Freedom, Security & Justice: European Legal Studies

Rivista giuridica di classe A

2025, n. 2

EDITORIALE SCIENTIFICA

Rivista quadrimestrale on line "Freedom, Security & Justice: European Legal Studies" www.fsjeurostudies.eu
Editoriale Scientifica, Via San Biagio dei Librai, 39 - Napoli
CODICE ISSN 2532-2079 - Registrazione presso il Tribunale di Nocera Inferiore n° 3 del 3 marzo 2017

Indice-Sommario
2025, n. 2

Editoriale

Dalla dichiarazione Schuman al Libro bianco sulla prontezza alla difesa europea: verso una revisione del progetto europeo? p. 1
Ugo Villani

Saggi, Articoli, Commenti e Note

Le origini dello Spazio di libertà, sicurezza e giustizia. Pace e conflitti armati (1945-2025) p. 14
Massimo Panebianco

Migrare: un diritto fondamentale? p. 26
Antonio Ruggeri

Il ruolo della Procura europea (EPPO) nella tutela dello Stato di diritto dell'Unione europea p. 42
Serena Crespi

Norme di diritto internazionale e disparità di genere, idee vecchie e nuove. Il caso del *mundio muliebre*, uno stereotipo da rileggere p. 82
Lucia di Cintio

Convenzione delle Nazioni Unite contro il *cybercrime* e tutela dei diritti umani: influenze europee sullo scenario internazionale p. 108
Marco Dimetto

The error in predictive justice systems. Challenges for justice, freedom, and human-centrism under EU law p. 131
Alessandro Ferrara

EU impact on Albanian medical civil liability: a case law approach p. 146
Enkelejda Koka, Denard Veshi, Aisha Morina

La promozione della parità di genere nelle relazioni tra l'Unione europea e i *partner* meridionali p. 162
Claudia Morini

FOCUS

Democracy and the Rule of Law: A New Push for European Values

Il Focus contiene contributi elaborati a seguito della riflessione realizzata nel Seminario conclusivo dello Jean Monnet Module Eu-Draw (2022-2025) "Democracy and the Rule of Law: A New Push for European Values", tenutosi presso l'Università degli Studi di Salerno (1 aprile 2025)

Presentazione del *Focus* p. 192
Angela Di Stasi

Values in the EU external action: mechanisms of implementation and their outcomes p. 194
Stefania Kolarz

Justice and Home Affairs Cooperation (JHAC) in the perspective of enlargement p. 211
Teresa Russo

Brevi riflessioni sulla tutela dei diritti nello "spazio digitale" europeo p. 228
Francesco Buonomenna

Consiglio d'Europa e intelligenza artificiale: un primo tentativo di regolamentazione a tutela dei diritti umani, democrazia e Stato di diritto p. 242
Anna Iermano

La disinformazione *online* come "minaccia ibrida" alla democrazia nell'Unione europea: meccanismi di tutela e strumenti a contrasto per uno Spazio di libertà, sicurezza e giustizia p. 272
Angela Festa

L'"approccio europeo" al contrasto alla disinformazione digitale e alla protezione dei valori democratici: quale contributo dell'*AI Act?* p. 296
Rossana Palladino

CONVENZIONE DELLE NAZIONI UNITE CONTRO IL *CYBERCRIME* E TUTELA DEI DIRITTI UMANI: INFLUENZE EUROPEE SULLO SCENARIO INTERNAZIONALE

Marco Dimetto*

SOMMARIO: 1. Introduzione. – 2. Il contesto normativo europeo e internazionale nel quale si inserisce la nuova Convenzione. – 3. Una panoramica degli obblighi di incriminazione discendenti dalla Convenzione. – 4. La complessa delimitazione dell'ambito di esercizio della giurisdizione penale fra gli Stati. – 5. Le misure di cooperazione giudiziaria internazionale previste dalla Convenzione. – 6. La previsione di ulteriori misure procedurali particolarmente invasive. – 7. Il ruolo degli Stati nella vigilanza sull'interpretazione e applicazione della Convenzione e l'assenza di disposizioni volte a disciplinare una loro diretta responsabilità per attacchi cibernetici. – 8. Brevi considerazioni conclusive.

1. Introduzione

L'identificazione del contenuto delle norme del diritto internazionale applicabili al dominio cibernetico, nonché la delimitazione dell'ambito di esercizio della sovranità degli Stati in tale dominio[1], costituiscono attività assai complesse, in ragione delle radicali divergenze esistenti in rapporto ad esse fra gli Stati[2].

Double-blind peer reviewed article.

* Ricercatore in Diritto internazionale, Università degli Studi di Padova. Indirizzo e-mail: marco.dimetto@unipd.it.

Finanziato dall'Unione europea – Next Generation EU, (PRIN) 2022 - 022LEBME7, Missione 4 Componente 1, CUP C53D23002940006.

[1] Sulla nozione di «dominio cibernetico» o «spazio cibernetico» nel contesto del diritto internazionale sia consentito rinviare a N. TSAGOURIAS, *The Legal Status of Cyberspace: Sovereignty Redux?*, in N. TSAGOURIAS, R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham – Northampton, II ed., 2021, p. 11 ss.

[2] La letteratura sul punto è sconfinata. Per un'analisi recente, nel cui ambito vengono inquadrate le diverse posizioni degli Stati in rapporto all'esercizio della sovranità degli Stati nello spazio cibernetico, si veda V. KRISHNAMURTHY, *Anchoring Digital Sovereignty*, in *Chicago Journal of International Law*, 2025, p. 436 ss. Per un'analisi, meno recente, dei diversi approcci regionali alla sicurezza cibernetica internazionale, si veda E. TIKK, M. KERTTUNEN (eds.), *Routledge Handbook of International Cybersecurity*, Abingdon – New York, 2020 (soprattutto la Parte Terza, dedicata al tema *National and Regional Perspectives on Cybersecurity*). Più specificamente, sulla difficoltà di elaborare norme volte ad assicurare la sicurezza del dominio cyber, cfr. M. FINNEMORE, D.B. HOLLIS, *Constructing Norms for Global Cybersecurity*, in *American Journal of International Law*, 2016, p. 425 ss.

In tale contesto, il 24 dicembre 2024, l'Assemblea generale delle Nazioni Unite ha dato prova di saper efficacemente realizzare iniziative multilaterali volte a regolamentare un ambito specifico del dominio cibernetico[3]. Infatti, con la risoluzione 79/243, l'Assemblea generale ha adottato la nuova Convenzione contro il *cybercrime*[4], che sarà sottoscritta nel corso di una cerimonia formale ad Hanoi, in Vietnam, nell'ottobre del 2025. Tale decisione costituisce l'esito di un tortuoso processo negoziale, avviato con la risoluzione 74/247 del 27 dicembre 2019, istitutiva di un Comitato intergovernativo speciale di esperti, a composizione non limitata, avente quale scopo l'elaborazione di una convenzione internazionale sulla lotta contro l'uso di tecnologie di informazione e di comunicazione a fini criminali («Comitato»)[5].

La proposta di elaborare una Convenzione internazionale sul *cybercrime*, originariamente avanzata dalla Federazione Russa, fu dapprima osteggiata dai governi di numerosi Stati occidentali[6]. Questi ultimi, invero, consideravano l'iniziativa della Federazione Russa come finalizzata a sovvertire il carattere liberale del dominio cibernetico, la cui natura – come noto – è definita anche dalle condotte di «*stakeholders*» privati, *in primis* le c.d. «*big tech*»[7]. A tale preoccupazione se ne aggiungeva un'altra, ossia il pericolo che la nuova Convenzione potesse costituire un mezzo di sorveglianza globale, utilizzabile dagli Stati autoritari per la repressione e la persecuzione dei dissidenti

[3] In un contesto, quale è quello del dominio cibernetico, in cui lo sviluppo delle norme di diritto internazionale è generalmente molto complesso e lento, si è parlato – in conseguenza dell'inizio dei lavori per l'elaborazione della Convenzione oggetto di analisi in questo saggio – del *cybercrime* come «*a test case of norm-development*» (A. SEGURA SERRANO, *Cybersecurity and Cybercrime: Dynamic Application versus Norm-Development*, in *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 2021, p. 718 ss.). Più in generale, sul ruolo delle Nazioni Unite, cfr. C. HENDERSON, *The United Nations and the Regulation of Cyber-Security*, in N. TSAGOURIAS, R. BUCHAN (a cura di), *Research Handbook on International Law and Cyberspace*, cit., p. 582 ss.

[4] Assemblea generale, risoluzione 79/243 del 24 dicembre 2024, UN. Doc. A/RES/79/243.

[5] Assemblea generale, risoluzione 74/247 del 27 dicembre 2019, UN. Doc. A/RES/74/247. Si veda anche la risoluzione 75/282 del 26 maggio 2021, con cui l'Assemblea generale decise che il Comitato intergovernativo speciale di esperti avrebbe svolto le proprie attività a New York e Vienna, a partire dal gennaio del 2022.

[6] I voti a favore della risoluzione 74/247 furono 79, mentre quelli contrari 60, fra i quali è opportuno segnalare gli Stati Uniti, il Regno Unito, tutti gli Stati membri dell'Unione europea, l'Australia e il Canada (cfr. Nazioni Unite, Assemblea generale, *Official records* – A/74/PV.52, p. 37).

[7] In questo senso, la proposta di elaborazione di una convenzione internazionale sul crimine cibernetico era stata interpretata come chiaro esempio di «multilateralismo autoritario» (sul punto, si veda M. RAYMOND, J. SHERMAN, *Authoritarian Multilateralism in the Global Cyber Regime Complex: The Double Transformation of an International Diplomatic Practice*, in *Contemporary Security and Policy*, 2024, p. 124), nel quadro di una serie di altre proposte finalizzate a ridurre drasticamente il ruolo degli stakeholder privati, quali le c.d. «*big tech companies*», nel governo di internet (ibid., pp. 128-131), al fine di incrementare il controllo non solo «territoriale», bensì anche «extra-territoriale», degli Stati sui dati, gli utenti e le infrastrutture digitali (cfr. A. SUKUMAR, A. BASU, *Back to the Territorial State: China and Russia's Use of UN Cybercrime Negotiations to Challenge the Liberal Cyber Order*, in *Journal of Cyber Policy*, 2024, p. 12). Tuttavia, è d'uopo anche rammentare come proprio le attività delle «*big tech*» nel dominio cibernetico possano costituire fonte di pregiudizio per i diritti umani, e – per questo – in dottrina ci si è interrogati su come estendere ad esse l'applicazione del diritto internazionale dei diritti umani (recentemente, cfr. Y. SHANY, *Big Tech Companies' Obligations under International Human Rights Law*, in *Israel Law Review*, 2025, p. 3 ss.).

e degli oppositori politici all'estero[8]. Tuttavia, una volta avviato il negoziato, i governi degli Stati occidentali, compreso quello statunitense, decisero di prendervi parte, e ciò – chiaramente – per scongiurare i rischi appena menzionati.

