LA CONVENZIONE DELLE NAZIONI UNITE CONTRO IL CYBERCRIME E LO SVILUPPO DELLE *SUPPRESSSION CONVENTIONS* SUI CRIMINI TRANSNAZIONALI. RILIEVI TEORICI E IMPLICAZIONI PRATICO-OPERATIVE

di Antonio Balsamo
(*Sostituto Procuratore generale presso la Corte di cassazione*)
e di Christian Ponti
(*Professore Associato di Diritto internazionale, Università degli studi di Milano*)

1. Negli ultimi decenni lo sviluppo della tecnologia digitale ha portato molteplici benefici per la società contemporanea, ma anche un profondo cambiamento del *cyberspace*[1], nel quale si è assistito ad una drammatica crescita e trasformazione dei

* Gli Autori dichiarano che Antonio Balsamo è autore dei paragrafi 2.4 e 2.5, e Christian Ponti è autore dei paragrafi 1.1, 1.2, 1.3, 2.1 2.3 e 3. Gli Autori sono co-autori dei paragrafi 2.2 e 4.

[1] Il termine *cyberspace* fu utilizzato per la prima volta da William Gibson in occasione della pubblicazione di alcuni racconti, ed in particolare un romanzo di fantascienza intitolato "Neuromancer" nel 1984. In dottrina si segnalano alcuni tentativi di configurare il *cybercrime* come un elemento del *cyberspace*, inteso come un vero e proprio spazio virtuale creato dagli utilizzatori di computer che interagiscono attraverso la rete (internet), da contrapporre allo spazio fisico, e dunque sottratto al potere di governo del territorio degli Stati entro confini geografici prestabiliti; in argomento D. Brodowski, *Transnational Organised Crime and Cybercrime,* in *International Law and Transnational Organized Crime*, (eds.) P. Hauck-S. Peterke, Oxford 2016, 334-358; Questa tesi può dirsi superata, in quanto il *cyberspace* è oggi considerato un mezzo di comunicazione. Come tale può essere regolamentato, seppure attraverso specifiche regole, in quanto questo particolare strumento di comunicazione, a differenza di altri, non fa riferimento ad uno specifico spazio territoriale.

reati informatici[2]. Ad oggi il *cybercrime* è considerato una minaccia globale per la sicurezza degli stati, lo sviluppo economico-sociale e la preservazione della *rule of law*[3]. Tra gli studiosi è opinione diffusa che un efficace contrasto ai *computer crimes* richieda un approccio globale, che sia basato sull'integrazione tra le politiche preventive e quelle repressive e che tenga nella dovuta considerazione la specifica natura transnazionale[4] di questi reati. La realizzazione di strumenti giuridici internazionali tesi ad armonizzare gli ordinamenti nazionali (definizione dei reati informatici, principi di giurisdizione penale, indagini transnazionali, raccolta delle prove elettroniche e cooperazione internazionale) costituisce una parte centrale, seppure non sufficiente, delle politiche di contrasto al *cybercrime*[5]. A fronte di un quadro giuridico regionale[6] e statale[7] molto frammentato, l'adozione della Convenzione delle Nazioni Unite contro il *cybercrime* (UNCC o Convenzione di Hanoi) da parte dell'Assemblea generale delle Nazioni Unite il 24 dicembre 2024[8] rappresenta il primo sforzo di realizzare a livello internazionale (e in una prospettiva tendenzialmente universale) un quadro giuridico 'armonizzato' sui reati informatici. Nella prospettiva del diritto internazionale la conclusione dell'UNCC costituisce un risultato molto rilevante in quanto si tratta, in ordine di tempo, della terza e più recente *suppression convention*[9] delle Nazioni Unite.

La prima parte di questo studio, dopo una breve ricostruzione del complesso negoziato che ha portato all'adozione dell'UNCC (paragrafo 1.1), esamina sul piano generale i rapporti tra l'UNCC e altre *suppression conventions* delle Nazioni Unite quali

---

[2] J. Clough, *Principles of Cybercrime*, Second Edition, Cambridge, 2015, 3-8; T. Tropina, *Cybercrime, Setting international standards*, in *Routledge Handbook of International Cybersecurity,* (eds.) E. Tikk-M. Kerttunen, First Edition, 2020, 148, scrive: "The threat of cybercrime has been evolving together with the evolution of the information technologies and increasing use of the information and communication networks. The last two decades have witnessed a dramatic change in the cybercrime landscape. From its early days, when computer crimes required technical skills and were committed mostly out of curiosity or to test the system vulnerabilities, digital crime grew in its scope and transformed in a complex highly sophisticated illegal industry".

[3] *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* (Preambolo, par. 3); UNGA Res. 79/243, 24.12.2024.

[4] T. Tropina, *Cybercrime, Setting international standards*, cit., 151; D. Brodowski, *op. cit*., 335-336.

[5] M. Goodman, *International dimensions of cybercrime*; in *Cybercrimes: A Multidisciplinary Analysis*, (eds.) S. Ghosh-S. Turrini, Berlin and Heidelberg, 2011, 311–339.

[6] T. Tropina, *Cybercrime, Setting international standards,* cit., 151; A. Gascón Marcén, *The Budapest Convention and the UN Cybercrime Convention negotiations*, in *Global Cybersecurity and International Law,* (ed.) A. Segura Serrano, First Edition, London, New York, 2024 (e-book), 176.

[7] UNODC, *Comprehensive Study on Cybercrime Draft—February 2013*, Vienna, 2013, 56-63. D. Brodowski, *op. cit*.,.347-351.

[8] Si veda la nota n. 3, *supra*.

[9] L'espressione *suppression conventions* è stata coniata dalla Commissione del diritto internazionale nel 1993 (UNGA Res. 48/10), e fa riferimento ad una specifica categoria di trattati multilaterali in materia penale che presentano una struttura standardizzata conclusi in particolare nell'ambito delle Nazioni Unite al fine di contrastare, per effetto dell'armonizzazione legislativa e del rafforzamento della cooperazione internazionale, specifici fenomeni criminali transnazionali.

la Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale (UNTOC o Convenzione di Palermo)[10] e la Convenzione delle Nazioni Unite contro la corruzione (UNCAC)[11] (paragrafo 1.2). Questa comparazione mira ad individuare i profili di complementarità, le potenziali sinergie e il livello di coordinamento, ma anche i potenziali conflitti normativi tra questi strumenti convenzionali, nonché il grado di apertura dell'UNCC rispetto ad altri settori del diritto internazionale, in particolare il diritto internazionale dei diritti umani (DIDU) (paragrafo 1.3). L'indagine prende altresì in considerazione, sul piano regionale, la Convenzione del Consiglio d'Europa sulla criminalità informatica (Convenzione di Budapest)[12] la quale, fino all'adozione dell'UNCC ha rappresentato, *de iure condito*, il più importante strumento convenzionale per contrastare i crimini informatici.

La seconda parte esamina i caratteri fondamentali dell'UNCC, in particolare al fine di stabilire se questo trattato realizza un adeguato bilanciamento tra la previsione di misure tese a garantire la sicurezza digitale degli stati da un lato e il rispetto dei diritti umani dall'altro. Questo tema ha infatti evidenziato una costante contrapposizione tra gli stati che hanno partecipato al negoziato che ha portato infine all'adozione dell'UNCC. Lo studio del regime giuridico delineato nell'UNCC presenta implicazioni teoriche molto rilevanti sul piano del diritto internazionale ma anche, in prospettiva, potenziali ricadute pratiche negli ordinamenti interni degli stati parti e nella cooperazione internazionale, per quanto concerne l'attività di procuratori, magistrati e forze dell'ordine impegnate nella repressione dei *computer crimes*. In particolare, sono approfonditi: l'assenza nel testo dell'UNCC di una definizione giuridica di *cybercrime* e gli obblighi di criminalizzazione riguardo ai reati informatici (paragrafo 2.1); i rapporti tra il *cybercrime* e la criminalità organizzata transnazionale nel quadro dell'UNCC (paragrafo 2.2); le questioni problematiche legate all'esercizio e al coordinamento della giurisdizione penale sui *cybercrimes* in quanto reati transnazionali alla luce dell'UNCC (paragrafo 2.3); la disciplina ivi contenuta in materia di indagini transnazionali e raccolta delle prove elettroniche (paragrafo 2.4) e cooperazione internazionale nella repressione dei reati informatici (paragrafo 2.5).

La terza parte affronta alcune questioni potenzialmente problematiche collegate all'entrata in vigore dell'UNCC e le sfide che si pongono al fine di promuovere la sua

[10] United Nations Convention against Transnational Organized Crime, UNGA Res. 55/25, 15.11.2000.
[11] United Nations Convention against Corruption, UNGA Res. 58/4, 31.10.2003.
[12] Convention on Cybercrime, Budapest, 23.XI.2001, Council of Europe, *European Treaty Series* – No. 185. La Convenzione di Budapest è entrata in vigore nel 2004 (81 stati parti); https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (ultimo accesso 29.1.2026).

attuazione sulla base di un approccio '*human rights oriented*' che coinvolga pienamente tutti gli *stakeholders* della società civile (paragrafo 3). La tesi qui sostenuta è infatti che un approccio di questo tipo sia fondamentale per rafforzare la cooperazione internazionale nel contrasto al *cybercrime* ed evitare abusi nell'interpretazione e utilizzo dell'UNCC.

All'esito dell'indagine svolta, lo studio propone alcune conclusioni rispetto ai profili teorico-pratici indagati; in particolare, in merito all'impatto dell'UNCC nello sviluppo delle *suppression conventions* e alla sua effettiva potenzialità operativa per il contrasto ai reati informatici nel rispetto dei diritti umani (paragrafo 4).

1.1. Il contrasto ai crimini informatici è entrato nell'agenda delle Nazioni Unite da più di due decenni[13]. Il dibattito riguardo alla realizzazione di una convenzione sul *cybercrime* si è tuttavia sviluppato concretamente soltanto a partire dal 2020, quando l'Assemblea generale delle Nazioni Unite, su iniziativa della Russia, ha istituito un *open-ended ad hoc intergovernmental committee of experts* (AHC)[14]. Il negoziato è entrato nel vivo nel biennio 2022-2024 e si è concluso positivamente nell'agosto del 2024 con l'adozione da parte dell'AHC di una bozza di trattato sul *cybercrime*[15], successivamente trasmessa all'Assemblea generale delle Nazioni Unite per la sua adozione formale. Peraltro, come già avvenuto in precedenza per UNTOC e UNCAC, le negoziazioni nell'AHC si sono svolte con il supporto dello *United Nations Office on Drugs and Crime* (UNODC), nel ruolo di segretariato.

La conclusione positiva del complesso negoziato[16] che ha portato all'adozione dell'UNCC rappresenta un duplice successo sul piano politico-diplomatico. Primo, a

[13] Cfr. UNGA Res. 55/59, Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century, 17.1.2001, par. 18. In questa Risoluzione l'Assemblea generale attribuisce alla *United Nations Commission on Crime Prevention and Criminal Justice* (Commissione crimine) il mandato a sviluppare risposte per il contrasto al *cybercrime*. Uno sviluppo importante al riguardo si ha nel dicembre del 2010 quando l'Assemblea generale adotta una Risoluzione (UNGA Res. 65/230, 1.4.2011, par. 9) in cui chiede, *inter alia*, alla Commissione crimine di istituire un *open-ended intergovernmental expert group* per svolgere uno studio sistematico sul *cybercrime* e sulle risposte degli stati a questo fenomeno criminale. Il risultato delle prime due sessioni di lavoro dell'*expert group* è la pubblicazione del già citato *Comprehensive Study on Cybercrime*, (si veda la nota n. 7, *supra*); per ulteriori approfondimenti si rinvia a T. Tropina, *Cybercrime, Setting international standards,* cit., 153-155.

[14] Cfr. UNGA Res. 74/401, *Countering the use of information and communications technologies for criminal purposes*, 27.12.2019.

[15] Cfr. UN Doc. A/AC.291/L.15, 7.8.2024, *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*.

[16] Per approfondimenti si rinvia a A. Gascón Marcén, *op. cit*., 174-192; 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*, vol. 9(2), 2024, pp. 221-238, https://www.tandfonline.com/doi/full/10.1080/23738871.2024.2428655#d1e141.

differenza dei processi negoziali relativamente agevoli che hanno portato alla stipulazione di UNTOC[17] e UNCAC grazie alla comunanza di obiettivi degli stati proponenti, nel caso dell'UNCC il risultato finale favorevole è stato conseguito con estrema difficoltà. In particolare, a causa di una forte contrapposizione originaria tra alcuni stati quali Russia, Cina e Iran, da un lato, che hanno sostenuto con forza negli anni il progetto di una convenzione 'universale' sul *cybercrime*[18]*;* e dall'altro molti paesi occidentali 'fedeli' alla Convenzione di Budapest[19] (questo gruppo comprende anche stati dell'America Latina) più riluttanti invece rispetto all'idea di stipulare un trattato sui reati informatici nell'ambito delle Nazioni Unite. Il contrasto tra questi due blocchi, peraltro, non ha riguardato esclusivamente divergenti valutazioni di opportunità politica[20], ma anche questioni giuridiche sostanziali di fondamentale importanza che hanno inciso sulla definizione dell'apparato normativo dell'UNCC. Ad esempio, in merito a quali reati informatici inserire nell'ambito di applicazione della futura convenzione, in particolare al fine di evitare abusi da parte dei governi nell'accesso ai dati con finalità di repressione politico-sociale[21].

