, p. 1470, evidenzia come l'arresto confermi, rispetto alla condotta di *produzione* di immagini intime tra minori, la scelta restrittiva dell'area del penalmente rilevante, da tempo salutata con favore dalla dottrina, mentre con riguardo soprattutto alla divulgazione del materiale denota al contrario un atteggiamento di grande rigore repressivo da parte della Corte di cassazione. Sulla sentenza, fra gli altri, v. altresì S. BERNARDI, *Le Sezioni unite chiariscono i limiti della (ir)rilevanza della "pedopornografia domestica" ai sensi dell'art. 600-*ter *c.p.,* in *Sist. pen.,* 2022, 25 febbraio 2025; M. GRANDE, *L'elemento oggettivo del reato di pornografia minorile,* in Cass. pen., 2022, fasc. 7-8, sez. 2, p. 2509; A. PECCIOLI, *La rilevanza penale della pedopornografia ad uso personale tra punti fermi e residui profili critici. (Pornografia minorile),* in *Dir. pen. e proc.*, 2022, fasc. 9, p. 1195.

forme di coercizione o di condizionamento della volontà del minore stesso, restando escluse dalla rilevanza penale solo condotte realmente prive di offensività rispetto all'integrità psico-fisica dello stesso»[42].

Si tratta, quindi, di un'area di liceità penale delineata dal diritto interno proprio per non incorrere nel rischio di *over-criminalization* degli stessi minorenni; evenienza che anche la nuova Convenzione delle Nazioni Unite ha inteso scongiurare, fermo restando che, come chiarito dalle Sezioni unite della Corte di cassazione, nell'ordinamento interno la circolazione del materiale "pornografico", pur realizzato con il libero consenso della persona che ha raggiunto l'età per manifestarlo, non potrà mai essere considerata lecita.[43]

3.6. La cooperazione internazionale: profili differenziali rispetto alla Convenzione di Budapest e ai suoi Protocolli.

Il Capitolo V comprende gli strumenti tradizionali di cooperazione internazionale (estradizione, trasferimento di persone condannate e di procedimenti penali, reciproca assistenza giudiziaria) e le nuove forme più idonee a fronteggiare la criminalità informatica, quali:

- la rete di punti di contatto attivi 24 ore su 24, 7 giorni su 7, in ciascuno Stato parte, al fine di facilitare l'assistenza immediata, ad esempio, nella conservazione delle prove elettroniche, nell'identificazione dei fornitori di servizi pertinenti o nella localizzazione dei sospetti (art. 41);
- le procedure rapide per la conservazione e l'acquisizione di dati elettronici (artt. 42 e 43);
- l'assistenza giudiziaria reciproca per l'accesso ai dati (art. 44), per l'acquisizione in tempo reale di dati di traffico (art. 45) e per l'intercettazione dei dati relativi ai contenuti (art. 46);
- la collaborazione diretta tra le forze di polizia (art. 47);
- le indagini congiunte (art. 48);
- la cooperazione finalizzata alla confisca e al recupero dei beni (artt. 49 e 50);
- la cooperazione speciale senza preventiva richiesta (art. 51) e quella finalizzata alla restituzione e destinazione dei beni confiscati (art. 52).

Si tratta di misure analoghe a quelle previste dalla Convenzione di Budapest, ma che nella nuova Convenzione presentano un ambito applicativo più circoscritto quando sono finalizzate alla raccolta della prova elettronica (che, come si è detto sopra, viene riferita soltanto ai reati gravi, ossia quelli puniti con pena massima non inferiore a

[42] Così Cass., sez. un., sentenza n. 4616 del 2022, cit.