Il presente articolo, dopo aver dato brevemente conto del panorama delle convenzioni regionali volte a contrastare la criminalità nel dominio cyber, si occuperà di analizzare la Convenzione ONU, e ciò al fine di identificare quali sue disposizioni possano potenzialmente essere interpretate e applicate in contrasto con norme a tutela di diritti umani, nonché per comprendere se le condizioni di salvaguardia introdotte nell'articolato, così come approvato dall'Assemblea generale, siano sufficienti per impedire efficacemente violazioni di tali norme. Sul punto, infatti, è opportuno evidenziare come il rappresentante degli Stati Uniti, pochi giorni prima dell'adozione del testo finale della Convenzione, avesse espresso grandi preoccupazioni, condividendo nella sostanza «*the legitimate concerns of many industry and civil society stakeholders that some States may seek to misuse this Convention or attempt to inappropriately leverage national legal frameworks that do not contain strong legal and human rights safeguards to facilitate bad acts*»[9].

2. Il contesto normativo europeo e internazionale nel quale si inserisce la nuova Convenzione

La Convenzione ONU sul *cybercrime* costituisce il primo strumento multilaterale che mette a disposizione degli Stati parte strumenti giuridici funzionali ad indagare e reprimere determinati crimini, realizzati attraverso sistemi di «*Information and Communication Technologies*» («sistemi ICT»), contribuendo così alla definizione di norme per la sicurezza cibernetica globale.

Tuttavia, va notato come – sul piano regionale – esistessero già delle convenzioni aventi medesime finalità. La più conosciuta è senz'altro la c.d. Convenzione di Budapest del 2001[10], promossa dal Consiglio d'Europa, di cui oggi sono parte 80 Stati, situati ben al di là dei confini europei[11]. In tempi più recenti, sono stati sottoscritti due diversi protocolli: il primo – del 2003 – concernente la criminalizzazione degli atti di natura razzista e xenofobica commessi tramite sistemi informatici, entrato in vigore nel marzo

[8] Cfr. ARTICLE 19, *UN Cybercrime Convention: A Blueprint for Human Rights Violations*, ove si sosteneva che «*[t]he Draft Convention enables intrusive surveillance measures without adequate judicial oversight or checks and balances*» (https://www.article19.org/resources/un-cybercrime-convention-a-blueprint-for-human-rights-violations/, ultimo accesso il 30 giugno 2025).

[9] Cfr. *United States Mission to the United Nations, Explanation of Position of the United States on the Adoption of the Resolution on the UN Convention Against Cybercrime in the UN General Assembly's Third Committee*, 11 novembre 2025 (https://usun.usmission.gov/explanation-of-position-of-the-united-states-on-the-adoption-of-the-resolution-on-the-un-convention-against-cybercrime-in-ungas-third-committee/, ultimo accesso il 30 giugno 2025).

[10] Consiglio d'Europa, *Convention on Cybercrime, E.T.S. No. 165*, 23 novembre 2001.

[11] Oltre agli Stati del continente europeo, sono parte della Convenzione di Budapest – fra gli altri – anche gli Stati Uniti, il Giappone, l'Australia, il Canada, l'Argentina, il Cile e la Turchia.

del 2003;[12] il secondo – del 2022 – concernente la cooperazione rafforzata e la «*disclosure*» di prove digitali, non ancora entrato in vigore[13]. Nonostante le iniziali ambizioni universalistiche della Convenzione di Budapest[14], è noto come essa sia vista con diffidenza da diversi Stati, primi fra tutti la Federazione Russa e la Cina, ma non solo. Alla base di tale diffidenza vi era il timore che l'adesione alla Convenzione di Budapest potesse recare pregiudizio alla loro «sovranità digitale», pregiudizio in primo luogo derivante – secondo i governi russo e cinese – dal contenuto dell'art. 32 della Convenzione, il quale prevede che le autorità giudiziarie di ciascuno Stato parte della Convenzione possano attivarsi presso un *service provider* straniero per accedere a od ottenere «dati informatici memorizzati su un supporto collocato in un altro Stato, se lo Stato richiedente ottiene il consenso lecito e autorizzato della persona legalmente autorizzata a divulgare tali dati»[15]. Peraltro, va osservato come proprio il secondo protocollo della Convenzione, non ancora entrato in vigore, punti a rafforzare significativamente la cooperazione fra le autorità giudiziarie di ciascuno degli Stati parte e gli attori privati siti in un altro Stato[16].

Proprio per reagire all'iniziativa promossa dal Consiglio d'Europa, la Comunità degli Stati Indipendenti, su iniziativa della Federazione Russa, ha negoziato e concluso, nel 2001, la Convenzione di Minsk sulla cooperazione «*in combating offences relating to computer information*»[17], meno articolata della Convenzione di Budapest. Successivamente, sempre la Federazione Russa, insieme con la Cina, ha avviato un negoziato nell'ambito della *Shanghai Cooperation Organization*, il quale è culminato nel 2009 nella conclusione della Convenzione di Ekaterinburg in materia di «*information security*»[18]. In tempi più recenti, anche la Lega degli Stati Arabi e l'Unione Africana si

[12] Consiglio d'Europa, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189*, 28 gennaio 2003.

[13] Consiglio d'Europa, *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CETS No. 224*, 12 maggio 2022.

[14] D. FLONK, M. JACHTENFUCHS, A. OBENDIEK, *Authority Conflicts in Internet Governance: Liberals vs. Sovereigntists?*, in *Global Constitutionalism*, 2020, pp. 377-378.

[15] M. FIDLER, *Fragmentation of International Cybercrime Law*, in *Utah Law Review*, 2025, p. 785 ss.

[16] A. GASCÓN MARCÉN, *The Budapest Convention and the UN Cybercrime Convention Negotiations*, in A. SEGURA SERRANO (ed.), *Global Cybersecurity and International Law*, Abingdon - New York, 2024, pp. 178-180. Incidentalmente, si noti come il ruolo degli attori privati sia decisivo nel contrasto al crimine cibernetico (cfr. J. BILLOW, *No Country is an Island: Embracing International Law Enforcement Cooperation to Reduce the Impact of Cybercrime*, in *Journal of Cyber Policy*, 2024, p. 155: «[…] *most times it will not be a public authority at all that is the first responder to a cyberattack or incident, but rather private sector entities and other third parties*»).

[17] *Agreement on cooperation among the States members of the Commonwealth of Independent States in combating offences relating to computer information*, 1° giugno 2001.
La traduzione inglese è presente sul sito della *Intellectual Property Agency* dell'Azerbaijan (https://copat.gov.az/docs/Qanunvericilik/Agreement%20on%20Cooperation%20in%20Combating%20Offences%20related%20to%20Computer%20Information%20-%20Commonwealth%20of%20Independent%20States.pdf?_t=1591267580, ultimo accesso il 30 giugno 2025).

[18] The Shanghai Cooperation Organisation, *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization*, 16 giugno

sono con successo dotate di strumenti regionali di contrasto alla criminalità informatica, rispettivamente la Convenzione del Cairo nel 2010 e la Convenzione di Malabo nel 2014[19].

Non si potrà in questa sede dare dettagliatamente conto dei contenuti di tutti questi strumenti regionali. Piuttosto, essi saranno considerati, in un'ottica di comparazione, nel corso dell'analisi sul contenuto della Convenzione delle Nazioni Unite. Quello che conviene sin d'ora evidenziare, tuttavia, è che tali strumenti manifestano la posizione che gli Stati, che di essi sono parti, hanno assunto in ordine alle modalità di esercizio delle loro prerogative sovrane nel dominio cibernetico. Come recentemente notato in dottrina, infatti, le convenzioni anzidette costituiscono un mezzo per affermare una specifica definizione di «sovranità digitale» rispetto a quella promossa da altri Stati[20].

3. Una panoramica degli obblighi di incriminazione discendenti dalla Convenzione

Il timore senza dubbio più significativo era legato alla portata degli obblighi di incriminazione discendenti dalla Convenzione. Nel corso dei negoziati, infatti, era stata avanzata la proposta di introdurre obblighi di incriminazione non soltanto per i reati informatici «tipici» (c.d. crimini «*cyber-dependent*»), i quali non possono essere perpetrati se non con l'utilizzo di un sistema informatico, bensì anche per i reati che possono essere commessi anche «*offline*», ma la cui commissione sia resa più agevole o efficace con l'utilizzo di sistemi ICT (c.d. crimini «*cyber-enabled*»)[21]. Se la Convenzione avesse contemplato l'obbligo di perseguire non soltanto i primi, bensì anche – e in via generalizzata – i secondi, maggiore sarebbe stato il rischio che tale strumento potesse

2009 (disponibile all'indirizzo https://eng.sectsco.org/files/207508/207508, ultimo accesso il 30 giugno 2025).

[19] Lega araba, *Arab Convention on Combating Information Technology Offenses*, 21 dicembre 2010; Unione Africana, *African Union Convention on Cybersecurity and Personal Data Protection*, 27 giugno 2014.

[20] M. FIDLER, *Fragmentation of International Cybercrime Law*, cit., pp. 741-742.

[21] A titolo di esempio, vanno menzionate le proposte del Regno Unito e del Ghana. Il primo aveva avanzato, fra le altre, l'idea di includere un obbligo di incriminazione della truffa, «*commited in whole or partly online*» (cfr. *UK Contribution on General Provisions, Criminalisation and Procedural Measures and Law Enforcement*, 2022, p. 5, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/United_Kingdom_contribution_E.pdf, ultimo accesso il 30 giugno 2025). Il secondo aveva proposto l'introduzione di obblighi di incriminazione concernenti, fra gli altri, i delitti di «*cyberstalking*», «*sextortion*» e minaccia di distribuzione di immagini intime (cfr. *Ghana's Contributions for the Provisions on Criminalisation, General Provisions and Provisions on Procedural Measures and Law Enforcement for the Future UN Convention on Countering the Use of ICTs for Criminal Purposes*, 2022, p. 5 ss., https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Ghana_contribution.pdf, ultimo accesso il 30 giugno 2025). Da ultimo, va segnalato come l'Iran avesse proposto l'introduzione, fra gli altri, di obblighi di incriminazione di condotte consistenti nell'insultare valori religiosi (cfr. *Comments of the Islamic Republic of Iran in response to the Guiding Questions presented by the Chair of the Ad Hoc Committee to Elaborate a Convention on Countering the Use of ICT for Criminal Purposes to the Second Session of the Committee*, 2022, p. 5, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/IRAN-CRIMINALIZATION.pdf, ultimo accesso il 30 giugno 2025).

essere impiegato dai governi di Stati illiberali per reprimere dissidenti e oppositori all'estero, cosa che peraltro già avviene negli ordinamenti giuridici di diversi Stati[22].