Il secondo aspetto positivo concerne il fatto che dopo più di venti anni dall'adozione di UNTOC e UNCAC è stata stipulata una nuova *suppression convention* delle Nazioni Unite per contrastare i crimini transnazionali. Tuttavia, mentre UNTOC e UNCAC sono state negoziate in continuità temporale l'una rispetto all'altra e in presenza di un contesto geo-politico favorevole al multilateralismo[22], l'UNCC è stata conclusa a distanza di molti anni dalle prime due e in un momento storico segnato da numerosi conflitti armati, forti tensioni internazionali e una profonda crisi del sistema di sicurezza collettiva delle Nazioni Unite, fortemente in discussione per la limitata capacità politico-diplomatica e operativa del Consiglio di sicurezza di prevenire, contenere e porre fine alle minacce e alle violazioni della pace e della sicurezza

[17] I. Tennant, *Storia politica della Convenzione delle Nazioni Unite Contro la Criminalità Organizzata Transnazionale*, Global Initiative Against Transnational Organized Crime, 2020; https://globalinitiative.net/wp-content/uploads/2020/12/La-Promessa-di-Palermo-GI-TOC.pdf

[18] Per un esame delle posizioni espresse dagli stati nel corso degli anni durante il negoziato si rinvia a A. Gascón Marcén, *op. cit*., 185-187; più limitatamente, riguardo alle posizioni degli stati nell'ambito dell'ultima sessione dell'AHC nel 2024 si veda S. Walker-A.P. Oliveira, *The Final Call. UN Member States Adopt a new Cybercrime Treaty,* Global Initiative Against Transnational Organized Crime, 12.9.2024; https://globalinitiative.net/analysis/the-final-call-un-member-states-adopt-a-new-cybercrime-treaty/

[19] *Ibidem*; in merito alle posizioni degli stati che si sono sempre opposti alla Convenzione di Budapest (ad esempio la Russia) si rinvia anche a T. Tropina, *Cybercrime, Setting international standards,* cit., 153.

[20] A. Gascón Marcén, *op. cit*., 186.

[21] L'utilizzo del diritto penale quale strumento di 'persecuzione digitale' da parte di stati autoritari è documentato da diversi studi; si veda ad esempio D. Brown, *Cybercrime is dangerous, but a New Un Treaty Could be Worse for Rights,* Human Rights Watch, 13.8.2021,
*h*ttps://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights

[22] I. Tennant-A.P. Oliveira, *op. cit*., 223-224.

internazionale. In questo scenario, l'adozione dell'UNCC rappresenta di per sé un risultato straordinario.

1.2. Il Preambolo sottolinea che l'UNCC tiene in considerazione gli accordi internazionali e regionali sulla cooperazione in materia penale in vigore, "[...] as well as similar treaties that exist between Member States of the United Nations"[23]. Questo riferimento (seppure soltanto indiretto) alle *suppression conventions* quale regime giuridico di riferimento, trova ampia conferma nell'apparato normativo dell'UNCC: a partire dalla descrizione delle sue finalità[24], riconducibili al rafforzamento della cooperazione internazionale e della capacità delle istituzioni interne degli stati parti di contrastare efficacemente i *computer crimes*; nonché dalla lettura del suo ampio ambito di applicazione (che comprende tutte le attività di prevenzione, indagine e esercizio dell'azione penale sui reati informatici)[25].

La struttura dell'UNCC (suddivisa in 9 capitoli e 68 articoli) rende altresì palese sotto vari profili che questo nuovo accordo internazionale si colloca nel settore delle *suppression conventions*. Innanzi tutto, riguardo all'armonizzazione penale a fini repressivi l'UNCC prevede quattro pilastri principali interconnessi, ispirandosi allo schema normativo utilizzato da UNTOC e UNCAC (e, con specifico riferimento al *cybercrime*, dalla Convenzione di Budapest)[26]. L'UNCC stabilisce infatti norme comuni in materia di definizione dei reati informatici e corrispondenti obblighi di criminalizzazione a carico degli stati parti; disposizioni sulla giurisdizione penale e sulle indagini digitali transnazionali, e una disciplina articolata che comprende diverse forme di cooperazione giudiziaria internazionale in materia penale. In secondo luogo, in linea con le *suppression conventions* più recenti, che mirano a disciplinare il contrasto a determinati fenomeni criminali transnazionali secondo un approccio di tipo integrato e multilivello, l'UNCC contiene un corposo insieme di disposizioni volte a prevenire i *computer crimes*[27]. Al pari di UNTOC e UNCAC, l'UNCC prevede inoltre

[23] Preambolo UNCC (ultimo paragrafo).
[24] Art. 1 UNCC "Statement of purpose": "The purposes of this Convention are to: (a) Promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively; (b) Promote, facilitate and strengthen international cooperation in preventing and combating cybercrime; and (c) Promote, facilitate and support technical assistance and capacity-building to prevent and combat cybercrime, in particular for the benefit of developing countries".
[25] Art. 3 UNCC "Scope of application": "This Convention shall apply, except as otherwise stated herein, to: (a) The prevention, investigation and prosecution of the criminal offences established in accordance with this Convention, including the freezing, seizure, confiscation and return of the proceeds from such offences; (b) The collecting, obtaining, preserving and sharing of evidence in electronic form for the purpose of criminal investigations or proceedings, as provided for in articles 23 and 35 of this Convention".
[26] T. Tropina, *Cybercrime, Setting international standards,* cit., 152.
[27] Art. 53 UNCC.

specifici strumenti di monitoraggio e la conclusione di programmi di assistenza tecnica per dare ad essa effettiva applicazione. Infine, l'UNCC presenta carattere aperto e si propone di realizzare un coordinamento e un'integrazione sistematica[28] tra il suo regime giuridico, l'apparato normativo di altre *suppression conventions* e altri sistemi giuridici internazionali (in particolare il DIDU). Questo obiettivo, di fondamentale importanza per la necessaria coerenza, il rafforzamento reciproco dei regimi giuridici considerati e per evitare la frammentazione e gli ostacoli generati dai conflitti normativi, trova conferme dirette e indirette nei vari capitoli e in specifiche disposizioni contenute nell'UNCC, alcune delle quali saranno riprese e commentate in seguito nel corso della trattazione, a partire dal paragrafo che segue.

1.3. Una questione che richiede un approfondimento concerne il ruolo assegnato alla protezione dei diritti umani nell'UNCC. Si tratta di un argomento delicato (e come tale è affrontato nelle *suppression conventions*), in quanto la tutela dei diritti umani si colloca in posizione potenzialmente conflittuale rispetto alla repressione penale[29]. Pur tuttavia, a seguito della piena affermazione della dottrina dei diritti umani a livello internazionale, la tutela dei diritti individuali ha assunto un'importanza crescente nel contesto della repressione dei crimini transnazionali. Sotto questo profilo le *suppression conventions* non presentano un quadro giuridico uniforme. Sul piano generale UNTOC e UNCAC non impegnano espressamente gli stati parti a adempiere ai loro obblighi convenzionali nel rispetto del DIDU[30], seppure un richiamo in tal senso si trovi nei due protocolli supplementari di UNTOC relativi al contrasto ai traffici di persone[31]. UNTOC e UNCAC si limitano ad indicare alcune garanzie individuali (nella

[28] Con questa espressione si fa riferimento ad un procedimento di interpretazione e applicazione dei trattati che tenga nella dovuta considerazione qualsiasi norma di diritto internazionale rilevante nelle relazioni tra gli stati parti di un trattato (si veda l'art. 31, para. 3, let. (c) della Convenzione di Vienna sul diritto applicabile ai trattati del 1969); il principio di integrazione sistematica postula che nell'interpretazione e applicazione di un trattato sia pienamente considerato il cosiddetto "normative environment", ossia che il trattato sia interpretato e applicato tenendo conto di altri trattati rilevanti; per approfondimenti cfr. *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law,* Report of the Study Group of the International Law Commission, finalized by Mr. Martti Koskenniemi, UN Doc A/CN.4/L.682 and Add.1, 13/4/2006, para. 410-423.

[29] I diritti umani pongono al centro la tutela dei valori della persona, mentre la repressione penale tende necessariamente a privilegiare la realizzazione degli interessi dello stato nella lotta al crimine.

[30] Per quanto riguarda UNTOC un riferimento espresso al rispetto del DIDU si trova soltanto nelle guide legislative predisposte da UNODC per assistere gli stati parti nella fase di adattamento legislativo: "[…] Bearing in mind the obligation of States under the Charter of the United Nations to cooperate with one another in the promotion and observance of human rights and fundamental freedoms, legislators need to pay particular attention to how the Organized Crime Convention interacts with international human rights law"; cfr. *Legislative Guides for the implementation of the United Nations Convention against Transnational Organized Crime and the Protocols thereto*, UNODC, 2017 (updated), par. 22. Le Guide legislative offrono un importante contributo all'interpretazione delle norme di UNTOC, ma non possono essere considerate alla stregua di *Travaux préparatoires* di questa Convenzione.

[31] "Nothing in this Protocol shall affect the rights, obligations and responsibilities of States and individuals under

forma di obblighi e raccomandazioni) nel quadro dell'esercizio dell'azione penale (misure di protezione delle vittime e dei testimoni nel processo)[32] e nel contesto della cooperazione giudiziaria penale[33]. Si tratta tuttavia di misure adottate per porre dei limiti nella repressione della criminalità organizzata transnazionale e della corruzione. Secondo alcuni commentatori[34] l'assenza di un coordinamento organico con il DIDU potrebbe trovare spiegazione nel fatto che durante i negoziati relativi a UNTOC e UNCAC il dibattito sui diritti umani ha occupato un ruolo marginale. Gli stati contraenti hanno infatti ritenuto che i rischi di violazione dei diritti umani nel quadro della repressione della criminalità organizzata transnazionale e della corruzione non fossero elevati. Al contrario, le preoccupazioni correlate alle violazioni dei diritti umani nel contrasto ai reati informatici sono sempre state al centro della discussione[35], ed hanno segnato fin dall'inizio il negoziato che ha portato all'adozione dell'UNCC. In particolare, per quanto concerne i rischi di eccessiva criminalizzazione dei reati informatici[36]. All'esito di questo negoziato, l'UNCC presenta una disciplina giuridica più evoluta rispetto a UNTOC e UNCAC, in quanto contiene una espressa *human rights safeguard clause*[37] che impegna gli stati parti ad attuare gli obblighi derivanti dalla Convenzione nel pieno rispetto dei diritti umani[38]. Alla luce di questa clausola, inserita nel Capitolo I dedicato alle disposizioni di carattere generale, tutte le norme dell'UNCC devono essere interpretate in modo da facilitare la repressione dei reati informatici in conformità ai diritti umani e alle libertà individuali stabilite dal DIDU[39].

---

international law, including international humanitarian law and international human rights law"; cfr. *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children* (art. 14); e *Protocol against the Smuggling of Migrants by Land, Sea and Air* (art. 19). Il rinvio al DIDU nei due protocolli sui traffici di persone si spiega con il fatto che essi hanno ad oggetto attività criminali che sono intrinsecamente lesive della dignità umana.

[32] Artt. 24 e 25 UNTOC; art. 32 UNCAC.

[33]Ad esempio, in materia di estradizione (cfr. art. 16, par. 13 UNTOC); si veda anche art. 44, par. 14 UNCAC).

[34] I. Tennant-A.P. Oliveira, *op. cit*., 229.

[35] Ad esempio, nelle fasi conclusive del negoziato nell'ambito dell'AHC l'Iran a più riprese ha proposto, senza successo, di stralciare le disposizioni sui diritti umani dal testo finale dell'UNCC; in argomento si rinvia a S. Walker-A.P. Oliveira, *op. cit*., 9-10.

[36] I. Tennant-A.P. Oliveira, *op. cit*., 229.

[37] Art. 6 par. 1 UNCC.

[38] L'UNCC appare più avanzata rispetto alla Convenzione di Budapest in quanto la clausola sui diritti umani prevista da quest'ultima (art. 15) fa riferimento soltanto ai profili procedurali, ossia ogni stato parte deve assicurare che l'instaurazione e l'applicazione dei poteri e delle procedure necessarie per svolgere le indagini e i procedimenti penali sui reati informatici conformemente alla Convenzione siano soggette alle condizioni e alle tutele previste dal proprio diritto interno, che deve assicurare un adeguato rispetto delle norme del DIDU; si veda A. Gascón Marcén, *op. cit*., 177.