[43] Cass., sez. un., sentenza n. 4616 del 2022, cit.: «ai fini dell'integrazione dei reati di cui ai commi terzo e quarto dell'art. 600-*ter* cod. pen. non rileva il consenso del minore alla circolazione, comunque sempre vietata, del materiale prodotto, provenendo da soggetto che presuntivamente non ha ancora raggiunto un livello di maturità tale da consentirgli una valutazione consapevole circa le ricadute negative della mercificazione del proprio corpo attraverso la divulgazione delle immagini erotiche, anche in considerazione di una eventuale circolazione ritardata nel tempo rispetto al momento della loro realizzazione».

quattro anni). Presentano, inoltre, un minor grado di vincolatività le misure più intrusive, consistenti nella raccolta in tempo reale di dati relativi al traffico e nell'intercettazione di dati relativi al contenuto. Per tali misure, in luogo di un preciso obbligo di fornire l'assistenza, gli artt. 45 e 46 prevedono un mero obbligo di "*sforzarsi*" di fornire l'assistenza («*shall endeavour to provide*»).

D'altro canto, la Convenzione del Consiglio d'Europa del 2001 rimane, ad oggi, più "competitiva" anche per effetto dell'adozione del suo Secondo Protocollo aggiuntivo sul rafforzamento della cooperazione e sulla divulgazione delle prove elettroniche. Esso contiene, infatti, meccanismi extraterritoriali semplificati più vicini agli strumenti dell'Unione europea, basati sul riconoscimento reciproco, non previsti dalla Convenzione delle Nazioni Unite.

Si fa riferimento, in particolare, alla:

- divulgazione diretta di informazioni sulla registrazione di nomi di dominio da parte di un soggetto che fornisce tali servizi sul territorio di un altro Stato;
- divulgazione diretta delle informazioni relative agli abbonati, da parte di un prestatore di servizi sul territorio di un altro Stato;
- esecuzione degli ordini di un altro Stato parte per la produzione accelerata di informazioni sugli abbonati e dei dati sul traffico;
- divulgazione accelerata dei dati informatici memorizzati attraverso i punti di contatto della rete 24/7 senza richiesta di assistenza giudiziaria
- assistenza giudiziaria reciproca in casi di emergenza;
- accesso transfrontaliero ai dati immagazzinati con il consenso dell'avente diritto o accessibili al pubblico (previsto dall'art. 32 della Convenzione di Budapest).

3.7. Le prospettive della Convenzione.

L'art. 65 della Convenzione prevede che essa entrerà in vigore il novantesimo giorno successivo al deposito del quarantesimo strumento di ratifica, accettazione, approvazione o accessione (art. 65).

Per l'Italia, come per gli altri Paesi dell'Unione Europea, il processo di ratifica sarà condizionato dalle decisioni dell'Unione europea, che dovrà valutare a sua volta se ratificare il trattato ed eventualmente se e quali riserve consentire. Quel che è certo, al momento, è che il Consiglio dell'Unione europea, con decisione del 13 ottobre 2025[44], ha autorizzato la firma della Convenzione da parte dell'Unione europea[45]. L'Unione

[44] La decisione del Consiglio (UE) 2025/2307 è reperibile al *link* https://eur-lex.europa.eu/eli/dec/2025/2307/oj/eng

[45] La competenza dell'Unione europea, con riferimento alle materie oggetto della Convenzione sul *Cybercrime*, viene in rilievo a un duplice livello: a) diritto penale sostanziale (armonizzazione); b) cooperazione giudiziaria.
Sotto il primo profilo, all'interno del Trattato di Lisbona, il nucleo centrale della competenza penale della Unione europea risiede nell'art. 83.1 TFUE, in base al quale il Parlamento europeo e il Consiglio possono stabilire "norme minime" relative ai reati e alle sanzioni concernenti le gravi forme di criminalità transfrontaliera ("*norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità*

europea, infatti, ha titolo essa stessa per firmare il trattato, quale organizzazione regionale di integrazione economica (art. 64, par. 2, della Convenzione) e ha reputato lo strumento internazionale conforme ai suoi obiettivi in materia di sicurezza, ai sensi dell'articolo 67, paragrafo 3, del trattato sul funzionamento dell'Unione europea (TFUE), volti a garantire «un livello elevato di sicurezza attraverso misure di prevenzione e di lotta contro la criminalità, attraverso misure di coordinamento e cooperazione tra forze di polizia e autorità giudiziarie e altre autorità competenti, nonché tramite il ravvicinamento delle legislazioni penali»[46].