All'esito del negoziato, il contrasto fra il gruppo dei paesi favorevoli a limitare quanto più possibile il novero degli obblighi di incriminazione, sulla scia di quanto già previsto nella Convenzione di Budapest[23], e quello dei paesi favorevoli, invece, ad una estensione del novero di tali obblighi, replicando quanto già avviene – almeno in parte – in altri strumenti regionali[24], si è risolto a favore della posizione sostenuta dal primo gruppo. Il testo finale, infatti, prevede obblighi di incriminazione soltanto di una serie ristretta di crimini «*cyber-dependent*» e di specifici e ben definiti crimini «*cyber-enabled*»[25]. Fra essi, alcuni sono dei crimini che mirano a tutelare la riservatezza e l'integrità di sistemi di informazione e comunicazione, quali – ad esempio – l'accesso illegale a tali sistemi[26], l'intercettazione illegale[27], il danneggiamento, l'alterazione o l'eliminazione di dati[28], la creazione di impedimenti al funzionamento degli anzidetti sistemi[29]. Altri crimini, invece, mirano ad approntare tutela anche a beni diversi, come – ad esempio – quelli concernenti la diffusione *online* di materiale attinente ad abusi sessuali su minori oppure a sfruttamento sessuale di minori[30], la divulgazione non autorizzata di immagini intime[31], e il riciclaggio dei proventi dei reati di cui si è appena detto[32].

Va però notato come il compromesso poc'anzi descritto sia stato accettato dai paesi favorevoli a obblighi di incriminazione più ampi soltanto in considerazione della

---

[22] T. TROPINA, *'This is not a Human Rights Convention!': the Perils of Overlooking Human Rights in the UN Cybercrime Treaty*, in *Journal of Cyber Policy*, 2024, pp. 6-7.

[23] Ibid. La Convenzione di Budapest prevede obblighi di incriminazione ristretti, se paragonata ad alcuni degli altri strumenti internazionali, di cui si è detto *supra*. In effetti, se è chiaro che essa prevede tanto crimini '*cyber-dependent*' quanto crimini '*cyber-enabled'*, è altresì vero che il novero dei secondi è notevolmente limitato (si veda la Sezione 1 del Capitolo II della Convenzione di Budapest).

[24] Alcune convenzioni regionali, infatti, prevedono obblighi di incriminazione più pervasivi e potenzialmente strumentalizzabili, da parte degli Stati, per il perseguimento di dissidenti od oppositori politici. Si consideri, ad esempio, la Convenzione della Lega Araba, la quale – all'art. 15 – prevede per gli Stati degli obblighi di incriminazione – formulati invero in maniera particolarmente generica – concernenti le seguenti condotte: la disseminazione e perorazione di idee e principi di gruppi terroristici; la facilitazione delle comunicazioni fra gruppi terroristici; la disseminazione di fanatismo e discordia religiosa («*religious fanaticism and dissention*»); l'aggressione a credi e religioni. Allo stesso modo, l'art. 29, par. 3, della Convenzione dell'Unione Africana prevede obblighi di incriminazione di crimini che potrebbero anche essere intesi in maniera particolarmente ampia, quali: (i) l'insulto, realizzato tramite un sistema informatico, a persone a motivo del fatto che esse appartengono a un gruppo distinto per razza, colore, discendenza, origine nazionale o etnica, oppure opinione religiosa o politica, «*if used as a pretext for any of these factors*», oppure contro un gruppo di persone distinte sulla base delle anzidette caratteristiche; (ii) la voluta negazione, oppure l'approvazione o la giustificazione, di atti che costituiscono genocidio o crimini contro l'umanità, tramite sistema informatico.

[25] I. TENNANT, A.P. OLIVEIRA, *Applying the Right Lessons from the Negotiation and Implementation of the UNTOC and the UNCAC to the Implementation of the Newly Agreed UN 'Cybercrime' Treaty*, in *Journal of Cyber Policy*, 2025, pp. 228-230.

[26] Art. 7 della Convenzione ONU contro il *cybercrime*.

[27] Art. 8 della Convenzione ONU contro il *cybercrime*.

[28] Art. 9 della Convenzione ONU contro il *cybercrime*.

[29] Art. 10 della Convenzione ONU contro il *cybercrime*.

[30] Art. 14 della Convenzione ONU contro il *cybercrime*.

[31] Art. 16 della Convenzione ONU contro il *cybercrime*.

[32] Art. 17 della Convenzione ONU contro il *cybercrime*.

formulazione, nella stessa risoluzione 79/243, di una sezione in cui espressamente si afferma che il Comitato dovrà continuare i propri lavori al fine di negoziare un protocollo supplementare alla Convenzione «*addressing […] additional criminal offences as appropriate*», il quale sarà discusso nell'ambito della Conferenza degli Stati parte della Convenzione, secondo un calendario ben definito[33]. Non è dunque affatto escluso che, in futuro, il numero degli obblighi di incriminazione possa subire un allargamento, anche significativo, e questa è la ragione alla base delle perduranti preoccupazioni circa la portata degli obblighi di incriminazione.

4. La complessa delimitazione dell'ambito di esercizio della giurisdizione penale fra gli Stati

Altre questioni della Convenzione meritevoli di analisi possono essere rinvenute nella disposizione che disciplina l'ambito di esercizio della giurisdizione penale domestica, ossia l'art. 22. Seguendo il modello di altre convenzioni internazionali volte a contrastare specifici crimini, quale ad esempio la Convenzione di Palermo contro il crimine organizzato transnazionale («Convenzione di Palermo»)[34], la Convenzione prevede che ciascuno degli Stati parte *debba* introdurre nel proprio ordinamento nazionale tutte le misure necessarie per l'esercizio della giurisdizione penale quando il crimine sia stato commesso nel proprio territorio[35]. In aggiunta, la stessa disposizione prevede che l'autorità giudiziaria di ciascuno Stato abbia *facoltà* di perseguire un crimine quando esso sia stato commesso contro un cittadino di tale Stato[36], oppure da un cittadino di tale Stato, ovvero da un apolide con residenza abituale in esso[37], nonché – in ogni caso – per perseguire crimini che siano stati commessi contro tale Stato[38]. Al contempo, l'art. 22 prevede che ogni eventuale esercizio *facoltativo* della giurisdizione penale debba avvenire nel rispetto di quanto previsto all'art. 5 della Convenzione. Quest'ultimo dispone che gli Stati parte della Convenzione debbano adempiere agli obblighi derivanti da essa in piena conformità ai principi di eguaglianza sovrana, di integrità territoriale degli altri Stati e di non intervento negli affari interni di questi ultimi[39]. Inoltre, è ivi previsto che nulla nella Convenzione potrà legittimare uno Stato a esercitare, nel territorio

[33] Cfr. il paragrafo 5 della risoluzione 79/243, cit., ove è precisato che «*two sessions of a duration of 10 days each, with the first session taking place two years after the adoption of the Convention by the General Assembly and the second session in the following calendar year, in Vienna and New York, respectively, shall be convened for the purpose of submitting the outcomes to the Conference of the States Parties to the Convention, for its consideration and further action in accordance with articles 57, paragraph 5 (g), 61 and 62 of the Convention*». Sulle prerogative della Conferenza degli Stati parte della Convenzione, cfr. *infra* nota 94.
[34] Si veda l'art. 15 della Convenzione di Palermo.
[35] Art. 22, par. 1, della Convenzione ONU contro il *cybercrime*.
[36] Art. 22, par. 2, lett. a), della Convenzione ONU contro il *cybercrime*.
[37] Art. 22, par. 2, lett. b), della Convenzione ONU contro il *cybercrime*.
[38] Art. 22, par. 2, lett. d), della Convenzione ONU contro il *cybercrime*.
[39] Art. 5, par. 1, della Convenzione ONU contro il *cybercrime*.

di un altro, competenze e funzioni che sono riservate in via esclusiva alle autorità di quest'ultimo, secondo quando previsto dal diritto interno di tale Stato[40].

Se una siffatta norma sulla tutela della sovranità è analoga a quelle inserite in altre convenzioni internazionali volte a contrastare specifici crimini, quale l'art. 4 della Convenzione di Palermo[41], gli effetti giuridici di tali disposizioni potrebbero però sembrare tutto sommato modesti, nella misura in cui esse si limitano a riaffermare l'applicazione di principi comunque già vigenti secondo il diritto internazionale generale. Tale considerazione sembrerebbe peraltro suffragata da quanto affermato dalla Corte internazionale di giustizia nella sentenza sulle obiezioni preliminari del 2018 nell'affare delle *Immunità e procedimenti penali*, fra Guinea Equatoriale e Francia. In quella sede, infatti, la CIG ha escluso che il riferimento al principio di eguaglianza sovrana fra gli Stati, operato nell'art. 4 della Convenzione di Palermo, potesse essere ricostruito come idoneo ad incorporare nel trattato le norme di diritto internazionale generale sull'immunità degli Stati e dei loro organi, come invece sosteneva la Guinea Equatoriale[42]. Da un punto di vista più generale, il giudice Abraham aveva affermato, nella sua opinione separata, che disposizioni pattizie – quali l'art. 4 della Convenzione di Palermo – debbono essere intese come mere «clausole di salvaguardia», le quali – in generale – né ambiscono a creare obblighi convenzionali per le parti del trattato, né hanno l'effetto di incorporare in esso preesistenti norme di diritto consuetudinario[43].

Nel contesto specifico della Convenzione sul *cybercrime*, tuttavia, l'introduzione della norma di «salvaguardia» della sovranità statuale dovrebbe essere intesa, a parere dello scrivente, come volta a impedire, o comunque ad ostacolare, qualsivoglia interpretazione delle norme convenzionali che possa legittimare interlocuzioni fra l'autorità giudiziaria di uno Stato e attori privati, quali *service provider*, siti in altri Stati, come già può avvenire sulla base del menzionato art. 32 della Convenzione di Budapest[44].

Da ultimo, va segnalato come anche la Convenzione in esame preveda un meccanismo non del tutto idoneo ad assicurare un efficace riparto fra l'esercizio dei poteri giudiziari fra due o più Stati, allorché in essi, per gli stessi fatti, siano stati instaurati diversi procedimenti penali. Infatti, l'art. 22 si limita ad affermare che in questo caso gli

---

[40] Art. 5, par. 2, della Convenzione ONU contro il *cybercrime*.