[39] L'art. 6, par. 1 dell'UNCC non indica espressamente alcuno strumento giuridico internazionale sui diritti umani, ad esempio il Patto internazionale sui diritti civili e politici del 1966, per quanto un rinvio ad esso si può indirettamente inferire dal riferimento testuale al DIDU contenuto in questo articolo. Secondo F. Seatzu, *The UN Convention on Cybercrime: Between Securing Cyberspace and Undermining Fundamental Rights and Freedoms*, in *La Comunità Internazionale*, Vol. LXXX, n. 2, 2025, 228, questa disposizione pone agli stati parti dell'UNCC non solo l'obbligo negativo di non violare i diritti umani, ma anche quello positivo di adottare azioni concrete per promuoverli.

L'articolo in esame sottolinea altresì i rischi specifici che potrebbero emergere nell'applicazione dell'UNCC, e richiama espressamente i diritti legati alla libertà di espressione, coscienza, opinione, religione o credo, riunione pacifica e associazione[40]. Questa *safeguard clause* si pone quale principio guida a protezione di eventuali abusi nell'attuazione della Convenzione[41] e, come si avrà modo di approfondire nei paragrafi che seguono, presenta ricadute 'sostanziali' rispetto a vari profili repressivi disciplinati dall'UNCC (obblighi di criminalizzazione, norme sulla giurisdizione penale, disposizioni sulle indagini transnazionali e sulla cooperazione giudiziaria internazionale in materia penale)[42]. Peraltro, al fine di stabilire se il bilanciamento tra le esigenze della sicurezza digitale e la tutela dei diritti umani possa essere conseguito pienamente alla luce dell'UNCC, è di fondamentale importanza approfondire il grado di coinvolgimento assicurato sul piano 'procedurale' a tutti gli attori della società civile dal sistema di *governance* previsto da questa Convenzione, in particolare per quanto concerne il processo di monitoraggio sulla sua effettiva applicazione da parte degli stati che la ratificheranno[43].

2.1. Un tratto caratteristico nelle *suppression conventions* concerne l'assenza di una definizione giuridica dei crimini transnazionali che esse mirano a sradicare. Tale mancanza, determinata dall'impossibilità di trovare sul piano giuridico internazionale un denominatore comune circa la definizione di un determinato fenomeno criminale, è tuttavia compensata nelle *suppression conventions* dalla previsione di un elenco di reati, frutto del compromesso raggiunto, che gli stati parti hanno l'obbligo di recepire negli ordinamenti interni, sempre che tali reati già non siano presenti nei codici penali statali. L'armonizzazione delle legislazioni penali statali sostanziali (definizione dei reati, ma non delle sanzioni penali correlate) [44] per effetto delle *suppression conventions* costituisce un caposaldo nella repressione dei crimini transnazionali, sul

[40] Art. 6, par. 2 UNCC. Questa disposizione è il risultato di una iniziativa canadese; si veda: "*Proposal by Canada on behalf of a group of 66 States and the European Union to the Ad Hoc Committee on Cybercrime (AHC) to further define the scope of the draft Convention*".

[41] S. Walker-A.P. Oliveira, *op. cit*., 3.

[42] Cfr. paragrafi da 2.1 a 2.5, *infra*.

[43] Cfr. paragrafo 3, *infra.*

[44] Le norme internazionali che definiscono i reati nelle *suppression conventions* presentano carattere *non-self-executing*, ossia non sono direttamente applicabili. Pertanto, nel rispetto del principio di legalità (*nullum crimen, nulla poena sine lege*) esse devono essere recepite e integrate negli ordinamenti interni da norme che indichino con precisione gli elementi costitutivi della fattispecie penale (*actus reus e mens rea*) (si veda anche nella nota n. 83, *infra*). Per quanto concerne i profili sanzionatori le *suppression conventions* stabiliscono soltanto alcuni criteri di carattere generale. Nella determinazione delle pene, gli stati hanno l'obbligo di tenere nella dovuta considerazione la 'grave natura' dei crimini da esse disciplinati, senza tuttavia indicare ulteriori parametri utili a stabilire quando tale principio risulti violato (cfr. art.11 par. 1 UNTOC; art. 30 par. 1 UNCAC). L'UNCC (art. 21 para. 1) stabilisce altresì che le sanzioni previste devono essere: 'effective, proportionate and dissuasive'.

piano interno e nella prospettiva internazionale[45], in particolare nel caso in cui l'accordo sia effettivamente applicato a livello universale.

Ad esempio, in relazione ad UNTOC l'insuperabile difficoltà riscontrata nel negoziato nell'individuare una definizione comune sul piano internazionale del concetto di 'criminalità organizzata' ha spinto gli stati ad escludere i reati-scopo delle organizzazioni criminali transnazionali dall'ambito di applicazione della Convenzione e a circoscrivere lo sforzo definitorio sugli attori (i gruppi criminali organizzati) identificati tramite parametri normativi molto ampi secondo la nozione di 'gruppo strutturato'[46]; con la previsione nella Convenzione madre di una serie di reati che tendono a rafforzare le potenzialità offensive dei gruppi criminali organizzati (partecipazione ad un gruppo criminale, riciclaggio, corruzione e ostacolo alla giustizia)[47], con l'aggiunta dei crimini gravi[48], e delle fattispecie criminali previste nei Protocolli supplementari. L'UNCAC invece, in assenza di una definizione sulla corruzione, stabilisce alcune fattispecie penali che descrivono modalità diverse attraverso cui si manifestano i fenomeni corruttivi statali e transnazionali[49], senza individuare nello specifico gli attori responsabili di questo variegato fenomeno criminale. L'UNCC si colloca nella scia di UNTOC e UNCAC in quanto, pur in assenza di una definizione condivisa a livello internazionale sul *cybercrime*[50], nel delimitare il suo ambito di applicazione individua un elenco di reati che possono essere commessi tramite "information and communications technology systems" (ICTs)[51]. Come già accennato, su questo aspetto cruciale il negoziato sull'UNCC si è polarizzato intorno a due principali schieramenti. Da una parte gli stati favorevoli a circoscrivere gli obblighi di criminalizzazione ai c.d. *cyber-dependent crimes,* ossia reati che possono essere commessi soltanto con l'uso di ICTs; con la previsione altresì di un numero limitato di

[45] Sul piano interno l'armonizzazione delle legislazioni penali nazionali per effetto delle *suppression conventions* consente una più efficace e generalizzata repressione dei crimini transnazionali, dal momento che i criminali hanno minori possibilità di sfruttare le lacune giuridiche presenti in alcuni stati per sfuggire alla punizione (c.d. *forum shopping*). A livello internazionale l'armonizzazione legislativa rafforza la cooperazione interstatale in materia penale tra stati posto che tale cooperazione, in particolare nella forma dell'estradizione, generalmente è subordinata al rispetto del principio della doppia incriminazione. Per un approfondimento su questi aspetti sia consentito rinviare a C. Ponti, *crimini transnazionali e diritto internazionale*, Milano, 2010, 67-72.
[46] Art. 2 let. c) UNTOC.
[47] Artt. 5, 6, 8, 23 UNTOC.
[48] Art. 2 let. b) UNTOC.
[49] Artt. 15-22 UNCAC.
[50] In argomento T. Tropina, *Cybercrime, Setting international standards,* cit., 150; J. Clough, *op. cit*., 8-11; D. Brodowski, *op. cit.*, 334-335.
[51] Chapter II 'Criminalization', artt. 7-16 UNCC. La definizione di ICTs comprende: "any device or group of interconnected or related devices, one or more of which, pursuant to a program, gathers, stores and performs automatic processing of electronic data" (cfr. art. 2 let. (a) UNCC). Quest'ampia definizione di ICTs include non solo computers, ma anche comunicazioni radio, telefoniche, tecnologia satellitare.

cyber-enabled crimes, cioè reati che possono essere commessi *offline*, ma che sono facilitati e possono divenire più pericolosi grazie all'uso di ICTs [52]. Dall'altra gli stati che propendevano invece per un trattato dai contenuti ampi e dunque per una più estesa lista di *computer crimes*[53]. Il primo e più restrittivo approccio (fondamentale per scongiurare i rischi di *over-criminalization*) mutuato dallo schema utilizzato nella definizione dei reati informatici nella Convenzione di Budapest[54] e sostenuto dai paesi occidentali, si è infine affermato nel testo dell'UNCC[55], la quale prevede sette *cyber-dependent crimes*; con l'aggiunta di alcuni *cyber-enabled crimes,* in particolare in materia di porno-pedofilia informatica [56], e con l'inserimento del riciclaggio dei proventi di reato[57].

L'UNCC contiene inoltre alcune disposizioni che consentono una estensione del suo ambito di applicazione ad altri *cybercrimes* non definiti nella Convenzione, tra cui un'apprezzabile norma di coordinamento dall'elevato potenziale repressivo che fa indirettamente riferimento alle *suppression conventions*, ed in base alla quale gli stati parti dell'UNCC hanno l'obbligo di assicurare che i reati previsti da "other applicable United Nations conventions and protocols to which they are Parties" siano considerati reati in base ai loro ordinamenti interni quando compiuti attraverso l'uso di ICTs[58].

Molto dibattuta è tuttavia un'altra disposizione contenuta nell'UNCC[59], ed in base alla quale gli stati parti possono cooperare nella condivisione e scambio di prove elettroniche in relazione a condotte che i loro ordinamenti interni qualifichino come "reati gravi"[60]. Secondo una parte della dottrina questa previsione potrebbe infatti

---

[52] I. Tennant-A.P. Oliveira, *op. cit*., 225. Si pensi ad esempio a reati quali il traffico illecito di droghe oppure al traffico illecito di armi da fuoco.

[53] In argomento si veda K. Bannelier, *Risks and opportunities of the UN Cybercrime Convention for the UNTOC & the fight against transnational organized crime: a first assessment*, in *Transnational Criminal Law Review,* 4(1), 2025, 149.

[54] D. Brodowski, *op. cit.,* 343-347.

[55] Sono compresi: illegal access (art. 7 UNCC); illegal interception (art. 8 UNCC); interference with electronic data (art. 9 UNCC); interference with an information and communications technology system (art. 10 UNCC); misuse of devices (art. 11 UNCC); information and communications technology system related forgery (art. 12 UNCC); information and communications technology system-related theft or fraud (art. 13 UNCC). Per un approfondimento sul negoziato e la definizione dei reati informatici previsti dall'UNCC, cfr. 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*, vol. 9(2), 2024, 200-220, spec. 203-209.

[56] Offences related to online child sexual abuse or child sexual exploitation material (art. 14 UNCC); solicitation or grooming for the purpose of committing a sexual offence against a child (art. 15 UNCC); è inoltre previsto un reato a contenuto sessuale commesso contro adulti (non-consensual dissemination of intimate images - art. 16 UNCC); per un approfondimento si rinvia a S. Walker-A.P. Oliveira, *op. cit.,* pp. 4-5.

[57] Art. 17 UNCC. Secondo K. Bannelier, *op. cit*., 150. Questo reato presenta carattere complementare e rafforzativo rispetto al reato di riciclaggio stabilito da UNTOC (art. 6); in particolare se si considerano le straordinarie opportunità offerte oggi dai ITC per riciclare denaro tramite le criptovalute e, sul piano repressivo, gli estesi poteri investigativi attribuiti dall'UNCC per il contrasto al *cyber-laundering*.

[58] Art. 4 UNCC.

[59] Art. 35, par. 1 let. (c), UNCC.

[60] La nozione di 'reato grave' (cfr. art. 2, let. (h), UNCC) è ripresa da UNTOC: "Serious crime" shall mean conduct constituting

consentire un ampiamento eccessivo dell'ambito di applicazione della Convenzione, fino a ricomprendere nella cooperazione internazionale la repressione di condotte protette dagli strumenti internazionali sui diritti umani, ma considerate reati nei regimi autoritari[61].

Un altro meccanismo previsto per ampliare l'ambito di applicazione dell'UNCC ad altri *cybercrimes* concerne infine la possibilità di stipulare protocolli supplementari[62] secondo lo schema già seguito da UNTOC.