Come già si è detto sopra[47], oltre alla stessa Unione europea, solo tredici Paesi membri dell'Unione (tra i quali non compare l'Italia) hanno sinora firmato la Convenzione. Complessivamente, alla data del 30 marzo 2026, risultano raccolte 75 firme. Un solo Paese (il Qatar) ha anche ratificato il trattato.

Dopo la sua entrata in vigore, la Convenzione sarà assistita da un meccanismo di attuazione governato dalla Conferenza degli Stati Parte (art. 57), analogamente a quanto già avviene per la UNTOC e la UNCAC.

La prima riunione della Conferenza sarà convocata entro l'anno successivo all'entrata in vigore della Convenzione (art. 57.2). La Conferenza adotterà, in questa occasione, le regole che ne disciplineranno il funzionamento e quelle del meccanismo di attuazione della Convenzione (art. 57.3). La risoluzione n. 79/243 dell'Assemblea Generale (paragrafo operativo n. 6) attribuisce il mandato di redigere la bozza delle regole di funzionamento della Conferenza degli Stati parte della Convenzione allo stesso Comitato *ad hoc* che ha elaborato la Convenzione, prevedendo a tal fine la convocazione a Vienna di una sessione di 5 giorni, un anno dopo l'adozione della Convenzione. La

---

particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni").

Sempre l'art. 83.1 contiene un'elencazione delle suddette sfere criminali (i c.d. euro-delitti): "*terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata*".

Per tali reati l'Unione europea può stabilire, tramite direttive, norme minime relative alla definizione dei reati e delle sanzioni (art. 83.2 TFUE).

Tra gli euro-delitti sono compresi i reati di criminalità informatica, riciclaggio e sfruttamento dei minori, riconducibili all'ambito di applicazione della Convenzione *Cybercrime*.

La base giuridica della competenza dell'Unione in materia di cooperazione giudiziaria penale è, invece, negli articoli da 82 a 86 TFUE.

In entrambi i casi (armonizzazione del diritto sostanziale e cooperazione giudiziaria) la competenza dell'Unione riguarda materie sulle quali gli Stati conservano la loro competenza. Non si tratta di competenza esclusiva, ma concorrente con quella degli Stati.

In ambedue gli ambiti, peraltro, l'Unione europea già dispone di norme comuni.

È invece di competenza esclusiva degli Stati quella in materia di diritto processuale interno. Proprio a questo proposito potranno porsi problemi atteso che alcuni Paesi non vogliono dover subire un obbligo di introduzione, nell'ordinamento interno, di misure intrusive come la raccolta in tempo reale di *traffic-data* o le intercettazioni di *content-data*. Questi Stati si aspettano, pertanto, che l'Unione europea lasci la possibilità di apporre riserve su questo punto, al momento della ratifica.

[46] Cfr. decisione del Consiglio (UE) 2025/2307, cit., punto (3).

[47] Cfr. paragrafo 3.1 e nota 36.

prima sessione è stata già tenuta il 26-30 gennaio 2026, senza che, tuttavia, sia stato raggiunto un consenso sul testo che, dopo dieci sessioni di negoziato, era stato proposto dal Presidente del Comitato. Come da calendario, la prossima sessione si terrà a Vienna, dal 18 al 29 gennaio 2027[48].

Al Comitato *ad hoc* la risoluzione (paragrafo operativo 5) assegna anche il compito di continuare il suo lavoro in vista della redazione di una bozza di protocollo addizionale («*with a view to negotiating a draft protocol supplementary to the Convention, addressing, inter alia, additional criminal offences as appropriate*»). A tale scopo saranno dedicate due ulteriori sessioni del Comitato, della durata di 10 giorni ciascuna, da tenersi rispettivamente a Vienna e a New York: la prima due anni dopo l'adozione della Convenzione da parte della Assemblea Generale, la seconda nell'anno successivo.