[41] In generale, cfr. F. CALDERONI, *Article 4 – Protection of Sovereignty*, in A. SCHLOENHARDT, F. CALDERONI, J. LELLIOT, B. WEIßER (a cura di), *UN Convention against Transnational Organized Crime. A Commentary*, Oxford, 2023, pp. 53-54.

[42] Corte internazionale di giustizia, sentenza del 6 giugno 2018, *Immunities and Criminal Proceedings (Equatorial Guinea v. France)*, *I.C.J. Reports 2018*, p. 322, par. 98.

[43] Ibid., Opinione Separata del giudice Abraham, pp. 376-377, par. 14.

[44] È questa, peraltro, la posizione sostenuta dalla Cina, sin dall'inizio del negoziato nell'ambito del Comitato (cfr. Nazioni Unite, *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Compilation of views submitted by Member States on the scope, objectives and structure (elements) of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, A/AC.291/4, p. 16: «*[c]ross-border collection of electronic evidence is necessary for combating the use of ICT for criminal purposes, but Member States should respect the sovereignty of the State where the evidence is located. […] States should not directly collect data housed by enterprises or individuals in foreign States or by using technical means that bypass network security protection measures if such means infringe the law of that foreign State*»).

Stati coinvolti sono tenuti a consultarsi, «per quanto ritengano appropriato», al fine di coordinare le loro azioni[45]. Tale disposizione replica nella sostanza quanto già previsto nella Convenzione di Palermo, dove – come è noto – non si è riusciti a formulare un principio di *ne bis in idem* transnazionale, né ad introdurre regole specifiche idonee a istituire una gerarchia fra gli Stati potenzialmente intenzionati a instaurare un procedimento penale per gli stessi fatti[46]. Se già in quelle convenzioni tale assenza era problematica, nella Convenzione contro il *cybercrime* essa rischia di esserlo ancora di più, in considerazione delle sfide poste dal crimine cibernetico al principio di territorialità[47], con la conseguenza che numerosi Stati potrebbero instaurare procedimenti penali per i medesimi fatti. Oltre all'eventuale sperpero di risorse processuali, ciò non è indifferente sol che si considerino i diversi strumenti, di cui si dirà appena *infra*, che la stessa Convenzione mette a disposizione dei giudici nazionali nello svolgimento delle loro attività di indagine.

5. Le misure di cooperazione giudiziaria internazionale previste dalla Convenzione

Al di là della previsione di obblighi di incriminazione, la Convenzione prevede altresì corposi obblighi concernenti la cooperazione giudiziaria internazionale[48]. È utile segnalare come tali obblighi di cooperazione non siano previsti soltanto per il perseguimento dei reati tipici, di cui si è detto *supra*, bensì anche per il perseguimento di quelli che la stessa Convenzione definisce come «gravi crimini» («*serious crimes*»)[49]. Il problema, tuttavia, è che la definizione del concetto di grave crimine è unilateralmente rimessa dalla Convenzione alla legislazione nazionale dei singoli Stati: secondo l'art. 2, par. 1, lett. h), infatti, è crimine grave ogni condotta che costituisca un reato punibile con una privazione massima della libertà personale di almeno quattro anni, o punita con una sanzione più grave[50]. Tale circostanza, unita al notevole numero e, soprattutto, alla notevole pervasività dei mezzi di cooperazione giudiziaria, ha indotto taluni a credere che essi costituiscano un potenziale pericolo per i diritti e le libertà degli individui, siti

[45] Art. 22, par. 5, della Convenzione ONU contro il *cybercrime*.
[46] B. WEIßER, *Article 15 – Jurisdiction*, in A. SCHLOENHARDT, F. CALDERONI, J. LELLIOT, B. WEIßER (eds.), *UN Convention against Transnational Organized Crime*, cit., p. 153.
[47] Per una panoramica generale sull'esercizio della giurisdizione degli Stati in rapporto a crimini commessi nel dominio cibernetico, cfr. F. STAIANO, *Transnational Organized Crime. Challenging International Law Principles on State Jurisdiction*, Cheltenham - Northampton, 2022, p. 60 ss. Inoltre, cfr. A. SEGURA SERRANO, *Cybersecurity and Cybercrime*, cit., p. 718 ss.
[48] Si veda il Capitolo V, artt. 35 ss., della Convenzione ONU contro il *cybercrime*.
[49] L'art. 35, par. 1, prevede che «*States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters, and domestic laws, for the purpose of: […] c) The collecting, obtaining, preserving and sharing of evidence in electronic form of any serious crime, including serious crimes established in accordance with other applicable United Nations conventions and protocols in force at the time of the adoption of this Convention*».
[50] L'art. 2, par. 1, lett. h), della Convenzione ONU contro il *cybercrime* prevede che: «*"Serious crime" shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penality*».

all'estero, interessati dall'uso di tali mezzi[51]. Sul punto, tuttavia, conviene evidenziare come la Convenzione preveda almeno quattro presidi volti a scongiurare tale pericolo.

In primo luogo, l'art. 40, par. 8, della Convenzione attribuisce a ciascuno Stato la facoltà di invocare l'assenza di doppia incriminazione quale motivo per rifiutare una richiesta di assistenza giudiziaria, come già previsto – peraltro – dall'art. 32, par. 5, della Convenzione del Cairo[52], e – in maniera meno generale – dall'art. 25, par. 5, della Convenzione di Budapest[53]. Tale presidio nella Convenzione ONU, tuttavia, sembra in qualche modo indebolito, o comunque reso meno incisivo, da quanto previsto nella parte immediatamente successiva dell'art. 40, par. 8, ossia che lo Stato richiesto, quando lo reputi appropriato, possa comunque dare seguito alla richiesta di assistenza giudiziaria, e ciò a prescindere dal fatto che la condotta per la quale è richiesta assistenza costituisca un reato punibile nello Stato richiesto[54].

Un secondo presidio è approntato dall'art. 40, par. 21, lett. c), della Convenzione. Secondo questa disposizione, una richiesta di assistenza giudiziaria può essere rifiutata nel caso in cui il diritto interno dello Stato richiesto vieterebbe alle sue autorità di adottare le misure richieste, qualora si trattasse di un reato analogo oggetto di un'indagine, di un procedimento penale o di un procedimento giudiziario nell'ambito della propria giurisdizione. Tale estensione delle garanzie domestiche alle richieste di assistenza giudiziaria sembra essere in qualche modo una rielaborazione di quanto già previsto da alcune convenzioni regionali. Così, l'art. 8, par. 1, della Convenzione di Minsk ammette la possibilità di rifiutare una richiesta di assistenza ove l'esecuzione di questa risulti in contrasto con l'ordinamento dello Stato richiesto[55]. In maniera forse meno incisiva, l'art. 25, par. 4, della Convenzione di Budapest prevede che, salvo che sia diversamente previsto, le misure di assistenza debbano essere assoggettate alle condizioni previste dal

[51] T. TROPINA, *'This is not a Human Rights Convention!'*, cit., p. 15: «*It is not uncommon to use criminal law to oppress freedom of expression, freedom of assembly and other human rights. Many such offences in different national laws would easily fall under the definition of serious crime […]. Even if they didn't, nothing prevents a state from raising the punishment for such crimes to meet the threshold*».

[52] L'art. 32, par. 5, della Convenzione della Lega Araba dispone che: «*[w]henever the State Party from which assistance is requested may provide such assistance only in the presence of dual criminality, this condition shall be considered fulfilled regardless of whether the laws of the State Party classify the offence in the same category as those of the requesting State Party, provided that the act leading to the offence in respect of which assistance is requested is considered an offence according to the laws of the State Party*».

[53] L'art. 25, par. 5, della Convenzione di Budapest prevede che «*[w]here, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws*».

[54] L'art. 40, par. 8, prevede poi la facoltà di rifiutare una richiesta di cooperazione quando essa abbia ad oggetto questioni *de minimis* oppure quando l'assistenza richiesta possa essere ottenuta sulla base di altre disposizioni della Convenzione medesima. Si noti, peraltro, che alcuni degli strumenti giuridici disciplinati dal Capitolo V della Convenzione prevedono sempre e comunque l'applicazione della regola della doppia incriminazione (come, ad esempio, l'art. 37 in materia di estradizione).

[55] L'art. 8, par. 1, della Convenzione di Minsk, prevede che «*[e]xecution of a request within the framework of this Agreement may be refused in part or in whole if the requested Party considers that such execution would be contrary to its national legislation*».

diritto interno dello Stato destinatario della richiesta o da trattati in vigore fra i due Stati, ivi inclusi i motivi di rifiuto della richiesta di assistenza[56]. Un'analoga disposizione è altresì prevista dalla Convenzione del Cairo (art. 32, par. 4)[57].

Un terzo presidio è approntato dall'art. 40, par. 22, ove si dispone che nulla nella Convenzione potrà essere inteso come implicante l'obbligo di assicurare assistenza giudiziaria quando l'autorità dello Stato richiesto abbia *fondati elementi* per ritenere che la richiesta sia stata formulata con l'obiettivo di perseguire o punire una persona sulla base del suo genere, razza, lingua, religione, nazionalità, origine etnica o per le sue opinioni politiche, oppure che l'evasione della richiesta possa recare pregiudizio alla posizione di tale persona per alcuno degli anzidetti motivi. Al di là del fatto che l'espressione «fondati elementi» sembra presentare notevoli difficoltà definitorie, e dunque applicative, tale salvaguardia va letta in combinato disposto con quanto già previsto, a titolo generale, dall'art. 6 della Convenzione. Quest'ultimo, su cui comunque si tornerà *infra*, dispone che nell'eseguire gli obblighi derivanti dalla Convenzione, gli Stati debbano conformarsi agli obblighi assunti dagli Stati in materia di diritti umani[58], e che – in nessun modo – la Convenzione potrà essere intesa quale strumento di soppressione dei diritti umani e delle libertà fondamentali[59].

Il riferimento alla necessità che l'esecuzione di richieste di cooperazione giudiziaria sulla base dello strumento pattizio non rechi pregiudizio a diritti umani e libertà fondamentali non è una novità nel panorama delle convenzioni regionali sul contrasto al *cybercrime*. È senz'altro vero che in alcune di esse, come ad esempio nell'art. 4 della Convenzione di Ekaterinburg, il rispetto dei diritti umani viene menzionato soltanto incidentalmente, insieme ad altri principi e norme, quali il divieto di uso della forza o il divieto di interferenza negli affari interni[60]. Tuttavia, altre convenzioni contengono disposizioni molto più elaborate e incisive rispetto all'obiettivo di tutela dei diritti umani. Così, l'art. 25, par. 3, della Convenzione di Malabo dispone in via generale che, nell'adottare misure per la cybersicurezza e nello stabilire il regime normativo per la loro implementazione, gli Stati siano obbligati a non violare i diritti dei cittadini, così come garantiti non solo dalle costituzioni nazionali e dagli ordinamenti giuridici interni, bensì

[56] L'art. 25, par. 4, della Convenzione di Budapest prevede che «*[t]he requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence*».