2.2. Un profilo dell'UNCC che presenta elementi di somiglianza con UNCAC concerne il fatto che così come quest'ultima non definisce i soggetti responsabili della corruzione, anche l'UNCC non individua gli attori responsabili dei *cybercrimes*. La mancata definizione della cybercriminalità potrebbe rappresentare un potenziale ostacolo e consentire agli stati parti di applicare l'UNCC in modo scarsamente uniforme, riducendo dunque la sua effettività nel contrasto ai reati informatici. I cybercriminali costituiscono una categoria variegata e fluida di soggetti. La prassi dimostra tuttavia che i gruppi criminali organizzati svolgono oggi un ruolo predominante nei *cybercrimes*[63]. Nel preambolo l'UNCC[64] sottolinea l'impatto che i *computer crimes* hanno nell'ampliare, accrescere e velocizzare talune attività criminali compiute dalle organizzazioni criminali transnazionali e dai gruppi terroristici (traffici di persone, fabbricazione e traffico illeciti di armi da fuoco, loro parti, componenti e munizioni, traffico di sostanze stupefacenti e di beni culturali). L'UNCC non disciplina però nello specifico questo profilo, né contiene norme di coordinamento con UNTOC, fatta eccezione per la già richiamata disposizione di carattere generale relativa all'applicabilità dell'UNCC ai reati definiti dalle *suppression conventions*[65].

In proposito si segnala che, in assenza di strumenti giuridici internazionali *ad hoc,* UNTOC è stata utilizzata nella prassi investigativa e giudiziaria per contrastare fenomeni di *cyber-organized crimes* caratterizzati dall'elemento della transnazionalità. L'uso della Convenzione di Palermo in questo settore è apparso indispensabile in un

an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty".

[61] I. Tennant-A.P. Oliveira, *op. cit*., 234, sottolineano che i rischi di ampiamento eccessivo dell'ambito di applicazione e di abusi governativi nell'attuazione dell'UNCC per effetto del ricorso alla nozione di reato grave sono riconducibili all'assenza dei due requisiti della transnazionalità e del coinvolgimento di un gruppo criminale organizzato, che invece circoscrivono l'applicazione della nozione di reato grave nel quadro di UNTOC. Questo punto sarà ripreso, anche con riferimento all'assistenza giudiziaria reciproca (art. 40, par. 1 UNCC) nel paragrafo 2.5, *infra*.

[62] Artt. 61-62 UNCC.

[63] D. Brodowski, *op. cit*., 337-339; si veda anche nella nota n. 66, *infra*.

[64] Preambolo UNCC (terzo paragrafo).

[65] Si veda la nota n. 58, *supra*.

momento storico nel quale stanno manifestandosi con chiarezza una molteplicità di tipologie di 'criminalità informatica organizzata', come quelle del *Mafia-type organized crime*, del *Network-based organized crime*, dell'*Economic organized crime*, dell'*Organized cybercrime-as-a-Service*, e del *Darknet organized crime*[66]. In presenza di questo incessante percorso evolutivo, la definizione estremamente ampia ed elastica di 'gruppo criminale organizzato' contenuta nell'UNTOC[67] ha rivelato tutta la sua attualità, garantendo il costante adeguamento delle strategie internazionali di contrasto nei confronti di tutte le nuove forme di criminalità caratterizzate da una natura collettiva e una dimensione economica.

Estremamente importanti sono altresì l'universalità della membership di UNTOC (che attualmente ha 194 stati parti, a fronte di 193 stati membri delle Nazioni Unite) e l'incisività e vastità delle obbligazioni da essa imposte, che vanno molto oltre i confini della giustizia penale, estendendosi alle più diverse attività di prevenzione, formazione, assistenza tecnica e sviluppo economico.

Questi ultimi impegni assumono una speciale importanza in presenza di una evidente propensione della criminalità organizzata a compiere un vero e proprio salto di qualità nel proprio rapporto con le tecnologie informatiche sotto il triplice profilo dei canali finanziari, degli strumenti di comunicazione e della subcultura mafiosa. In particolare, negli ultimi anni, si è intensificato il ricorso al circuito delle criptovalute allo scopo di veicolare i flussi monetari di alcune delle più potenti organizzazioni criminali sia per lo svolgimento dei traffici illeciti, sia per le attività di riciclaggio[68].

Al tempo stesso, si è registrato il ricorso a nuovi strumenti di comunicazione come i 'criptofonini', operanti su piattaforme informatiche criptate e finalizzati a rendere impermeabili alcune delle più lucrose attività delittuose transnazionali rispetto alle tecniche di intercettazione, comprese quelle considerate più avanzate fino ad epoca assai recente.

Il tema della comunicazione ha assunto, poi, una dimensione pubblica che ha indotto anche i mass-media italiani a parlare di una 'social mafia'. Sul punto, appare estremamente significativa la ricostruzione compiuta da due dei maggiori esperti di criminalità organizzata[69], che hanno segnalato l'emergere di una 'Google Generation Criminale' con la quale le piattaforme social sono divenute teatri di una strategia di

[66] Sul tema v. A. Di Nicola, G. Baratto, B. Vettori, *Criminological definitions of organized crime on the digital test bench: towards a physical–digital framework*, in *Trends in Organized Crime*, 2025; si veda anche L. Picarella, *Il cybercrime come nuova sfida definitoria al concetto di criminalità organizzata*, *in Studi sulla questione criminale*, vol. XIX, n. 1, 2024, 105-127.
[67] Si veda la nota n. 46, *supra.*
[68] Si veda anche nella nota n. 57, *supra*.
[69] N. Gratteri, A. Nicaso, *Il Grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta*, Milano, 2023.

presidio, simile a quella già utilizzata nel mondo fisico. Per effetto di questa presenza massiccia nello spazio virtuale, i social media sono stati utilizzati come motore di un continuo rinnovamento della subcultura mafiosa, che promuove una sorta di post-verità, e costruisce consenso, senso di identità e di appartenenza, attraverso una predominanza dell'estetica della ricchezza e una idealizzazione del ruolo degli esponenti mafiosi, percepiti come fornitori di protezione e risolutori di problemi per le comunità in cui operano, ovvero come 'antieroi' protagonisti della ribellione contro una società che produce diseguaglianza e marginalità.

Di fronte a queste nuove sfide lanciate dalle organizzazioni criminali nell'era di Internet è evidente la necessità di una strategia di prevenzione e di contrasto idonea ad intervenire con l'ampiezza di visione, di metodi e di obiettivi che è propria della Convenzione di Palermo - dotata di una speciale capacità anticipatrice che la fa sempre più apparire come uno strumento pensato guardando al futuro - e che rappresenterà una caratteristica importante anche per la Convenzione di Hanoi.

2.3. I crimini informatici sono intrinsecamente transnazionali[70], pur non potendosi escludere casi (molto rari) in cui questi reati hanno luogo interamente all'interno di un unico stato. La transnazionalità dei reati informatici talvolta si manifesta anche nei casi in cui l'autore del reato e la vittima si trovino nella stessa giurisdizione. I reati informatici presentano una dimensione fisica (computers, tablets, server, ecc…) e, ai fini dell'esercizio della giurisdizione penale, lasciano tracce digitali che possono essere localizzate in termini geografici[71]. I problemi relativi all'esercizio dell'azione penale sui reati informatici sono correlati al loro specifico carattere extraterritoriale. Si pongono dunque alcune specifiche questioni giurisdizionali, la cui soluzione richiede una collaborazione effettiva tra stati. Il problema più rilevante concerne i potenziali conflitti di giurisdizione[72].

Sul piano della *prescriptive jurisdiction* l'UNCC non appare particolarmente innovativa in quanto, al pari di UNTOC e UNCAC[73], indica quale regola generale

[70] Si veda la nota n. 4, *supra*.

[71] Le prove digitali (dati elettronici) sono per definizione estremamente volatili e pongono problemi rilevanti nell'accertamento della responsabilità penale sui reati informatici; cfr. J. Clough, *op. cit*., 7; D. Brodowski, *op.cit.,* 354.

[72] Si fa riferimento alla determinazione dello stato che abbia competenza giurisdizionale su un determinato crimine transnazionale in presenza di più stati intenzionati a far valere la pretesa punitiva, e quindi che intendono esercitare o esercitano in concreto la giurisdizione penale sugli stessi fatti. L'assenza nel diritto internazionale consuetudinario di una norma che imponga agli stati dei principi di collegamento su cui determinare l'ambito di applicazione della legge penale e fondare la legittimazione ad esercitare la giurisdizione penale trova ampia conferma nella prassi, a partire dalla celebre pronuncia della Corte permanente di giustizia internazionale nel caso *Lotus* (CPGI, Francia c. Turchia, sentenza del 7 settembre 1927, in *C.P.J.I, Recueil*, Série A, n. 10, p. 19), e contribuisce ad alimentare questo tipo di problemi.

[73] Cfr. art. 15, par. 1 UNTOC; art. 42, par. 1 UNCAC.

obbligatoria in materia di giurisdizione penale sui reati informatici il solo principio di *territorialità*[74]. Come dimostra la prassi statale si tratta del principio di giurisdizione più utilizzato in relazione ai reati informatici[75]. L'operatività in concreto di questo principio si presta tuttavia ad interpretazioni diverse[76], non favorisce l'armonizzazione legislativa e non consente di evitare il rischio dei richiamati conflitti di giurisdizione sui *cybercrimes*[77].

Nell'UNCC la giurisdizione obbligatoria è prevista soltanto in un altro caso, che viene configurato come un'eccezione alla regola generale. Si tratta della previsione del principio *aut dedere aut iudicare* il quale nelle *suppression conventions* è però articolato in modo molto restrittivo[78]. Per effetto di questo principio, l'obbligo dello stato parte richiesto di esercitare l'azione penale (in alternativa all'estradizione) in relazione ai reati informatici definiti nell'UNCC si configura soltanto nell'ipotesi in cui l'unica motivazione alla base del rifiuto di concessione dell'estradizione si fondi sulla qualità di cittadino dello stato richiesto della persona di cui sia richiesta l'estradizione[79]. In tutte le altre ipotesi il principio della personalità attiva, al pari del principio della personalità passiva, è previsto unicamente quale regola di giurisdizione facoltativa[80]. Si tratta di un limite dell'UNCC. In dottrina[81] è stato infatti evidenziato come il principio di personalità attiva costituisca un valido strumento per limitare i conflitti di giurisdizione sui reati informatici generati dall'applicazione del principio di territorialità 'oggettiva'[82]; ed in tal modo prevenire il rischio di violazione di alcuni

[74] Art. 22, par. 1 UNCC. La formulazione del principio segue uno schema classico: ogni stato parte ha l'obbligo giuridico di stabilire nell'ordinamento interno la giurisdizione penale in relazione ai reati informatici previsti dall'UNCC, nel caso in cui tali crimini siano commessi nel territorio dello stato, ovvero su una nave battente la sua bandiera o su un velivolo registrato conformemente alle leggi dello stato.

[75] A. Klip, *Section IV - International criminal law. Information society and penal law. General Report*, in *Revue internationale de droit pénal*, 2014 n. 1, vol. 85, 391.

[76] Si veda nella nota n. 83, *infra*.

[77] Questo rischio, peraltro, risulta accentuato dal fatto che le *suppression conventions*, contengono una disposizione di carattere generale che consente agli stati parti di mantenere in vigore tutti i principi di giurisdizione previsti nelle legislazioni interne (cfr. art. 22 par. 6 UNCC).

[78] Art. 22, par. 3 UNCC; art. 15, par. 3 UNTOC; art. 42, par. 3 UNCAC.

[79] Ne consegue che uno stato parte dell'UNCC, in presenza nel proprio territorio di un suo cittadino non estradabile per legge ha l'obbligo di esercitare la giurisdizione in base al principio di nazionalità attiva del (presunto) reo, riguardo a reati informatici commessi anche al di fuori del proprio territorio.

[80] Artt. 22, par. 2 e 24 UNCC. In merito ai rischi per le libertà individuali connessi alla previsione della regola di giurisdizione facoltativa basata sul principio di personalità passiva nell'UNCC si rinvia a E. Scher-Zagier, *The New UN Cybercrime Treaty Is a Bigger Deal Than* Even Its Critics Realize, in *Lawfare*, 2024, https://www.lawfaremedia.org/article/the-new-un-cybercrime-treaty-is-a-bigger-deal-than-even-its-critics-realize.

[81] Cfr. J.B. Maillart, *The Need to Think Beyond Objective Territoriality to Better Protect the Rights of the Suspect of a Cybercrime*, in *Rethinking Cybercrime, Critical Debates*, (eds.) T. Owen-J. Marshall, 2021, (eBook), 105-120.

[82] Per effetto del principio di territorialità la giurisdizione penale può essere esercitata quando l'azione od omissione che costituisce il reato è avvenuta in tutto o in parte nel territorio dello Stato (applicazione soggettiva del principio di territorialità), ovvero si è ivi verificato l'evento (o una parte di esso) che è conseguenza dell'azione od omissione (applicazione oggettiva del principio di territorialità).

diritti fondamentali dell'accusato quali il quali il principio *nullum crimen nulla poena sine praevia lege*[83], ed il principio del *ne bis in idem* (la cui applicabilità a situazioni di transnazionalità, pur essendo oggetto di crescente attenzione, non è tuttavia ancora espressamente prevista dal DIDU)[84].