I risultati del lavoro del Comitato saranno poi sottoposti alla Conferenza delle Parti, che potrà adottare eventuali protocolli addizionali nel rispetto di quanto previsto dagli artt. 57, 61 e 62 della Convenzione. Sarà quindi necessario che almeno 60 Paesi ratifichino la Convenzione prima che la Conferenza degli Stati parte possa adottare qualsiasi protocollo; in ogni caso, l'adozione del protocollo dovrà avvenire per consenso o, in mancanza, con la maggioranza qualificata di 2/3 dei Paesi presenti e votanti nella Conferenza (art. 62).

La strada da percorrere per la concreta operatività della Convenzione, quindi, è ancora lunga e incerta.

Considerato l'interesse con cui sono stati seguiti i negoziati, specialmente dai tantissimi Paesi che non sono parte della Convenzione del Consiglio d'Europa, è possibile che la soglia (pur piuttosto alta) delle quaranta ratifiche fissata per l'entrata in vigore del trattato sia raggiunta. La persistente attenzione nei confronti del trattato sembra confermata, del resto, dall'alta partecipazione registratasi in occasione della recente riunione del Comitato *ad hoc*, per la prima sessione dedicata alla preparazione del testo con le regole di funzionamento della Conferenza degli Stati parte: dal *report* della sessione[49], infatti, risulta che alla riunione dello scorso gennaio hanno partecipato 122 Stati parte delle Nazioni unite, oltre ai numerosi osservatori (Stati non membri, enti intergovernativi, enti ed organizzazioni non governative, tra i quali moltissimi soggetti provenienti dalla società civile, dalle istituzioni accademiche e dal settore privato).

Bisognerà vedere, tuttavia, se tali aspettative non siano divenute irrealistiche, alla luce dell'ulteriore, grave contraccolpo che il multilateralismo e, in generale, la credibilità e la tenuta del diritto internazionale hanno subito per effetto, nell'ultimo anno, dell'acuirsi dei conflitti e dell'instabilità nello scenario geopolitico mondiale.

Sicuramente poco probabile appare la prospettiva, a breve, di un allargamento dell'ambito applicativo della Convenzione, nonostante l'impegno immediato ad avviare i lavori in vista di un protocollo addizionale. E ciò sia per la soglia di ratifiche e per la maggioranza qualificata richiesta a tal fine dall'art. 62 della Convenzione, sia per l'obiettiva difficoltà, nell'attuale contesto, di trovare un consenso su un'estensione

---

[48] I documenti di lavoro e il *report* della sessione sono reperibili al *link* https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_session_on_RoP/main.html

[49] Reperibile al *link* https://docs.un.org/en/A/RES/79/243

dell'ambito di armonizzazione e/o degli strumenti utilizzabili per la cooperazione internazionale. Alla accentuata polarizzazione che, in generale, contraddistingue le dinamiche multilaterali più recenti si aggiunge, infatti, la peculiarità della materia oggetto del contendere, in cui il confronto tecnico è condizionato da contrapposizioni di matrice ideologica, politica e religiosa. Non solo: è fortissima anche la pressione esterna proveniente dalle associazioni per i diritti umani e dall'industria informatica (le c.d. *big-tech*), entrambe preoccupate per l'ampiezza della portata del trattato e per i rischi che esso favorisca una "sorveglianza globale", lesiva della *privacy*, della libertà di espressione del pensiero e, in generale, dei diritti e delle libertà fondamentali.

Converrà, quindi, concentrarsi sui risultati sin qui conseguiti e lavorare perché gli stessi si traducano in strumenti effettivamente utilizzabili, nella consapevolezza (pragmatica) che la Convenzione della Nazioni unite rappresenta un punto di caduta tra diverse e contrapposte visioni, sintesi ultima possibile in una stagione – quella dei grandi trattati internazionali – ormai al crepuscolo.

Pur con i suoi limiti, essa consente, per la prima volta, di allargare l'orizzonte della cooperazione internazionale per il contrasto alla criminalità informatica a un consesso potenzialmente universale. Al contempo, realizza un bilanciamento equilibrato tra l'esigenza di effettività nella prevenzione e nel contrasto del *cybercrime* e – grazie a un robusto apparato di condizioni, *caveat* e *ground for refusal* – quella di salvaguardia dei diritti umani e delle libertà fondamentali.