[57] L'art. 32, par. 4, della Convenzione del Cairo dispone che: «*[e]xcept as otherwise stated in this chapter, bilateral assistance shall be subject to the requirements set forth in the law of the State Party from which assistance is requested or in mutual assistance treaties, including the grounds on which the State Party can rely to refuse cooperation*».

[58] Art. 6, par. 1, della Convenzione ONU contro il *cybercrime*.

[59] Art. 6, par. 2, della Convenzione ONU contro il *cybercrime*.

[60] L'art. 4 della Convenzione di Ekaterinburg dispone che «*[t]he Parties shall cooperate and their activities in the international information space in the framework of this Agreement shall be carried out in such a way that these activities contribute to social and economic development and are compatible with objectives of maintaining international security and stability, consistent with universally recognized principles and norms of the international law, including the principles of peaceful settlement disputes and conflicts, non-use of force, non-interference in internal affairs, respect for human rights and fundamental freedoms, as well as the principles of regional cooperation and noninterference in the information resources of the Parties*».

anche dagli strumenti giuridici internazionali, quale la Carta Africana sui diritti umani e dei popoli. Specificamente in rapporto alle misure di cooperazione giudiziaria, l'art. 27 della Convenzione di Budapest prevede che, al di là di quanto previsto dall'art. 25, par. 4, di cui già si è detto *supra*, ciascuno Stato possa rifiutare una richiesta di assistenza nel caso in cui questi ritenga che la richiesta si riferisca a un «*political offence*» o a un «*offence connected with a political offence*». Un'analoga disposizione, ossia l'art. 35, è prevista nella Convenzione del Cairo[61].

Un quarto e ultimo presidio è previsto all'art. 36 della Convenzione, mirante a tutelare i dati personali individuali coinvolti nell'esecuzione delle misure di cooperazione giudiziaria. È interessante notare come la disposizione in esame, dopo aver affermato che il trasferimento dei dati personali dovrà avvenire secondo quanto previsto dal diritto interno dello Stato da cui i dati provengono e, in ogni caso, nel rispetto degli eventuali obblighi di diritto internazionale esistenti per tale Stato, preveda che gli Stati parte della Convenzione non siano tenuti al trasferimento di dati, quando ciò non sia conforme alle loro normative nazionali in materia di dati personali[62]. In ogni caso, la medesima disposizione prevede che lo Stato richiesto, al fine di dare seguito ad una richiesta di trasferimento di dati personali, possa esigere il rispetto di specifiche condizioni volte a rendere lecito il trasferimento, secondo il proprio diritto interno[63]. Inoltre, la Convenzione manifestamente incoraggia la conclusione di trattati bilaterali o multilaterali, volti a facilitare il trasferimento di dati personali[64]. Il medesimo art. 36, infine, dispone che il trasferimento verso uno Stato terzo di dati, ricevuti da un altro Stato in esecuzione di una richiesta di cooperazione, possa avvenire soltanto con l'autorizzazione espressa da parte di quest'ultimo[65].

L'introduzione di una disposizione espressamente volta ad assicurare tutela ai dati personali degli individui interessati da misure di assistenza giudiziaria non è una novità assoluta, giacché l'art. 14 del Secondo Protocollo alla Convenzione di Budapest, non ancora entrato in vigore, mira proprio a realizzare questo fine[66]. Sebbene non sia possibile

[61] L'art. 35 della Convenzione del Cairo dispone che «*[…] the State Party from which assistance is requested may refuse assistance if: 1. The request relates to an offence that the law of the State Party from which assistance is requested considers as a political offence*».
[62] Art. 36, par. 1, lett. a), della Convenzione ONU contro il *cybercrime*.
[63] Art. 36, par. 1, lett. b), della Convenzione ONU contro il *cybercrime*.
[64] Art. 36, par. 1, lett. c), della Convenzione ONU contro il *cybercrime*.
[65] Art. 36, par. 3, della Convenzione ONU contro il *cybercrime*.
[66] Conviene evidenziare come le materie oggetto del Secondo Protocollo alla Convenzione di Budapest siano state oggetto di una pluralità di atti di diritto derivato dell'Unione europea (cfr. Decisione (UE) 2022/722 del Consiglio del 5 aprile 2022 che autorizza gli Stati membri a firmare, nell'interesse dell'Unione europea, il secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche; Decisione (UE) 2023/436 del Consiglio del 14 febbraio 2023 che autorizza gli Stati membri a ratificare, nell'interesse dell'Unione europea, il secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche), e questo in virtù del fatto che «[l]e disposizioni del protocollo rientrano in un settore disciplinato in larga misura da norme comuni ai sensi dell'articolo 3, paragrafo 2, del trattato sul funzionamento dell'Unione europea (TFUE), compresi gli strumenti che agevolano la cooperazione giudiziaria in materia penale, garantendo norme minime in

dare dettagliatamente conto del contenuto di tale ultima disposizione citata, basti notare come essa contenga pervasive prescrizioni per assicurare *inter alia* (i) che i dati trasmessi da uno Stato ad un altro siano trattati per la realizzazione delle finalità previste[67], (ii) che l'utilizzo dei dati personali sensibili non provochi un pregiudizio ingiustificato nei confronti della persona cui essi si riferiscono[68], (iii) che il ricorso a decisioni automatizzate sia limitato[69], (iv) che la trasmissione di dati personali a Stati terzi possa avvenire solamente su autorizzazione dell'autorità dello Stato di origine di tali dati[70]. Secondo un'impostazione diversa, le altre convenzioni regionali contengono disposizioni per salvaguardare la «*confidentiality*» dei dati trasmessi, ma soltanto nell'ottica di evitare un pregiudizio allo Stato destinatario della richiesta oppure a eventuali indagini che le sue autorità stiano conducendo[71].

In considerazione di quanto si è detto, è evidente come un ruolo chiave nel ricorso ai presidi introdotti dalla Convenzione ONU sarà giocato anzitutto dai giudici nazionali, i quali saranno direttamente chiamati a valutare richieste di assistenza giudiziaria provenienti da colleghi di altri Stati. Come già notato in dottrina, le preoccupazioni legate alla potenziale violazione di diritti umani potranno e dovranno dunque essere affrontate dalle autorità giudiziarie nazionali, sulle quali graverà l'onere di evitare che la Convenzione possa essere impiegata come strumento lesivo di diritti e libertà individuali fondamentali[72].

6. La previsione di ulteriori misure procedurali particolarmente invasive

Il Capitolo IV della Convenzione (articoli 23 e ss.) vincola gli Stati a introdurre nei loro ordinamenti nazionali una serie di misure procedurali volte a consentire, o comunque facilitare, specifiche indagini, in maniera analoga a quanto già previsto nella Convenzione di Budapest. Fra queste misure, spiccano la «conservazione accelerata di dati elettronici» (art. 25), la «conservazione e divulgazione parziale di dati di traffico» (art. 26), «la ricerca e il sequestro di dati elettronici» (art. 28), e la «raccolta in tempo reale di dati di traffico»

materia di diritti processuali e garanzie in merito alla protezione dei dati e alla riservatezza» (cfr. Decisione (UE) 2022/722 del Consiglio del 5 aprile 2022, cit., Considerando 3). Per una incisiva analisi critica sui potenziali profili di incompatibilità fra le norme del Secondo protocollo e la normativa dell'UE in materia di trattamento dei dati personali, cfr. M. BUCCARELLA, *Digitalizzazione della cooperazione giudiziaria internazionale in materia penale e tutela dei dati personali nel diritto dell'UE: alla ricerca di una compatibilità (im)possibile*, in questa *Rivista*, 2023, p. 229 ss.

[67] Art. 14, par. 2, del Secondo Protocollo alla Convenzione di Budapest.

[68] Art. 14, par. 4, del Secondo Protocollo alla Convenzione di Budapest.

[69] Art. 14, par. 6, del Secondo Protocollo alla Convenzione di Budapest.

[70] Art. 14, par. 10, del Secondo Protocollo alla Convenzione di Budapest.

[71] Art. 28, par. 2, della Convenzione di Budapest; art. 36, par. 2, della Convenzione del Cairo; art. 6 della Convenzione di Ekaterinburg; art. 9 della Convenzione di Minsk.

[72] Secondo A. BALSAMO, *Spazio virtuale e processo penale: la nuova Convenzione ONU sul cybercrime*, in *Diritto penale e processo*, 2025, p. 244: «[…] i timori legati alla nuova Convenzione potranno trovare una efficace risposta soltanto attraverso la decisa valorizzazione del ruolo della giurisdizione, che appare insostituibile per garantire un giusto equilibrio tra tutti i diritti fondamentali coinvolti».

(art. 29)[73]. Poiché tali misure possono significativamente impattare sulla sfera di riservatezza degli individui, già nella Convenzione di Budapest era stata introdotta in rapporto ad esse una disposizione di salvaguardia, l'art. 15, notevolmente più incisiva dell'art. 27 – già descritto *supra* – applicabile alle misure di cooperazione giudiziaria.

Invero, l'art. 15 della Convenzione di Budapest prevede che l'implementazione e l'applicazione da parte degli Stati delle summenzionate misure e procedure concernenti i dati di traffico debba avere luogo non solo nel rispetto delle condizioni e delle salvaguardie previste nel diritto interno, bensì anche che tale diritto interno *debba* assicurare tutela adeguata ai diritti umani e alle libertà fondamentali, inclusi i diritti derivanti dalla Convenzione europea dei diritti umani, dal Protocollo sui diritti civili e politici, e dagli altri strumenti internazionali in materia di diritti umani. È poi opportuno notare come l'art. 15 prescriva altresì che, oltre a dover osservare diritti umani e libertà fondamentali, il diritto interno debba prevedere l'incorporazione del principio di proporzionalità (par. 1)[74], e che le condizioni e salvaguardie previste da tale diritto debbano includere – «*as appropriate in view of the nature of the procedure or power concerned*» – meccanismi di controllo giurisdizionale (o altra forma di controllo indipendente), l'identificazione di motivi che giustifichino l'applicazione delle misure in questione e la limitazione della portata e della durata di esse (par. 2).