Le *suppression conventions* più recenti stabiliscono meccanismi di coordinamento 'parziali'[85], che accentuano l'importanza della repressione dei crimini transnazionali, ma non consentono di evitare che lo stesso fatto possa essere oggetto di procedimenti giudiziari in più stati[86]. In particolare, l'UNCC riprende testualmente una norma di coordinamento contenuta nell'UNTOC e nell'UNCAC[87], ed in base alla quale sussiste un generico dovere di consultazione tra stati parti dell'accordo, nel caso in cui essi vengano a conoscenza che in altri stati che hanno aderito a questa Convenzione siano in corso delle indagini o dei procedimenti penali in relazione allo stesso crimine. Si tratta però di una disposizione che indica una semplice facoltà e richiama gli stati parti all'obbligo di buona fede. Lo stato ha il dovere di procedere a consultazioni, ma deve darvi effettivamente corso soltanto nei casi in cui ciò sia ritenuto indispensabile ai fini della repressione penale[88]. In altre parole, questa disposizione non consente di evitare il rischio dei conflitti di giurisdizione né quello di una duplicazione dell'azione penale

[83] Il principio *nullum crimen nulla poena sine praevia lege* (ossia il diritto di ciascun individuo di non essere punito se i propri comportamenti, nel momento in cui sono posti in essere, non sono rilevanti secondo il diritto penale interno vigente nello Stato dove hanno luogo) è previsto dai principali strumenti giuridici universali e regionali a protezione dei diritti umani, contro l'arbitrarietà dell'azione punitiva esercitata dal potere esecutivo o da quello giudiziario; cfr. art. 15, par. 1 Patto internazionale sui diritti civili e politici del 1966; art. 7 par. 1 Convenzione europea dei diritti dell'uomo del 1950.

[84] Il *ne bis in idem*, come noto, è un principio di diritto penale in base al quale un individuo che sia stato giudicato con sentenza definitiva non può essere processato nuovamente per gli stessi fatti. Il *ne bis in idem* ha due principali applicazioni: il *ne bis in idem* 'interno', il quale attribuisce effetto preclusivo ad una sentenza pronunciata da un giudice dell'ordinamento penale dello stato; e il *ne bis in idem* 'internazionale', che invece agisce come meccanismo di riconoscimento di effetti giuridici rispetto a sentenze pronunciate all'estero ad opera di un giudice dell'ordinamento penale di un altro stato. Gli strumenti internazionali che tutelano i diritti umani, al pari della maggior parte delle legislazioni statali, contemplano il *ne bis in idem*, limitandone però l'ambito di operatività alle sentenze interne (cfr. art. 14, par. 7 del Patto internazionale sui diritti civili e politici.; art. 4, par. 1 del VII Protocollo addizionale alla Convenzione europea dei diritti dell'uomo (firmato a Strasburgo il 22.11.1984, in ETS n. 117; in vigore dal 1.11.1988).

[85] Con questa espressione si fa riferimento a trattati che non contengono norme idonee a prevenire o risolvere i conflitti di giurisdizione, ma al contrario li legittimano a fini repressivi. A questi si contrappongono i trattati che prevedono invece meccanismi di coordinamento "completi", i quali individuano a priori (e in astratto) l'ordinamento che presenta il collegamento più stretto con la fattispecie, cui spetta in via esclusiva l'esercizio della giurisdizione, ovvero prevedono regole sul trasferimento dei procedimenti penali o dell'esecuzione delle sentenze verso gli ordinamenti più idonei.

[86] D'altro canto, nel diritto internazionale consuetudinario non vi sono norme di coordinamento obbligatorio delle giurisdizioni penali statali e non potrebbe essere diversamente, in considerazione della già accennata inesistenza di regole generali volte a delimitare la sfera della giurisdizione statale (si veda nella nota n. 72, *supra*).

[87] Art. 22, par. 5 UNCC; art. 15, par. 5 UNTOC; art. 42, par. 5 UNCAC.

[88] Neppure la previsione di un obbligo di consultazione potrebbe garantire una soluzione efficace ai conflitti di giurisdizione penale. Gli stati potrebbero infatti trovarsi comunque in disaccordo sulle soluzioni prospettabili, ed essendo tutti posti in una posizione di assoluta parità, ciascuno potrebbe legittimamente continuare a rivendicare il proprio diritto all'esercizio della giurisdizione penale. A ciò si aggiunga che le *suppression conventions* non prevedono meccanismi obbligatori per la soluzione delle controversie tra stati parti (si veda nel paragrafo 3, *infra*).

in relazione agli stessi fatti. Nelle *suppression conventions* (compresa l'UNCC) questi rischi sono ulteriormente accentuati dall'assenza di una norma convenzionale che imponga agli stati parti l'obbligo di rispettare il *ne bis in idem* internazionale.

2.4. La transnazionalità, oltre a contraddistinguere intrinsecamente i crimini informatici, caratterizza necessariamente le relative indagini. In proposito, un dato particolarmente significativo è emerso già nel 2018, quando la Commissione europea[89], sulla base di un sondaggio rivolto alle autorità pubbliche degli stati membri e dei rapporti sulla trasparenza dei principali *service provider* (Facebook, Google, Microsoft, Twitter e Apple), ha stimato che in più della metà (precisamente, il 55%) di tutte le indagini sia stata formulata una richiesta transfrontaliera di accesso alle prove elettroniche. Questa conclusione è stata tratta da due premesse: da un lato, le prove elettroniche, in qualsiasi forma, sono risultate rilevanti in circa l'85% delle indagini penali; dall'altro lato, nel 65% delle indagini in cui le prove elettroniche hanno assunto rilevanza, si è riscontrata la necessità di una richiesta a *service provider* con sede in un'altra giurisdizione.

Da allora, la necessità di impiego delle prove elettroniche si è ulteriormente accresciuta. È stato quindi persuasivamente osservato che nella ricerca della prova di tipo penale non è più possibile distinguere tra il reato commesso in rete e il reato commesso nel mondo fisico, perché tutti i reati ormai lasciano tracce digitali, a cui è fondamentale risalire per identificare i colpevoli[90]. Risulta pertanto evidente la necessità di una profonda revisione della disciplina normativa e della prassi che governano le indagini penali, in corrispondenza con cinque caratteristiche fondamentali della prova elettronica: la sua localizzazione in più ambienti del mondo digitale, sottoposti a diverse giurisdizioni; la natura privata delle fonti (in particolare, *Internet service provider*) presso cui essa è reperibile; il carattere tipicamente transnazionale dei reati nel cui ambito essa assume frequentemente rilevanza; la necessità di strumenti investigativi ad alto tasso tecnologico per la sua acquisizione e per l'intellegibilità dei dati in essa contenuti; la sua volatilità e la sua durata limitata nel tempo[91].

La centralità assunta dai temi dell'accesso transfrontaliero alle prove digitali, della

[89] V. il *Commission Staff Working Document* del 17.4.2018, contenente la valutazione di impatto che ha accompagnato le proposte del pacchetto "E-evidence", relativo alle prove elettroniche.
[90] F. Spiezia, *Attacco all'Europa*, Milano, 2020, 188-189.
[91] F. Spiezia, *Minaccia cibernetica e nuovi paradigmi della cooperazione giudiziaria internazionale: il ruolo di Eurojust*, in *Sistema penale*, 14.7.2023, 1-41.

conservazione dei dati (*data retention*), della cooperazione pubblico-privato, dell'adattamento dell'attività investigativa alle caratteristiche dell'ambiente virtuale, si riflette su tutta la disciplina dettata dal Capitolo IV della Convenzione di Hanoi in materia di misure processuali e attività di indagine, che riprende largamente le previsioni corrispondenti contenute nella Convenzione di Budapest, integrandole con altre disposizioni che trovano il loro precedente nella Convenzione di Palermo.

I poteri e le procedure previsti nel Capitolo IV formano oggetto di precisi obblighi gravanti su tutti gli stati parte, che sono tenuti ad adottare il complesso delle misure, legislative o di altra natura, finalizzate ad introdurli per il successivo impiego in sede investigativa e processuale, e devono farne applicazione non soltanto con riguardo ai reati specificamente previsti dalla Convenzione di Hanoi, ma anche con riferimento agli altri reati commessi mediante sistemi informatici e telematici, e, in termini ancor più generali, per la raccolta di prove in formato elettronico di qualsiasi reato[92]. Si tratta, chiaramente, di una impostazione coerente con l'evoluzione della realtà criminale e delle dinamiche probatorie riscontratasi negli ultimi anni. Ciò che conta è, però, che a questa ampia estensione dei poteri di indagine e di raccolta di prove, che incidono profondamente sulla tutela dei dati personali e sull'intero sistema delle libertà dei cittadini, si accompagni una intensa valorizzazione delle garanzie dei diritti fondamentali di tutte le persone a vario titolo coinvolte nel procedimento penale.

Le speciali caratteristiche delle indagini informatiche – che si distinguono da quelle tradizionali per la promiscuità dei dati coinvolti, la natura tipicamente non selettiva dell'accesso al sistema in cui essi sono inseriti, l'agevole duplicabilità dei relativi supporti[93], la loro conservazione e consultazione per un tempo potenzialmente illimitato - rendono, infatti, quanto mai attuale l'insegnamento di chi ha sottolineato come la protezione rafforzata di alcuni aspetti della vita privata sia servita, in realtà, a rafforzare la libertà collettiva, la libertà di agire nella sfera pubblica, contro la formula dell' 'uomo di vetro', che è nata nella Germania nazista ed è tipica di tutti i totalitarismi, i quali si fondano sulla negazione assoluta di ogni distinzione tra sfera privata e sfera pubblica[94].

Per questa ragione, appare particolarmente importante il contenuto dell'art. 24

[92] Questa è la regola-base dettata dai paragrafi 1 e 2 dell'art. 23 dell'UNCC che, nei paragrafi successivi, autorizza la possibilità di apporre riserve volte a restringere la sfera di operatività delle misure della raccolta, in tempo reale, dei dati di traffico e dell'intercettazione dei dati di contenuto, con una articolata disciplina che comunque è accompagnata dall'invito a prendere in considerazione la più ampia applicazione delle misure in questione.

[93] Cfr. M. Torre, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48*, in *Informatica e diritto*, 2015, n. 1-2, 65 ss.

[94] S. Rodotà, *Intervista su privacy e libertà*, a cura di P. Conti, Roma-Bari, 2005, 28-29.

dell'UNCC, il cui par. 1 stabilisce che "ogni stato parte deve assicurare che l'istituzione, l'attuazione e l'applicazione dei poteri e delle procedure previsti nel presente capitolo siano soggette alle condizioni e alle garanzie previste dal proprio diritto interno, che deve prevedere la protezione dei diritti umani, in conformità con i propri obblighi derivanti dal diritto internazionale dei diritti umani, e che deve incorporare il principio di proporzionalità". Il par. 2 aggiunge che, "in conformità e ai sensi del diritto interno di ciascuno stato, le predette condizioni e garanzie, ove opportuno in considerazione della natura della procedura o del potere in questione, includono anche un controllo giudiziario o altro controllo indipendente, il diritto a un ricorso effettivo, i motivi che giustificano l'applicazione, e la limitazione dell'ambito e della durata di tale potere o procedura".

Si tratta di una disposizione che ha suscitato numerose critiche: alcuni autori hanno lamentato la mancanza di una espressa previsione dei principi fondamentali di legalità, necessità e non discriminazione; altri hanno osservato che anche le suddette garanzie specificamente previste dal par. 2 sono caratterizzate dalla discrezionalità e restano subordinate alla disciplina interna di ciascuno stato. Da più parti, inoltre, si è segnalato come le norme dell'UNCC possano essere utilizzate impropriamente per condurre una sorveglianza di massa, violando così diritti umani come la libertà di parola e la *privacy*[95].

Deve tuttavia rilevarsi che i primi due paragrafi dell'art. 24 della Convenzione di Hanoi contengono una regolamentazione del tutto analoga a quella dei corrispondenti paragrafi contenuti nella Convenzione di Budapest[96]. Vi sono soltanto quattro principali differenze tra le disposizioni in esame. La prima diversità testuale consiste nella mancanza, nel par. 1 dell'art. 24 dell'UNCC, di un espresso riferimento alla Convenzione europea per la protezione dei diritti umani e le libertà fondamentali del Consiglio d'Europa (Cedu), specificamente richiamata nel par. 1 dell'art. 15 della Convenzione di Budapest. Si tratta, chiaramente, di una differenza che si ricollega al diverso contesto istituzionale nel quale si colloca l'UNCC, inserita nel sistema giuridico delle Nazioni Unite, dove numerosi stati non aderiscono alla Cedu, la quale assume invece un ruolo di assoluta centralità nell'ambito del Consiglio d'Europa, dove è nata la Convenzione di Budapest.