Si è convincentemente affermato come l'art. 15 della Convenzione di Budapest incorpori quei principi che sono usualmente applicati dalla Corte europea dei diritti dell'uomo («Corte EDU») nel valutare eventuali violazioni dell'art. 8 della Convenzione europea sul diritto al rispetto della vita privata e familiare[75]. Senza che sia possibile in questa sede esplorare la corposa giurisprudenza della Corte EDU in materia[76], va rammentato come da lungo tempo essa abbia riconosciuto la «fondamentale importanza» della protezione dei dati personali ai fini del godimento del diritto di cui all'art. 8, affermando la necessità che il diritto nazionale appronti adeguate salvaguardie contro un uso improprio di tali dati, soprattutto quando questi ultimi siano assoggettati a trattamenti

[73] L'art. 25 della Convenzione ONU replica quanto previsto nell'art. 16 della Convenzione di Budapest («*Expedited preservation of stored computer data*»); l'art. 26 della Convenzione ONU replica quanto previsto nell'art. 17 della Convenzione di Budapest («*Expedited preservation and partial disclosure of traffic data*»); l'art. 28 della Convenzione ONU replica quanto previsto nell'art. 19 della Convenzione di Budapest («*Search and seizure of stored computer data*»); l'art. 29 della Convenzione ONU replica quanto previsto nell'art. 20 della Convenzione di Budapest («*Real-time collection of traffic data*»); infine, l'art. 30 della Convenzione ONU replica quanto previsto nell'art. 21 della Convenzione di Budapest («*Interception of content data*»).

[74] Sul punto, cfr. S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, pp. 262-267. In generale, può dirsi che un atto investigativo informatico sia conforme al principio di proporzionalità quando: (i) è idoneo a raggiungere lo scopo previsto dalla norma che lo prevede; (ii) è necessario a raggiungere quello scopo; (iii) il sacrificio richiesto all'individuo destinatario dell'atto è giustificabile rispetto alla repressione del reato.

[75] L. TOSONI, *Rethinking Privacy in the Council of Europe's Convention on Cybercrime*, in *Computer Law & Security Review*, 2018, p. 1206. Tali principi sono quelli di (i) legalità e liceità, (ii) finalità legittima, (iii) necessità e (iv) proporzionalità.

[76] Cfr. Organization for Security and Co-operation in Europe (OSCE), *Ensuring Human Rights Compliance in Cybercrime Investigations*, Vienna, 2023, p. 26 ss.

automatizzati, anche da parte di forze di polizia[77]. In diversi casi, dunque, la Corte EDU ha condannato lo Stato convenuto per aver implementato meccanismi di sorveglianza segreta, in assenza di adeguate garanzie contro il rischio di arbitrarietà e abusi[78]. È peraltro interessante notare come la violazione dell'art. 8 sia stata ravvisata anche per mancanza di chiarezza della normativa nazionale, così come applicata dai giudici interni, sull'acquisizione da parte di forze di polizia di «*subscriber information*» associate a indirizzi IP dinamici, e per mancanza in tale normativa di sufficienti salvaguardie contro interferenze arbitrarie[79].

Va altresì segnalato come il ricorso a strumenti informatici da parte delle autorità nazionali per la repressione dei crimini possa portare anche alla violazione dell'art. 6 della Convenzione europea sul diritto all'equo processo. Si pensi, giusto a titolo di esempio, al caso *Yüksel Yalçinkaya c. Turchia*, deciso nel 2023[80]: i giudici turchi avevano condannato il ricorrente per aver partecipato al tentato golpe in Turchia nel luglio del 2016, e questo esclusivamente sulla base del mero utilizzo – da parte sua – di una applicazione («*ByLock*»), documentato da ingente materiale probatorio informatico raccolto dall'accusa[81]. I giudici turchi avevano rifiutato la richiesta della difesa di accedere a tale materiale probatorio. Per la Corte, un siffatto rifiuto – di per sé non illegittimo – avrebbe dovuto però essere bilanciato dal ricorso ad altre misure idonee a garantire la complessiva equità del procedimento, cosa non avvenuta nel caso di specie[82].

Alla luce di quanto si è detto, non sorprende, dunque, che anche la Convenzione ONU, in rapporto alle misure procedurali anzidette, preveda una disposizione di salvaguardia, ossia l'art. 24, analoga all'art. 15 della Convenzione di Budapest. Riprendendo quanto già previsto in quest'ultima disposizione, l'art. 24 afferma che l'esercizio dei poteri e delle procedure di cui al Capitolo IV debba essere assoggettato al rispetto delle condizioni e delle salvaguardie previste dal diritto nazionale, «*which shall provide for the protection of human rights, in accordance with its obligations under international human rights law, and which shall incorporate the principle of*

[77] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 4 dicembre 2008, ricorsi nn. 30562/04 e 30566/04, *S. e Marper c. Regno Unito*, par. 103.
[78] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 4 dicembre 2015, ricorso n. 47143/06, *Roman Zakharov c. Russia*, par. 302; Corte europea dei diritti dell'uomo, Quarta Sezione, sentenza del 12 gennaio 2016, ricorso n. 37138/14, *Szabó e Vissy c. Ungheria*, par. 89.
[79] Corte europea dei diritti dell'uomo, Quarta Sezione, sentenza del 24 aprile 2018, ricorso n. 62357/14, *Benedik c. Slovenia*, par. 132-133.
[80] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 26 settembre 2023, ricorso n. 15669/20, *Yüksel Yalçinkaya c. Turchia*.
[81] L'applicazione ByLock, secondo gli stessi giudici turchi, era stata creata con l'esclusivo scopo di consentire ai membri del gruppo FETÖ/PDY, responsabile del tentato golpe, di comunicare fra loro (ibid., par. 87), e il suo utilizzo da parte del ricorrente era stato ricostruito anche grazie alle attività dei servizi di intelligence turca, che – nei primi mesi del 2016 – avevano acceduto abusivamente ai server di ByLock, siti in Lituania, e da lì avevano estratto gli indirizzi IP di coloro che si erano collegati al server (ibid., par. 21).
[82] Corte europea dei diritti dell'uomo, Grande Camera, *Yüksel Yalçinkaya*, cit., par. 329 ss. Per un'analisi esaustiva, cfr. R. PRETTATO, *Digitalizzazione e giusto processo: la* digital evidence *nella giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in *DPCE online*, 2024, p. 728 ss.

proportionality» (par. 1)[83]. La stessa disposizione riproduce poi l'obbligo di introdurre le stesse cautele di cui all'art. 15, par. 2, della Convenzione di Budapest, precisando però che esso debba essere adempiuto «*in accordance with and pursuant to the domestic law of each State Party*» (par. 2)[84].

Giova formulare alcune considerazioni sul rapporto fra l'art. 15 della Convenzione di Budapest e l'art. 24 della Convenzione ONU. Come già è stato notato da un autorevole commentatore, mentre il primo si rivolge a un gruppo ben definito di Stati, i quali condividono valori e strutture normative, il secondo coinvolgerà Stati in rapporto ai quali vi è «minore omogeneità delle rispettive strutture costituzionali e dei principi ispiratori dei rispettivi ordinamenti giuridici», con la conseguenza che «disposizioni identiche [potranno] essere applicate in modo profondamente diverso nei vari ordinamenti»[85]. Per questo, anche in rapporto all'implementazione delle misure e delle procedure di cui al Capitolo IV della Convenzione ONU va ribadito quanto già si è precedentemente sostenuto in rapporto all'applicazione delle norme in materia di cooperazione giudiziaria: nell'applicazione della Convenzione, un ruolo decisivo sarà senz'altro svolto dai giudici nazionali, i quali saranno chiamati – auspicabilmente – a sviluppare un approccio comune e rispettoso dei diritti fondamentali e delle libertà individuali. A questo va aggiunta la messa a disposizione da parte della Convenzione ONU di un significativo armamentario di strumenti di cooperazione, su cui non è possibile soffermarsi in questa sede, che ambiscono ad accrescere lo sviluppo delle capacità tecniche e organizzative degli Stati meno tecnologicamente avanzati e strutturati[86].

[83] Va altresì notato come la Convenzione ONU, al par. 4 dell'art. 24, preveda che tutte salvaguardie di cui all'art. 24 debbano trovare applicazione alle «*procedural measures and law enforcement*» sia quando esse siano implementate nell'ambito di indagini penali a livello domestico sia quando siano applicate nell'ambito delle iniziative di cooperazione giudiziaria internazionale.

[84] Particolarmente critico in ordine al rinvio al diritto nazionale è F. SEATZU, *The New UN Convention on Cybercrime: between Securing Cyberspace and Undermining Fundamental Rights and Freedoms*, in *La Comunità internazionale*, 2025, pp. 233-236.

[85] A. BALSAMO, *Spazio virtuale e processo penale*, cit., pp. 246-247.

[86] Ad esempio, l'art. 54 della Convenzione ONU prevede che gli Stati debbano, «*according to their capacity*», prestarsi l'un l'altro il massimo dell'assistenza tecnica possibile, ivi compreso lo scambio di esperienza e conoscenza tecnica e il trasferimento tecnologico, prendendo in considerazione gli interessi e le necessità degli Stati in via di sviluppo (par. 1). La medesima disposizione, poi, vincola alla cooperazione fra gli Stati e fra Stati e organizzazioni internazionali e regionali, organizzazioni non-governative, società civile, accademia e entità del settore privato, al fine di rafforzare l'implementazione della Convenzione (par. 4). Inoltre, gli Stati dovranno rafforzare gli sforzi per massimizzare l'effettività dell'assistenza tecnica e del «*capacity-building*» nell'ambito di organizzazioni regionali e internazionali e nel contesto di rilevanti accordi bilaterali o multilaterali (par. 8). L'art. 55 della Convenzione ONU disciplina meccanismi facoltativi di condivisione di dati e informazioni sulla criminalità informatica di cui gli Stati siano in possesso, nonché degli esiti della loro valutazione circa l'efficacia delle misure assunte per combattere il crimine cibernetico. L'art. 56 incoraggia gli Stati a fare gli sforzi necessari per rafforzare l'assistenza finanziaria e l'assistenza tecnica a favore degli altri Stati, soprattutto quelli in via di sviluppo.

7. Il ruolo degli Stati nella vigilanza sull'interpretazione e applicazione della Convenzione e l'assenza di disposizioni volte a disciplinare una loro diretta responsabilità per attacchi cibernetici

Si è sin qui notato come le disposizioni di salvaguardia già analizzate, ossia l'art. 6 (di applicazione generale, da osservare in rapporto a qualsiasi atto applicativo della Convenzione), l'art. 24 (disposizione da rispettare nell'esercizio delle misure procedurali) e l'art. 40 (disposizione cui attenersi nell'esecuzione di iniziative di cooperazione giudiziaria internazionale) costituiscano degli strumenti «passivi» nelle mani dei giudici nazionali per impedire che tanto gli Stati cui essi appartengono quanto gli Stati da cui provengano richieste di assistenza possano impiegare la Convenzione ONU quale strumento per recare pregiudizio a diritti umani individuali e libertà fondamentali.

Al tempo stesso, tuttavia, va notato come i richiami, formulati negli articoli 6 e 24, al diritto internazionale dei diritti umani, nonché la menzione nell'art. 40 della necessità di evitare che misure di cooperazione internazionale possano perseguire finalità discriminatore e repressive, possano essere inquadrate anche come strumento «proattivo», su cui gli Stati possono fare leva per indurre Stati non particolarmente attenti al rispetto dello Stato di diritto a rendere il proprio ordinamento interno maggiormente rispettoso dei diritti individuali.

Così, si è già detto che l'art. 6 prevede che «gli Stati parte *dovranno* far sì che l'esecuzione dei loro obblighi discendenti dalla Convenzione avvenga in conformità con i loro obblighi ai sensi del diritto internazionale dei diritti umani». Certo, è difficile affermare che tale norma abbia l'effetto di incorporare nell'ambito di applicazione *ratione materiae* della Convenzione ONU le norme internazionali sui diritti umani, quali quelle incluse nel Patto internazionale sui diritti civili e politici, che menziona e tutela, fra gli altri, tanto la libertà di pensiero, coscienza e religione[87], quanto il diritto di associazione[88]. Tuttavia, nel caso in cui uno Stato – col pretesto di adeguare la propria legislazione nazionale alla Convenzione – ponesse in essere le condizioni per un utilizzo strumentale di essa, oppure nel caso in cui uno Stato decidesse di mantenere nel proprio ordinamento processuale disposizioni che possano essere utilizzate dai giudici nazionali in modo contrastante con l'art. 6 della Convenzione ONU, ecco che qualsiasi altro Stato parte della Convenzione potrebbe lamentare la violazione di quest'ultima.

Ancora più intenso sembra l'obbligo discendente dall'art. 24 della Convenzione. Come già si è ricordato sopra, esso prevede che gli Stati, nell'implementare le misure procedurali di cui al Capitolo IV della Convenzione, non solo debbano osservare gli obblighi derivanti dal diritto internazionale dei diritti umani, bensì anche adottare tutta una serie di salvaguardie ulteriori, finanche l'attribuzione di diritti soggettivi agli individui, quali quello al controllo giurisdizionale e quello ad un rimedio effettivo, in caso di loro violazione. Nel caso in cui uno Stato risulti inadempiente rispetto a tali pervasivi obblighi, potrà dunque ben insorgere una controversia internazionale, tale inadempimento

[87] Art. 18 del Patto internazionale sui diritti civili e politici.
[88] Art. 22 del Patto internazionale sui diritti civili e politici.

costituendo la violazione di un obbligo dovuto a tutti gli altri Stati parte della Convenzione. Sul punto, vanno formulate due diverse considerazioni.

In primo luogo, gli Stati, al momento della ratifica, non potranno apporre riserve miranti ad escludere o limitare l'ambito applicativo delle salvaguardie appena descritte. Da un lato, infatti, quando le parti contraenti della Convenzione abbiano inteso consentire l'apposizione di riserve, esse l'hanno fatto espressamente[89], e ciò nel solco dell'art. 19, lett. b), della Convenzione di Vienna sul diritto dei trattati, disposizione che – come noto – consente l'apposizione di riserve solo lì dove sia previsto. Se è vero che tale disposizione risulta spesso essere di non facile applicazione[90], è altrettanto vero che il grado di dettaglio con cui è stata circoscritta la facoltà degli Stati di apporre riserve[91], e soltanto in relazione a specifiche disposizioni, può ben essere letto come indice del disfavore per l'apposizione di riserve *tout court*. Dall'altro lato, anche qualora si ritenesse inapplicabile l'art. 19, lett. b), della Convenzione di Vienna, potrebbe comunque venire a rilievo l'art. 19, lett. c), della medesima Convenzione. In effetti, una riserva che miri a nullificare una o più fra le salvaguardie approntate dalle disposizioni anzidette difficilmente potrebbe dirsi in armonia con lo scopo del trattato in questione, che è sì quello di introdurre uno strumento in grado di rafforzare la cooperazione internazionale nel contrasto alla criminalità cibernetica, ma al contempo – come ribadito nel preambolo della Convenzione – assicurando massima tutela al rispetto dei diritti umani e delle libertà fondamentali, «*as enshrined in applicable international and regional instruments*», e – in particolare – del diritto alla protezione contro interferenze arbitrarie e illegittime nella sfera di riservatezza individuale[92].

In secondo luogo, vanno valutati i meccanismi di controllo, tanto politico quanto giurisdizionale, approntati dalla Convenzione per la sua implementazione. Quanto al

---

[89] Si vedano, a titolo di esempio, l'art. 11, par. 3, l'art. 23, par. 3, e l'art. 42, par. 5, della Convenzione ONU contro il *cybercrime*.

[90] A. PELLET, *Article 19*, in O. CORTEN, P. KLEIN (eds.), *The Vienna Conventions on the Law of Treaties*, Oxford, 2011, p. 438: «*It is not sufficient that some reservations are expressly permitted by the treaty for every other reservation to be permitted. Nor is it sufficient that a treaty expressly authorizes the formulation of some reservations for all others to be prohibited*».

[91] Ad esempio, l'art. 11 della Convenzione ONU contro il *cybercrime*, che obbliga gli Stati a criminalizzare il cattivo utilizzo di strumenti informatici, prevede – al par. 3 – che «*[e]ach State may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution, or otherwise making available of the items referred to in paragraph 1 (a) (ii) of this article*».

[92] Si veda il preambolo della Convenzione ONU sul *cybercrime*. Si noti, peraltro, come la necessità di introdurre significativi strumenti di tutela dei diritti umani nella Convenzione fosse già stata affermata nel corso del primo scambio di vedute realizzato nell'ambito dei negoziati in seno al Comitato (cfr. Nazioni Unite, *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Compilation of views submitted by Member States on the scope, objectives and structure (elements) of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, A/AC.291/4, e precisamente la posizione australiana (p. 6), la posizione canadese (pp. 9-10), la posizione della Repubblica Domenicana (pp. 21-22), la posizione dell'Unione europea (pp. 34-36), la posizione giamaicana (p. 40), la posizione giapponese (p. 42), la posizione del Liechtenstein (p. 45), la posizione messicana (p. 46 e p. 49), la posizione neozelandese (pp. 50-52), la posizione nigeriana (pp. 53-54), la posizione norvegese (p. 56), la posizione svizzera (pp. 58-59), la posizione del Regno Unito (pp. 61-62), la posizione statunitense (pp. 63-64)).

controllo politico, sebbene in assenza di un meccanismo di monitoraggio[93], l'art. 57 della Convenzione istituisce una Conferenza degli Stati parte del trattato, la quale dovrà essere convocata a intervalli regolari e che costituirà un luogo ove dibattere delle strategie per superare eventuali difficoltà applicative della Convenzione[94]. Quanto al controllo giurisdizionale, poi, va considerato che l'art. 63 della Convenzione, sulla risoluzione delle controversie relative all'interpretazione e all'applicazione della Convenzione stessa, prevede che, nel caso in cui il negoziato fra le parti, oppure l'esperimento di qualsiasi altro mezzo di risoluzione pacifica, non porti alla risoluzione della controversia in un tempo ragionevole, ciascuna delle parti coinvolte potrà presentare una richiesta di arbitrato nei confronti dell'altra[95]. Se le parti non sono in grado di accordarsi sull'organizzazione della procedura arbitrale nei sei mesi successivi alla presentazione della richiesta di arbitrato, allora ciascuno Stato potrà rivolgersi unilateralmente alla Corte internazionale di giustizia[96]. Anche se il par. 3 dell'art. 63 della Convenzione prevede espressamente la facoltà di ciascuno Stato di formulare una riserva che abbia l'effetto di sottrarre tale Stato al meccanismo di risoluzione delle controversie appena descritto, occorrerà vedere quanti degli Stati che ratificheranno la Convenzione decideranno di valersi della possibilità di apporre una siffatta riserva[97].

Sia come sia, a prescindere dall'esistenza o meno della giurisdizione della CIG, rimane comunque vero ciò che poc'anzi si è sostenuto: per rendere la Convenzione uno strumento effettivo di salvaguardia dei diritti individuali, non solo i giudici nazionali, bensì anche i governi degli Stati parte della Convenzione, dovranno vegliare e agire quali custodi di essa, per assicurare che quest'ultima, lungi dal costituire un potenziale *vulnus* alla tutela internazionale dei diritti umani, contribuisca, in maniera armoniosa con altri strumenti internazionali, tanto regionali quanto multilaterali, a far sì che i delitti più pericolosi nello spazio cibernetico possano essere efficacemente combattuti dalla Comunità internazionale.

---

[93] Secondo F. SEATZU, *The New UN Convention on Cybercrime*, cit., p. 244: «*States should establish independent oversight bodies capable of assessing how cybercrime laws are applied and investigating potential human rights violations. These bodies should include members of civil society, human rights experts, and technicians who have a deep understanding of the challenges posed by modern technology*».

[94] L'art. 57, par. 5, della Convenzione ONU contro il *cybercrime* dà conto delle responsabilità della Conferenza degli Stati parte di essa. Fra queste, «*a) Facilitating the effective use and implementation of this Convention, the identification of any problems thereof, as well as the activities carried out by States Parties under this Convention, including encouraging the mobilization of voluntary contributions; […] e) Reviewing periodically the implementation of this Convention by its States Parties*». Inoltre, il par. 6 della medesima disposizione prevede che «*[e]ach State Party shall provide the Conference […] with information on legislative, administrative and other measures, as well as on its programmes, plans and practices, to implement this Convention, as required by the Conference*».

[95] Art. 63, par. 2, della Convenzione ONU contro il *cybercrime*.

[96] Ibid.

[97] Nell'ambito della Convenzione di Palermo è previsto un meccanismo di risoluzione delle controversie analogo rispetto a quello della Convenzione oggetto del presente scritto (cfr. art. 35 della Convenzione di Palermo). A fronte di 193 ratifiche, gli Stati che hanno formulato una riserva per sottrarsi alla giurisdizione della Corte internazionale di giustizia sono circa una trentina (https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en, ultimo accesso il 30 giugno 2025).

In ogni caso, in attesa di valutare come si declinerà il rapporto fra esercizio dei poteri derivanti dalla Convenzione e tutela dei diritti individuali, occorre formulare alcune altre considerazioni sulla effettiva capacità della Convenzione di contribuire alla legalità del dominio cibernetico. È noto come un numero notevole di atti malevoli, spesso miranti a ledere infrastrutture di altri Stati o di società fornitrici di servizi strategici, o comunque di importanza notevole per la collettività, sia posto in essere direttamente da Stati oppure, più frequentemente, da gruppi che agiscono secondo indicazioni formulate da Stati (c.d. «attacchi cibernetici»)[98]. La Convenzione ONU risulta essere del tutto silente sul punto.