Va comunque osservato che la Cedu, unitamente al Patto internazionale sui diritti

[95] Per una sintesi delle diverse posizioni, v. M. Watney, *The Legal Pitfalls to Ratification of the United Nations Convention Against Cybercrime*, in *The Proceedings of the 24th European Conference on Cyber Warfare and Security*, 24 (1) 2025, 717-718.
[96] Art. 15 Convenzione di Budapest.

civili e politici, costituisce una delle fonti principali di quel "diritto internazionale dei diritti umani" cui fa riferimento il par. 1 dell'art. 24 dell'UNCC, ed è produttiva di precise obbligazioni, per gli stati che ad essi aderiscono, anche per quanto attiene alla materia del contrasto al *cybercrime*[97]. È chiaro, quindi, che la disciplina che verrà adottata da questi stati per dare attuazione al Capitolo IV della Convenzione di Hanoi dovrà essere pienamente coerente con la Cedu e con il Patto internazionale sui diritti civili e politici. Tale conclusione è ulteriormente confermata dalla già commentata disposizione di carattere generale contenuta nel par. 1 dell'art. 6 dell'UNCC[98], che impegna gli stati parte ad assicurare che l'implementazione delle obbligazioni assunte con la stessa Convenzione avvenga in coerenza con gli ulteriori obblighi posti a loro carico dal diritto internazionale dei diritti umani. Inoltre, il par. 2 dello stesso art. 6 esclude ogni interpretazione delle nuove disposizioni convenzionali che renda possibile la soppressione dei diritti umani e delle libertà fondamentali, compresi i diritti relativi alle libertà di espressione, coscienza, opinione, religione, riunione e associazione, ai sensi del diritto internazionale dei diritti umani applicabile.

La seconda differenza tra la Convenzione di Hanoi e la Convenzione di Budapest consiste nel fatto che la prima include un espresso riferimento al diritto ad un ricorso effettivo[99], non specificamente menzionato dalla seconda. Si tratta, dunque, di una ulteriore garanzia richiamata testualmente dall'UNCC.

La terza differenza, che segna una estensione dell'ambito oggettivo di operatività delle tutele, è insita nel disposto del par. 5 dell'art. 24 dell'UNCC, il quale prevede che le condizioni e le garanzie stabilite in conformità allo stesso articolo si applicano a livello nazionale ai poteri e alle procedure previsti nel capitolo IV della Convenzione non solo ai fini delle indagini e dei procedimenti penali interni, ma anche ai fini della cooperazione internazionale da parte dello stato richiesto.

Infine, la quarta differenza è data dal contenuto del par. 5 dell'art. 24 dell'UNCC, il quale chiarisce che il riferimento del precedente par. 2 al controllo giudiziario o altro controllo indipendente riguarda i relativi meccanismi istituiti a livello nazionale. Può ritenersi, peraltro, che una simile precisazione sia sostanzialmente superflua, non ravvisandosi, allo stato, sistemi preventivi di controllo di livello sovranazionale sui mezzi di ricerca della prova disposti nell'ambito dei procedimenti penali dei diversi stati.

---

[97] V. sul tema M. Dimetto, *Convenzione delle Nazioni Unite contro il cybercrime e tutela dei diritti umani: influenze europee sullo scenario internazionale*, in *Freedom, Security & Justice: European Legal Studies*, 2025, n. 2, 121-123.
[98] Si veda nel paragrafo 1.3, *supra*.
[99] Art. 24, par. 2 UNCC.

Una valutazione complessiva del contenuto normativo conduce quindi alla logica conclusione che la regolamentazione dettata dell'art. 24 della Convenzione di Hanoi non determina, di per sé, un arretramento sul piano della tutela dei diritti umani rispetto agli standard garantiti dall'art. 15 della Convenzione di Budapest.

Il vero elemento di diversità sostanziale, sicuramente idoneo di incidere sul 'diritto vivente', deriva dall'ampiezza della cerchia degli stati coinvolti nei due strumenti internazionali. È chiaro, infatti, che alla maggiore ampiezza del potenziale numero degli stati che aderiranno alla Convenzione di Hanoi (già sottoscritta da 74 Parti, a poche settimane dalla sua apertura alla firma) corrisponde una minore omogeneità delle rispettive strutture costituzionali e dei principi ispiratori dei rispettivi ordinamenti giuridici. Ed è altrettanto evidente che disposizioni identiche possono essere interpretate e applicate in modo molto diverso nell'ambito dei vari ordinamenti. Ma ciò non rappresenta una valida ragione per rinunciare all'obiettivo di predisporre strumenti normativi che diano vita ad una strategia condivisa a livello globale contro fenomeni criminali emergenti.

Un approccio costruttivo per predisporre una graduale soluzione alla suddetta problematica può invece realizzarsi attraverso lo sviluppo di una cultura dei diritti umani comune all'autorità giudiziaria dei diversi stati, valorizzando gli strumenti del 'dialogo tra le Corti', della *cross-fertilization* tra ordinamenti, dell'assistenza tecnica, e dei sistemi di revisione volti ad assicurare la conformità del diritto interno alla normativa convenzionale, con la diffusione delle migliori prassi adottate nei vari contesti nazionali e con l'impulso alle opportune riforme legislative e organizzative. Sono sicuramente condivisibili, in questa materia, le riflessioni della dottrina sulla rilevanza del ruolo attribuibile alla messa a disposizione, nel contesto dell'UNCC, di un significativo armamentario di strumenti di cooperazione, finalizzati ad accrescere lo sviluppo delle capacità tecniche e organizzative degli stati meno tecnologicamente avanzati e strutturati[100].

Passando adesso ad esaminare la specifica regolamentazione dei poteri e delle procedure costituenti oggetto del capitolo IV della Convenzione di Hanoi, va osservato che essi possono raggrupparsi in due distinti insiemi, i quali trovano il loro immediato antecedente rispettivamente nella Convenzione di Budapest e nella Convenzione di Palermo. Precisamente, vi è un primo gruppo di norme in cui è contenuta la regolamentazione di una serie di misure processuali costruite in modo del tutto analogo a quelle corrispondenti disciplinate dalla Convenzione di Budapest, quali:

[100] M. Dimetto, op. cit., 123.

a) la conservazione rapida di dati elettronici immagazzinati[101]; b) la conservazione e la parziale divulgazione rapide di dati relativi al traffico[102]; c) l'ordine di produzione[103]; d) la perquisizione e il sequestro di dati informatici immagazzinati[104];e) la raccolta in tempo reale di dati relativi al traffico[105]; f) l'intercettazione di dati relativi al contenuto[106], che impegna gli stati parti a introdurre tale misura con riferimento a una serie di reati gravi, da definire nelle legislazioni dei singoli Paesi.

Vi è poi un secondo gruppo di norme che disciplinano ulteriori misure processuali, riferite ai reati informatici 'tipici', le quali trovano il loro antecedente nelle omologhe previsioni della Convenzione di Palermo, quali: a) il congelamento, il sequestro e la confisca dei proventi del reato[107]; b) la protezione dei testimoni[108]; c) l'assistenza e la protezione delle vittime[109]. Attraverso queste ultime disposizioni, viene delineata una nuova strategia di intervento giudiziario, capace di intervenire sulla dimensione economica della criminalità informatica, di ricostruire l'intera rete relazionale su cui si innestano le attività illecite, e di offrire tutela a quella vastissima gamma di persone offese riscontrabile in un contesto nel quale "la vulnerabilità dei cittadini, delle economie e dei governi aumenta proporzionalmente alla loro connettività e interdipendenza"[110].

Una valutazione complessiva porta a riconoscere che l'integrazione tra le logiche ispiratrici della Convenzione di Budapest e della Convenzione di Palermo ha consentito di inserire nella Convenzione di Hanoi una complessiva regolamentazione che risponde alla duplice esigenza di adeguare gli strumenti di indagine e di raccolta della prova all'evoluzione tecnologica, e di tenere conto della crescente sovrapposizione tra cybercrime e criminalità organizzata. Un risultato, quindi, ampiamente positivo.

[101] Art. 25 UNCC.
[102] Art. 26 UNCC
[103] Art. 27 UNCC.
[104] Art. 28 UNCC.
[105] Art. 29 UNCC.
[106] Art. 30 UNCC.
[107] Art. 31 UNCC.
[108] Art. 33 UNCC.
[109] Art. 34 UNCC.
[110] In questi termini, l'intervento dell'allora coordinatore antiterrorismo dell'Unione Europea, G. De Kerchove, nel *Justice and Home Affairs (JHA) Council meeting* del 6 e 7 giugno 2019.

2.5. Nel Capitolo V dell'UNCC trova ampio spazio la disciplina della cooperazione internazionale, che rappresenta il percorso obbligato per rendere realmente efficace l'intervento giudiziario su quell'universo del *cybercrime* che oggi appare, in larga misura, come "un mondo enorme, smisurato, inesplorato": proprio come apparve la mafia a Giovanni Falcone all'inizio degli anni '80 del secolo scorso, quando l'Ufficio Istruzione del Tribunale di Palermo si impegnò nei primi procedimenti nei quali venne sperimentato il nuovo modello delle indagini transnazionali[111].

Secondo alcuni degli osservatori più qualificati, nella presente fase storica sta delineandosi una seconda rivoluzione copernicana della cooperazione giudiziaria, dopo quella che ha visto il passaggio dalla dimensione intergovernativa ai rapporti diretti tra autorità giudiziarie, con le forme di mutuo riconoscimento[112]. Si tratta di una naturale conseguenza del carico di novità riversato sui nostri ordinari paradigmi concettuali e normativi dai connotati tipici della prova elettronica, sopra descritti, i quali vengono ad aggiungersi alle linee di tendenza che contrassegnano tipicamente la criminalità informatica, come la smaterializzazione, la deterritorializzazione, la velocizzazione, la detemporalizzazione.

Per comprendere pienamente, e valutare appropriatamente, le potenzialità del quadro giuridico internazionale attualmente in via di implementazione, occorre assumere come punto di partenza la distinzione, tracciata dalla dottrina[113], tra quattro forme di circolazione transnazionale delle prove elettroniche:

a) il modello del 'trasferimento probatorio', in cui uno stato chiede a un altro stato la trasmissione di elementi probatori di cui l'autorità giudiziaria straniera è già venuta autonomamente in possesso ai fini di un procedimento interno e, quindi, 'precostituiti';

b) il modello della 'raccolta transnazionale della prova', in cui uno stato commissiona ad un altro stato (mediante rogatoria, attraverso un ordine europeo di indagine, oppure richiedendo la costituzione di una squadra investigativa comune) il compimento di una specifica attività probatoria in relazione ad un procedimento penale in corso;

c) il modello delle 'indagini transfrontaliere', tipico della Procura europea (EPPO - *European Public Prosecutor's Office*), in cui la raccolta probatoria oltre i confini dello stato nel cui territorio è stata avviata l'indagine è affidata a una differente articolazione

[111] G. Falcone, *Intervista*, in *Rapporto sulla mafia degli anni Ottanta,* (a cura di) L. GALLUZZO-F. LA LICATA- S. LODATO, Palermo, 1986.
[112] F. Spiezia, *Minaccia cibernetica,* cit.
[113] G. Di Paolo, *La circolazione transfrontaliera delle prove elettroniche*, in *Penale diritto e procedura*, 13.5.2024.

territoriale del medesimo organismo requirente sovranazionale;

d) il modello previsto nell'Unione Europea dal Regolamento UE 2023/1543, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali, che troverà applicazione dal 18 agosto 2026 e configura moduli di circolazione delle prove elettroniche che prescindono dai tradizionali meccanismi di cooperazione orizzontale e, quindi, da un dialogo fra autorità giudiziarie: infatti, al fine di acquisire i dati conservati in formato elettronico all'estero da un prestatore di servizi operante nell'Unione Europea, le autorità competenti non dovranno più chiedere l'intervento delle autorità giudiziarie dello stato di esecuzione, ma potranno - sulla base del principio del mutuo riconoscimento, a certe condizioni e se consentito per casi interni analoghi - rivolgersi direttamente al prestatore di servizi straniero, per ingiungergli di produrre (o conservare) dati relativi agli abbonati, al traffico o al contenuto (in senso comprensivo di "qualsiasi dato in formato digitale, come testo, voce, video, immagini o suono"), con esclusione delle intercettazioni.

In effetti, proprio la percezione delle difficoltà che la costante evoluzione della criminalità informatica crea per l'effettivo esercizio della giurisdizione nazionale di ciascun Paese ha spinto la comunità internazionale a progettare nuove forme di cooperazione giudiziaria, che trovano adesso un preciso fondamento giuridico nella Convenzione di Hanoi. Sotto numerosi profili, anche in questo ambito, la Convenzione di Hanoi si pone in uno stretto nesso di continuità con la Convenzione di Budapest, della quale diffonde la logica ispiratrice in un contesto territoriale molto più ampio (in correlazione con la dimensione potenzialmente universale della sua *membership*). La maggiore estensione, tuttavia, si accompagna inevitabilmente ad un *work in progress* nella costruzione della reciproca fiducia, che si riflette in senso limitativo sulla intensità di alcune forme di cooperazione giudiziaria.