Da una parte, tale silenzio può costituire un indice della volontà degli Stati di considerare superflua qualsivoglia regolamentazione internazionale pattizia in materia di attacchi cibernetici, a ciò bastando il diritto internazionale generale. In effetti, è questa la posizione adottata da alcuni autori, i quali reputano che il diritto internazionale generale, e soprattutto le norme che regolano la responsabilità internazionale degli Stati, sia idoneo – sia pure ammettendo l'esistenza di qualche difficoltà di natura tecnica, soprattutto in materia probatoria – a disciplinare anche la responsabilità degli Stati per illeciti commessi nel dominio cyber[99]. Secondo tali posizioni, il fatto che, nella prassi, gli Stati siano restii ad affermare la responsabilità internazionale di altri Stati per attacchi cibernetici sarebbe da imputare ad una volontà squisitamente politica[100], e non già ad una impossibilità nell'utilizzo e nella concreta applicazione delle categorie del diritto internazionale[101].

---

[98] Si rammenti come lo studio promosso dalla NATO, mirante a chiarire quali siano le norme del diritto internazionale applicabili al «*cyber warfare*» sia denominato «Manuale di Tallin», proprio perché esso è stato realizzato, in seguito al compimento da parte della Federazione Russa, nel 2007, di una serie di intense operazioni cibernetiche malevole, che hanno causato danni significativi all'Estonia (cfr. E. TIKK, K. KASKA, L. VIHUL, *International Cyber Incidents: Legal Considerations* (Cooperative Cyber Defence Centre of Excellence, 2010), p. 14 ss.). Sulle concrete difficoltà nella repressione penale delle attività realizzate da gruppi che agiscano sotto la guida o le istruzioni di Stati (c.d. «*state-nexus actors*»), cfr. L. BARTOLI, *Cybersecurity and the Fight against Cybercrime: Partners or Competitors?*, in *European Journal of Risk Regulation*, 2025 (pubblicato online), pp. 8-9.

[99] Cfr. A. STIANO, *Attacchi informatici e responsabilità internazionale dello Stato*, Napoli, 2023, pp. 260-261. In questo senso, cfr. anche M.C. VITUCCI, *Le ciberoperazioni e il diritto internazionale, con alcune osservazioni sul conflitto ibrido russo-ucraino*, in *La Comunità internazionale*, 2023, p. 15 ss. Maggiormente critico, invece, sullo stato attuale del diritto internazionale in materia di attribuzione dell'illecito in rapporto al dominio cibernetico è F. DELERUE, *Cyber Operations and International Law*, Cambridge, 2020, p. 184 ss.

[100] Secondo una prospettiva critica, la scelta diffusa – comunque avente natura politica – degli Stati di astenersi dall'invocare la responsabilità internazionale di altri Stati per attacchi cibernetici sarebbe un segno di ipocrisia, perlomeno quando tali Stati affermino di considerare il diritto internazionale come senz'altro applicabile al dominio cibernetico (I. BRUNNER, *Attributing Cyber Operations under International Law: Political and Legal Issues*, in *Questions of International Law, Zoom-In 110*, 2025, p. 42: «*[…] states are either not interested in solving their disputes in cyberspace through international law, or feel like existing international law is not equipped to deal with the abundance of cyber operations being conducted in recent times. If either were true, this reveals a hypocrisy among those states who so vehemently advocate for the applicability of existing international law to cyberspace at the United Nations and in their national positions, but refuse to put their arguments to the test in a real-life scenario*»).

[101] A questo proposito, è opportuno segnalare come, in passato, siano state formulate diverse proposte di creazione di un meccanismo internazionale per l'attribuzione agli Stati di attività cibernetiche malevole (cfr. Nazioni Unite, *Our Common Agenda Policy Brief 9: A New Agenda for Peace*, 2023, p. 27, ove viene indicato quale obiettivo quello di costituire «*an independent multilateral accountability mechanism for*

D'altra parte, tuttavia, vi è chi sostiene che il diritto internazionale, e più specificamente le sue norme di *jus ad bellum*, risulti inidoneo a disciplinare gli attacchi informatici perpetrati dagli Stati, e questo soprattutto a motivo delle caratteristiche tecniche di tali attacchi[102]. Da questo punto di vista, allora, il silenzio serbato dalla Convenzione in ordine alle attività malevole realizzate, o commissionate, dagli Stati starebbe a indicare la volontà di essi di non disciplinare un ambito dei rapporti internazionali, attualmente privo di regolamentazione giuridica, tanto delicato quanto strategico per i loro interessi di sicurezza.

Che si adotti la prima o la seconda prospettiva, un punto è indiscutibile: la Convenzione ONU difficilmente potrà essere intesa quale mezzo utile a contribuire, in un senso o nell'altro, alla «pace» cibernetica internazionale fra gli Stati. Piuttosto, essa rimarrà uno strumento applicabile nel caso in cui attacchi cibernetici siano messi in atto da soggetti privati, anche su sollecitazione o indicazione delle autorità di uno Stato, ma soltanto nella prospettiva della punizione individuale di tali soggetti, e senza che la condotta di tale Stato possa venire in qualche modo a rilievo ai fini dell'applicazione della Convenzione.

8. Brevi considerazioni conclusive

La Convenzione ONU contro il *cybercrime* costituisce senz'altro uno strumento innovativo, che – basandosi in larga parte su quanto già previsto nella Convenzione di Budapest, soprattutto (ma non solo) in ordine al novero degli obblighi di incriminazione e alle misure procedurali di cui al Capitolo IV della Convenzione – mette a disposizione degli Stati strumenti di cooperazione molto pervasivi per fronteggiare la criminalità cibernetica internazionale. Alla pervasività di tali strumenti, tuttavia, corrisponde un incremento del rischio che essi possano essere utilizzati dagli Stati per porre in essere condotte lesive dei diritti umani individuali e delle libertà fondamentali.

Proprio per far fronte a tali rischi, la Convenzione appronta una serie di salvaguardie e cautele, le quali da una parte consentiranno ai giudici nazionali di arginare eventuali utilizzi abusivi della Convenzione, dall'altra prevederanno per gli Stati degli obblighi significativi, da rispettare nella fase di attuazione della Convenzione. Come si è visto,

malicious use of cyberspace by States to reduce incentives for such conduct»; per un'analisi critica di tali proposte, cfr. F. DELERUE, *Reflections on the Opportunity of an International Attribution and Accountability Mechanism for Cyber Operations*, in *Questions of International Law, Zoom-in*, 2024, p. 19: «*[b]uilding on the observations made in the previous sections, I believe that an international mechanism could be developed to assist States in the investigation and attribution of cyber operations. This mechanism would be relevant in the pre-dispute phase, when the victim State conducts the investigation, collects and assesses the evidence, and evaluates the possible next steps*»).

[102] L. BAUDIN, *Cyberattaques et droit international public: de la négociation entre États à l'intégration des acteurs privés pour parvenir à la cyberpaix?*, Parigi, 2023, p. 140: «*[d]e nos observations sur le jus ad bellum, nous parvenons à la conclusion que celui-ci est, en l'état actuel, inadapté dans les cas d'attaques informatiques. […] Déjà parce que les différentes notions liées à l'emploi du cyberespace n'ont pas été définies, ensuite parce que les particularités techniques des attaques informatiques n'ont pas été prises en considération*».

tuttavia, solo un'azione sinergica fra giudici nazionali e governi potrà far sì che la Convenzione, lungi dal costituire una minaccia per l'esercizio delle libertà individuali fondamentali, possa efficacemente adempiere alla funzione di contrasto alla criminalità cibernetica, che le è propria.

In ogni caso, al di là delle preoccupazioni per la salvaguardia dei diritti umani, si è altresì evidenziato come nella Convenzione manchi qualsivoglia norma deputata a disciplinare la responsabilità degli Stati per attacchi cibernetici che gli stessi abbiano realizzato a danno di altri Stati o di soggetti privati. Si è visto quanto diversi possano essere i motivi dietro a tale silenzio, ma rimane il fatto che, per quanto la Convenzione ONU contro il *cybercrime* costituisca senz'altro un passo in avanti nella costruzione della legalità dello spazio cibernetico, essa difficilmente potrà essere intesa anche quale strumento di promozione della pace cibernetica internazionale, per la realizzazione della quale occorrerà attendere tempi migliori.

ABSTRACT: Questo articolo offre un'analisi critica della Convenzione delle Nazioni Unite contro il *cybercrime*, adottata dall'Assemblea Generale dell'ONU il 24 dicembre 2024. Il lavoro esamina l'architettura della Convenzione, concentrandosi sulle disposizioni riguardanti gli obblighi di incriminazione, la delimitazione della competenza giurisdizionale tra gli Stati e i pervasivi meccanismi di cooperazione giudiziaria internazionale. Particolare attenzione è poi rivolta al potenziale impatto di tutti questi strumenti sulla protezione dei diritti umani e delle libertà fondamentali, gettando luce tanto sull'efficacia delle tutele incorporate nella Convenzione quanto sui rischi che da essa discendono. Infine, l'articolo critica il silenzio della Convenzione in ordine alla responsabilità degli Stati per attacchi cibernetici, concludendo che, sebbene tale Convenzione possa contribuire al contrasto internazionale della criminalità informatica, essa difficilmente potrà dirsi in grado di promuovere norme più ampie, volte a garantire la pace nel cyberspazio.

KEYWORDS: cybercrime – diritti umani – dominio cibernetico – giurisdizione – cooperazione giudiziaria internazionale.

UN CONVENTION ON CYBERCRIME AND PROTECTION OF HUMAN RIGHTS: EUROPEAN INFLUENCES ON THE INTERNATIONAL SCENARIO

ABSTRACT: This article offers a critical analysis of the newly adopted United Nations Convention on Cybercrime, approved by the UN General Assembly on 24 December 2024. It examines the Convention's normative framework, focusing on provisions concerning the obligations of criminalization, the delimitation of jurisdictional

competences among States, and the extensive mechanisms of international judicial cooperation. Particular attention is given to the potential impact of these legal instruments on the protection of fundamental rights and freedoms, highlighting both the safeguards embedded in the Convention and the risks of its misuse by authoritarian regimes. Lastly, it critically reflects on the Convention's silence regarding State responsibility for cyberattacks, concluding that while the Convention contributes to the international legal regulation of cybercrime, it falls short of promoting broader norms, aimed at ensuring cyber peace.

KEYWORDS: cybercrime – human rights – cyber domain – jurisdiction – international judicial cooperation.