Precisamente, nella Convenzione di Hanoi, rispetto alla Convenzione di Budapest, si prevede un ambito di applicazione più circoscritto per l'assistenza giudiziaria obbligatoria nella raccolta, conservazione e condivisione della prova elettronica tra le autorità degli stati parti, che viene limitata dall'art, 35 par. 1 dall'art. 40 par. 1 ai delitti costituenti oggetto degli obblighi di incriminazione e ai reati gravi, cioè quelli puniti con pena detentiva massima non inferiore a quattro anni[114]. Si riscontra, inoltre, un grado inferiore di vincolatività - espresso con il riferimento testuale ad un 'impegno' "*States Parties shall endeavour to provide mutual legal assistance*", piuttosto che a un

[114] Cfr. nota n. 60, *supra.*

obbligo, nel testo degli artt. 45 e 46 dell'UNCC - nei settori della raccolta in tempo reale di dati relativi al traffico e dell'intercettazione di dati relativi al contenuto, rispetto a quanto previsto dalla Convenzione di Budapest.

Per quanto attiene alla tutela dei diritti fondamentali, all'applicazione delle condizioni e garanzie stabilite in conformità dell'art. 24 dell'UNCC anche ai fini della cooperazione internazionale, prevista dal par. 5 della stessa norma (come già evidenziato)[115], viene ad aggiungersi una specifica disciplina sulla protezione dei dati personali, contenuta nell'art. 36. In particolare, si attribuisce agli stati richiesti la facoltà di rifiutare di compiere ogni trasferimento di dati personali che si ponga in contrasto con le disposizioni vigenti in materia nel proprio ordinamento, e si impone agli stati richiedenti l'obbligo di assicurare che i dati personali ricevuti siano soggetti a garanzie efficaci e appropriate nei rispettivi ordinamenti giuridici. Inoltre, il trasferimento, ad opera degli stati parti, dei dati personali ricevuti a un Paese terzo o a un'organizzazione internazionale è subordinata alla previa autorizzazione dello stato parte che ha effettuato il trasferimento originario. Si tratta, chiaramente, di un complesso di previsioni finalizzate al rafforzamento di quella reciproca fiducia che risulta essenziale per la effettiva funzionalità della cooperazione giudiziaria internazionale[116].

Alla stessa logica risponde, nell'art. 37 dell'UNCC che contiene la disciplina relativa all'estradizione, la disposizione prevista dal par. 15, che esclude ogni obbligo di accogliere le relative richieste quando lo stato cui esse sono rivolte ha fondati motivi di ritenere che le medesime siano finalizzate a perseguire o punire una persona a causa del suo sesso, razza, lingua, religione, nazionalità, origine etnica o opinioni politiche. Viene così introdotta una ulteriore garanzia antidiscriminazione che si aggiunge alla facoltà, prevista dal par. 8, di rifiuto dell'estradizione in base alle condizioni stabilite dal diritto nazionale dello stato parte richiesto.

Sul modello dell'art. 35 della Convenzione di Budapest, l'art. 41 dell'UNCC prevede la istituzione di una Rete 24/7 di punti di contatto sempre disponibili per assicurare un'assistenza immediata ai fini delle indagini e dei procedimenti penali sui delitti costituenti oggetto degli obblighi di incriminazione, nonché della raccolta, trasmissione e conservazione della prova elettronica relativa ai reati gravi. Alla minore

[115] Si veda nel paragrafo 2.4, *supra*.

[116] Sul punto, risulta ampiamente significativo che la Decisione UE 2025/2307 del 13.10.2025 del Consiglio dell'Unione Europea (in GUUE L del 11.11.2025), relativa alla firma, a nome dell'Unione, della Convenzione delle Nazioni Unite contro la criminalità informatica, abbia esplicitato che la nuova Convenzione si pone "in conformità con gli obiettivi dell'Unione in materia di protezione dei dati di carattere personale, della vita privata e dei diritti fondamentali, in linea con l'articolo 16 TFUE e con la Carta dei diritti fondamentali dell'Unione europea" (considerando n. 7).

ampiezza dell'area oggettiva di operatività di tale Rete rispetto a quella analoga introdotta dalla Convenzione di Budapest (che si riferisce alle prove elettroniche di qualsiasi reato) fa riscontro un 'arsenale di strumenti' più ricco nell'UNCC (la quale fa riferimento anche alla fornitura di dati elettronici per evitare un'emergenza).

Tra le ulteriori norme sulla cooperazione giudiziaria internazionale di contenuto analogo alle corrispondenti previsioni della Convenzione di Budapest, vi sono anche gli artt. 42-46 della Convenzione di Hanoi, che disciplinano specifiche tipologie di misure di assistenza giudiziaria reciproca, quali la conservazione rapida dei dati elettronici memorizzati, la divulgazione rapida dei dati sul traffico conservati, l'accesso ai dati elettronici memorizzati, la raccolta in tempo reale di dati relativi al traffico e l'intercettazione di dati relativi al contenuto (con la minore efficacia vincolante che - come si è anticipato - caratterizza l'impegno gravante sugli stati per le ultime due misure, ritenute maggiormente invasive, rispetto alle altre, per le quali viene previsto un preciso obbligo di cooperazione, suscettibile di venir meno soltanto qualora non siano soddisfatte le condizioni stabilite ovvero venga esercitato uno dei motivi di rifiuto applicabili).

A questo primo gruppo di disposizioni se ne affianca un secondo, che trova il proprio modello di riferimento nell'UNTOC, e che comprende il trasferimento delle persone condannate[117]; il trasferimento dei procedimenti penali[118]; la cooperazione di polizia[119]; le investigazioni comuni[120]; e la cooperazione internazionale ai fini della confisca[121].

Infine, vi è un terzo gruppo di disposizioni che si ricollega alle corrispondenti previsioni dell'UNCAC e che riguarda i meccanismi di recupero di beni mediante la cooperazione internazionale ai fini della confisca[122]; la cooperazione speciale[123] e la restituzione e destinazione dei proventi di reato o beni confiscati[124].

Alcuni dei suesposti strumenti costruiti sul modello dell'UNTOC e dell'UNCAC apportano un significativo valore aggiunto rispetto alle previsioni sulla cooperazione giudiziaria internazionale contenute nella Convenzione di Budapest.

Da un lato, l'articolata disciplina dettata dagli artt. 49-52 dell'UNCC appare idonea a dare un preciso impulso alle iniziative giudiziarie mirate sulla dimensione economica

[117] Art. 38 UNCC
[118] Art. 39 UNCC.
[119] Art. 47 UNCC.
[120] Art.48 UNCC.
[121] Art. 50 UNCC.
[122] Art. 49 UNCC.
[123] Art. 51 UNCC.
[124] Art. 52 UNCC.

della criminalità informatica, secondo una metodologia che ha prodotto risultati importanti nel contrasto alla criminalità organizzata e alla corruzione.

Dall'altro lato, un percorso innovativo di speciale rilievo viene prefigurato nell'art. 48 dell'UNCC, che richiede agli stati parte di valutare l'opportunità di concludere accordi o intese bilaterali o multilaterali per la creazione di organi investigativi comuni, ad opera delle autorità competenti, in relazione ai reati informatici ai quali si riferiscono gli obblighi di incriminazione previsti dalla stessa Convenzione e che formano oggetto di indagini, azioni penali o procedimenti giudiziari in uno o più stati. Tale disposizione, che riprende puntualmente il contenuto dell'art. 19 dell'UNTOC, fa riferimento alla nozione di "organi investigativi comuni", comprensiva di una pluralità di tipologie, delle quali alcune sono state già diffusamente sperimentate con importanti risultati - come nel caso delle squadre investigative comuni - mentre altre sono ancora da esplorare e possono dare vita a sviluppi ordinamentali di straordinario interesse.

La prospettiva che si delinea è quella del passaggio dal semplice coordinamento delle indagini alla creazione di veri e propri organi comuni, dotati di funzioni investigative proprie, poste in una relazione di complementarità con quelle degli organi inquirenti dei singoli stati. Per questa via, potrebbe avviarsi un nuovo sistema di organizzazione delle indagini, sostanzialmente analogo al terzo dei modelli di circolazione transnazionale delle prove elettroniche sopra descritti, che trova la sua espressione più significativa nella Procura Europea. Uno sviluppo, questo, che supererebbe anche i più avanzati risultati finora conseguiti attraverso il Secondo Protocollo addizionale alla Convenzione di Budapest[125], il quale si limita a dettare disposizioni sulle squadre investigative comuni e sulle indagini congiunte, senza però parlare di 'organi investigativi comuni'.

Un simile percorso innovativo potrebbe trarre alimento dall'elaborazione compiuta negli ultimi anni nell'ambito dei Gruppi di Lavoro della Conferenza delle Parti della Convenzione di Palermo, dove si è sottolineata la possibilità di tracciare una distinzione tra le semplici "squadre investigative comuni" (*joint investigative teams*), formate per svolgere attività di indagine su specifici casi entro un periodo limitato di tempo, e gli "organi investigativi comuni" (*joint investigative bodies*), contrassegnati da una struttura permanente e competenti per le indagini su determinate tipologie di reato[126]. A ben vedere, una strategia moderna volta a contrastare gli aspetti più

[125] Consiglio d'Europa, Secondo Protocollo aggiuntivo alla Convenzione sulla criminalità informatica sulla cooperazione rafforzata e la divulgazione delle prove elettroniche, STCE, n. 224.
[126] Al riguardo, risulta di notevole interesse l'elaborazione contenuta nel *Background paper* preparato dal Segretariato per il

complessi della criminalità informatica transnazionale può imperniarsi proprio sulla istituzione di organi investigativi comuni, capaci di sganciare l'intervento giudiziario dai vincoli territoriali e idonei a produrre prove processualmente utilizzabili in una pluralità di ordinamenti, sulla base della applicazione di un insieme di garanzie ampiamente condiviso.

Una complessiva valutazione del quadro normativo esaminato induce a condividere le considerazioni espresse nella Dichiarazione nazionale del Regno Unito resa nella cerimonia di firma tenutasi ad Hanoi il 25 e 26 ottobre 2025, secondo cui "l'accordo raggiunto per consenso sul testo della Convenzione delle Nazioni Unite contro la criminalità informatica, poco meno di un anno fa, ha segnato un momento storico per la cooperazione internazionale su questa questione critica e complessa"[127]. In effetti, sotto vari profili le potenzialità insite nelle norme della Convenzione di Hanoi sulla cooperazione giudiziaria internazionale oltrepassano quelle della Convenzione di Budapest.

Al contempo, deve però rilevarsi che nell'UNCC rimangono assenti alcune importanti innovazioni introdotte dal Secondo Protocollo addizionale alla Convenzione di Budapest, che possono inquadrarsi nel quarto dei modelli di circolazione transnazionale delle prove elettroniche sopra descritti: *in primis*, la previsione di procedure volte a rafforzare la cooperazione diretta tra autorità statali ed enti privati, con la possibilità degli organi investigativi di uno stato parte di ottenere informazioni, riguardanti la registrazione di nomi di dominio e gli abbonati, direttamente dagli *Internet Service Provider* aventi sede principale o secondaria nel territorio di un altro Paese.

Appare comunque significativo il giudizio espresso nella Decisione del 7 ottobre 2025 del Consiglio dell'Unione Europea, relativa alla firma della Convenzione di Hanoi, dove si è sottolineato che "poiché la Convenzione prevede procedure che migliorano l'accesso transfrontaliero alle prove in formato elettronico e un elevato livello di garanzie, aderendo alla Convenzione si promuoverà la coesione dell'impegno dell'Unione nella lotta contro la criminalità informatica e altre forme di criminalità a livello mondiale. Si faciliterà inoltre la cooperazione fra gli Stati Parte appartenenti all'UE e gli stati parti non appartenenti all'UE, garantendo al tempo stesso un elevato livello di protezione delle persone"[128].

Working Group on International Cooperation riunitosi a Vienna nei giorni 7-8 luglio 2020 sul tema: *The use and role of joint investigative bodies in combating transnational organized crime* (UN Doc. CTOC/COP/WG.3/2020/2, 17.5.2020).

[127] https://hanoiconvention.org/

[128] Decisione UE 2025/2307 del 13.10.2025 del Consiglio dell'Unione Europea, cit., considerando n. 13.

3. L'influenza di UNTOC e UNCAC sull'UNCC trova conferma nella disciplina di alcuni profili procedurali di fondamentale importanza per consentire un effettivo funzionamento di questo trattato internazionale[129]. Primo, l'UNCC stabilisce quale condizione per la sua entrata in vigore il raggiungimento di 40 ratifiche[130]. Durante il negoziato si è discusso dell'opportunità di prevedere una soglia minima più alta riguardo al numero di ratifiche richieste per la sua entrata in vigore[131], in particolare allo scopo di accelerare il processo di universalizzazione dell'UNCC, ma ha infine prevalso il criterio già adottato nell'UNTOC[132].

Secondo, l'UNCC non contiene alcuno sviluppo significativo rispetto a UNTOC e UNCAC circa la previsione di un meccanismo obbligatorio per la soluzione delle controversie concernenti la sua interpretazione e applicazione. Gli stati parti hanno infatti l'obbligo di cercare di risolvere le controversie tramite negoziato, ma non quello di sottoporle ad arbitrato o alla Corte internazionale di giustizia[133]. In relazione a questo punto va tuttavia sottolineato che nel quadro delle *suppression conventions* controversie di questo tipo vengono generalmente affrontate e risolte per via diplomatica, salvo alcune rilevanti eccezioni[134].

L'esame del quadro giuridico svolto nei paragrafi precedenti conferma che in relazione all'UNCC la necessità di promuovere un approccio *human rights oriented* che coinvolga pienamente la società civile (accademia, ONG, e settore privato) nel processo di monitoraggio e attuazione dell'UNCC, come auspicato dall'AHC, appare di cruciale importanza al fine di evitare che la Convenzione possa trasformarsi in uno strumento di potere nelle mani dei governi autoritari per comprimere i diritti umani e le libertà individuali[135]. Il "mechanism of implementation" delineato nell'UNCC si richiama all'esperienza di UNTOC e UNCAC, in quanto affida la responsabilità principale di monitorare l'applicazione della Convenzione alla Conferenza degli Stati parti (COP)[136], un organismo intergovernativo che si riunisce periodicamente con la supervisione amministrativa di UNODC, privo però del potere di adottare decisioni vincolanti (e di stabilire sanzioni nei confronti degli stati parti). L'UNCC, a differenza

[129] Chapter VIII 'Mechanism of implementation', artt. 56-57 UNCC; Chapter IX 'Final provisions', artt. 59-68 UNCC.
[130] Art. 65 UNCC.
[131] S. Walker-A.P. Oliveira, *op. cit*., 9.
[132] Art. 38 UNTOC; L'UNCAC (art. 68) prevede invece una soglia più bassa ed è entrata in vigore al raggiungimento delle trenta ratifiche previste.
[133] Art. 66 UNCC.
[134] Si veda *Immunities and Criminal Proceedings (Equatorial Guinea v. France),* Judgment, I.C.J. Reports 2020, 300.
[135] In argomento si veda F. Seatzu, *op. cit.,* 242-245.
[136] Art. 57 UNCC.

di UNTOC e UNCC, prevede espressamente alcuni *entry points* che pongono le basi per un maggior coinvolgimento attivo degli *stakeholders* della società civile nel contesto istituzionale della futura COP, seppure tale partecipazione sia delineata come facoltativa e subordinata ad alcune condizioni che richiedono un impegno degli stati parti in tal senso[137].

L'assenza di un obbligo per gli stati parti di realizzare un *review mechanism* preposto a monitorare lo stato di attuazione dell'UNCC rappresenta un limite. La prassi di UNTOC e UNCAC ha infatti dimostrato che l'istituzione di un *treaty monitoring body* è fondamentale per (cercare di) garantire effettività nell'applicazione delle *suppression conventions*. In proposito, l'UNCC stabilisce in termini generici che la COP potrà istituire un *review mechanism*[138], senza però entrare nel merito. Nel dibattito che ha accompagnato il negoziato questa questione non è mai stata affrontata nello specifico. Se e quando sarà avviato in futuro un negoziato su questo punto è tuttavia ragionevole attendersi che i due *peer review mechanisms* di UNTOC e UNCAC costituiranno il modello di riferimento. In proposito, appare di fondamentale importanza che uno strumento di questo tipo, ove fosse istituito, facesse tesoro dei limiti finora emersi nell'operatività dei due *review mechanisms* di UNTOC e UNCAC in termini di (limitata) trasparenza e (scarsa) inclusività[139]. Non solo. Al fine di evitare derive autoritarie nell'attuazione della Convenzione, l'istituzione di un meccanismo di monitoraggio sull'UNCC dovrebbe prevedere l'accertamento indipendente sul piano internazionale del rispetto dei diritti umani da parte degli stati che ratificheranno la Convenzione. Sul piano sistemico si tratterebbe, peraltro, di uno sviluppo molto significativo, in quanto nel quadro delle *suppression conventions*, fino ad ora non sono

[137] "The Conference of the States Parties shall agree upon activities, procedures and methods of work to achieve the objectives set forth in paragraph 1 of this article, including: [...] Facilitating the exchange of information on legal, policy and technological developments pertaining to the offences established in accordance with this Convention and the collection of evidence in electronic form among States Parties and relevant international and regional organizations, as well as non-governmental organizations, civil society organizations, academic institutions and private sector entities, in accordance with domestic law, as well as on patterns and trends in cybercrime and on successful practices for preventing and combating such offences" (art. 57, par. 5, let. b) UNCC; "Each State Party shall provide the Conference of the States Parties 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. The Conference shall examine the most effective way of receiving and acting upon information, including, inter alia, information received from States Parties and from competent international and regional organizations. Inputs received from representatives of relevant non-governmental organizations, civil society organizations, academic institutions and private sector entities, duly accredited in accordance with procedures to be decided upon by the Conference, may also be considered (art. 57, par. 6 UNCC). L'UNCC invita gli stati parti a collaborare nello scambio di informazioni con gli stakeholders della società civile anche al di fuori del contesto istituzionale della COP (v. art. 55, par. 1 UNCC).

[138] Art. 57, para. 7 e 8 UNCC.

[139] I. Tennant-A.P. Oliveira, *op. cit*., 231-232.

mai stati istituiti *treaty monitoring bodies* con finalità di protezione dei diritti umani[140].

Le *suppression conventions* più recenti contengono delle disposizioni sull'assistenza tecnica, indispensabile per consentire a tutti gli stati parti (anche quelli meno favoriti) di dare concreta attuazione a questi accordi internazionali [141]. Nell'UNCC la promozione e il rafforzamento dell'assistenza tecnica e della "*capacity building*" degli stati parti, al fine di prevenire e sradicare i *cybercrimes*, in particolare a beneficio dei paesi in via di sviluppo (meno attrezzati sul piano delle competenze tecnologiche e delle risorse disponibili)[142] costituisce una priorità, in quanto è espressamente indicata nelle disposizioni di carattere generale, tra gli obiettivi della Convenzione [143]. Nonostante l'UNCC attribuisca carattere prioritario ai programmi di assistenza tecnica e preveda una serie di misure a tale scopo[144], sono emerse alcune critiche al riguardo. In particolare, alcuni commentatori hanno sottolineato che queste misure (rispetto alle quali gli stati parti riceveranno il supporto di UNODC)[145] sono delineate in termini troppo restrittivi, in quanto focalizzate sul rafforzamento delle capacità delle autorità di *law enforcement* di tracciare e raccogliere dati elettronici, prove e proventi dei crimini informatici; mentre mancano invece disposizioni volte a rafforzare in termini più ampi i sistemi di giustizia penale degli stati parti (ad esempio, programmi sulla formazione giuridica, o per la supervisione giudiziaria e il buon funzionamento dei procedimenti penali relativi ai reati informatici)[146].

4. Da questo studio è emerso che l'adozione dell'UNCC offre un contributo significativo al rafforzamento e allo sviluppo del cosiddetto *transnational criminal law*[147]. In proposito, si segnala innanzi tutto la coerenza sistemica, la sostanziale uniformità dello schema normativo seguito (nonché l'assenza di rilevanti conflitti

[140] Secondo F. Seatzu, *op. cit*., 230-233, un'alternativa per garantire il rispetto dei diritti umani nel quadro dell'UNCC potrebbe consistere nell'istituzione di meccanismi indipendenti di valutazione e di monitoraggio all'interno degli stati parti, ma questo risultato, in assenza di specifici obblighi nella Convenzione, potrebbe essere raggiunto soltanto grazie alla buona volontà degli stati, e risentire negativamente delle differenti culture giuridiche nonché dei diversi orientamenti politici degli stati.
[141] Art. 29 UNTOC; art. 60 UNCAC.
[142] "Stressing the need to enhance coordination and cooperation among States by, inter alia, providing technical assistance and capacity-building, including the transfer of technology on mutually agreed terms, to countries, in particular developing countries, upon their request, to improve national legislation and frameworks and enhance the capacity of national authorities to deal with cybercrime in all its forms, including its prevention, detection, investigation and prosecution, and emphasizing in this context the role that the United Nations plays"; preambolo UNCC (sesto paragrafo).
[143] Chapter I 'General Provisions', art. 1 let c), UNCC.
[144] Artt. 54-56 UNCC.
[145] Cfr. UNGA Res. 79/243, 24.12.2024, par. 4; e art. 56 par. 2, let. c) UNCC.
[146] Cfr. S. Walker-A.P. Oliveira, *op. cit*., 6-7.
[147] Per un inquadramento generale si rinvia a N. Boister, *An Introduction to Transnational Criminal Law*, Second Edition, Oxford, 2018.

normativi) tra il regime giuridico delineato nell'UNCC ed altre precedenti *suppression conventions* quali UNTOC e UNCAC, in particolare, per quanto concerne le norme tese ad armonizzare gli ordinamenti penali interni degli stati parti sui crimini transnazionali (definizione dei reati, disposizioni sulla giurisdizione penale, sulle indagini transnazionali e la cooperazione internazionale); pur con i necessari adattamenti e integrazioni dovute ai differenti crimini transnazionali disciplinati (nel caso dell'UNCC i reati informatici). Al riguardo, un elemento di criticità può essere individuato nel fatto che nell'UNCC, il legislatore in relazione alla giurisdizione penale obbligatoria si sia limitato a riprodurre le norme contenute in precedenti *suppression conventions*, e non abbia colto l'occasione per stabilire una disciplina *ad hoc* più innovativa e funzionale alla repressione dei *computer crimes*. Più in generale, sul piano sistemico non appare pienamente sfruttata la potenziale complementarità e alcuni possibili sinergie dal punto di vista repressivo tra l'UNCC e altre *suppression conventions*. Ad esempio, in assenza di una norma generale di coordinamento, sarà compito dell'interprete ricostruire sul piano applicativo gli effetti positivi di una lettura combinata tra l'UNCC e UNTOC nel contrasto ai fenomeni di *cyber organized crime*.

Dal punto di vista dell'ordinamento giuridico internazionale l'aspetto più significativo, che non trova corrispondenza in UNTOC e UNCAC, è tuttavia un altro, e concerne la piena integrazione e il coordinamento normativo che l'UNCC realizza con il DIDU elevando, nel quadro della repressione dei crimini transnazionali, la tutela e la protezione dei diritti umani a componente fondamentale dell'attuale *transnational criminal law*. A livello sistemico permane, in negativo e in continuità con UNTOC e UNCAC, l'assenza di norme obbligatorie per la soluzione delle controversie riguardo all'interpretazione e all'applicazione delle disposizioni contenute nell'UNCAC; la mancata previsione di meccanismi internazionali di monitoraggio dell'UNCC indipendenti e pienamente inclusivi della società civile; ed infine l'assenza di disposizioni sulla cooperazione interistituzionale tra la futura COP dell'UNCC e altri strumenti di *governance* delle *suppression conventions* più recenti quali le Conferenze degli stati parti di UNTOC e di UNCAC.

Nella Convenzione di Hanoi sono presenti importanti potenzialità, per la sua attitudine a coinvolgere un numero assai elevato di stati, compresi quelli in via di sviluppo, nell'adeguamento del complesso degli strumenti di indagine e di raccolta della prova all'incessante evoluzione della tecnologia e nella progettazione di strategie globali di contrasto alla dimensione economica della criminalità informatica, ormai largamente sovrapponibile alla criminalità organizzata.

La seconda rivoluzione copernicana della cooperazione giudiziaria, che sta delineandosi in questo momento storico, può trovare nell'UNCC un punto di riferimento essenziale, segnatamente per la prospettiva insita nel passaggio dal semplice coordinamento delle indagini alla creazione di veri e propri organi investigativi comuni.

La nuova Convenzione può, inoltre, segnare un netto progresso sul piano delle attività di prevenzione, che attraverso una appropriata sinergia tra istituzioni e società civile possono assumere un ruolo centrale per fronteggiare la crescente tendenza ad utilizzare lo spazio virtuale come terreno di sviluppo di una subcultura criminale.

È comunque essenziale che a tutto ciò si accompagni, sul piano del 'diritto vivente', un preciso impegno di rafforzamento della tutela dei diritti fondamentali, che - grazie anche alle iniziative di assistenza tecnica - può divenire un importante fattore di effettività della cooperazione giudiziaria internazionale e di formazione di una cultura comune nel campo giuridico e sociale, nella prospettiva di un autentico umanesimo digitale.