Freedom, Security & Justice: European Legal Studies

Rivista giuridica di classe A

2026, n. 2

EDITORIALE SCIENTIFICA

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

Indice-Sommario
2026, n. 2

Editoriale

La riforma della legislazione sulla cittadinanza tra Corte costituzionale e Corte di giustizia dell'Unione europea p. 1
Bruno Barel

Saggi, Articoli e Commenti

Free movement of persons in the agreement between the EU and the United Kingdom in respect of Gibraltar. Special status of military personnel p. 21
Pablo Antonio Fernández Sánchez

Storia diplomática: Italia-Europa-Occidente p. 44
Massimo Panebianco

¿Hacia un modelo de Estado híbrido? Entre *court-packing* e intentos de revertir la *backsliding* p. 53
Valentina Faggiani

Vulnerabilità digitale del minore e forme di tutela nel contesto europeo p. 93
Gisella Pignataro

The case law of the European Court of Human Rights regarding contested territories: "Differentiated" jurisdiction as a panacea or as an Achille's heel? p. 120
Elisa Ruozzi

The EU legal framework on social security for migrants: A comparative assessment of national practices p. 139
Paolo Iafrate

Il danno ambientale sistemico e la soglia di gravità: tra qualificazione giuridica e tutela giurisdizionale p. 163
Adelaide Francesca Daniela Luminari

FOCUS

The EU as a Global Security Provider: Countering Transnational Crime and New Cooperation Architectures

Collected Papers of the Jean Monnet Module (2023-2026) Transnational Crime & EU Law: Towards Global Action against Cross-border Threats to Common Security, Rule of Law and Human Rights (EU-GLOBACT) – (Coordinator: Prof. Dr. Anna Oriolo)

Presentazione del Focus/Focus Overview
Anna Oriolo p. 185

Parte I
Contrasto alla criminalità transnazionale e minacce globali/Countering Transnational Crime and Global Threats

Traffico illecito di armi via mare, criminalità transnazionale e sicurezza globale: verso un nuovo paradigma di legalità universale p. 191
Anna Oriolo

The tragedy of the global commons in the age of artificial intelligence: Illegal mining, transnational crime, and the future of EU global enforcement p. 216
David Schultz

The European legal framework on the return of cultural objects: An effective tool to foster civil and administrative cooperation between EU Member States? p. 241
Fulvia Staiano

Il ruolo degli Stati nella prevenzione e nella repressione degli illeciti contro il patrimonio culturale subacqueo: obiettivi e strumenti comuni tra la Convenzione UNESCO del 2001 e le politiche dell'Unione europea p. 257
Patrizia Vigni

Parte II
Nuove architetture di cooperazione e strumenti di contrasto dell'Unione europea/New Cooperation Architectures and Enforcement Tools of the European Union

Il principio di fiducia reciproca nella cooperazione giudiziaria penale a dieci anni dal caso *Aranyosi*. Alcune considerazioni sull'attualità del "doppio test" alla luce della sentenza *Commissione c. Ungheria* (*Valeurs de l'Union*) p. 281
Angela Festa

Intelligence, diritti umani e sicurezza: criticità e prospettive in ambito internazionale ed europeo p. 312
Francesco Foccillo

War-crimes investigations: New technologies, new complexities, new vulnerabilities. A strategic shortfall or evolutionary opportunity for NATO p. 334
Luigi Bramati

AI tools for combating transnational crime within the EU p. 345
Roxana Matefi

Parte III
Responsabilità e giustizia penale/Accountability and Criminal Justice

Luci e ombre (soprattutto) occidentali sul consolidamento della giustizia penale internazionale p. 355
Paolo Bargiacchi

The EU's cross-border cybercrime enforcement and the limits of extraterritorial jurisdiction p. 388
Heybatollah Najandimanesh

La vittima di tratta al centro della sicurezza in Europa tra standard CEDU e nuove sfide nell'era digitale p. 410
Anna Iermano

La regolamentazione delle catene di approvvigionamento in Europa come strumento per combattere la criminalità: dall'opposizione alla convergenza dei modelli francese e italiano p. 442
Virginie Mercier

La responsabilità penale degli enti creditizi nella gestione delle misure restrittive UE: tra obblighi di garanzia e nuove fattispecie sovranazionali di incriminazione p. 453
Carmine Renzulli

Parte IV
Diritti umani e minacce transfrontaliere/Human Rights and Cross-Border Threats

La *transnational repression* quale minaccia "rinnovata" a diritti umani e sicurezza: la necessità di una risposta mirata da parte dell'Unione europea p. 465
Stefano Busillo

Children pornography, online sextorsion, revenge porn: the provisions of Greek penal code and the EU regulatory developments p. 507
Georgios Nouskalis

Intelligenza artificiale e "fenomeno religioso" nel prisma dei diritti umani p. 518
Daniela Marrani

Postfazione/Afterword p. 539
Angela Di Stasi

Appendice p. 541
EU-GLOBACT Policy Recommendations and Guidelines
Francesco Foccillo, Emanuele Sorgente

INTELLIGENCE, DIRITTI UMANI E SICUREZZA: CRITICITÀ E PROSPETTIVE IN AMBITO INTERNAZIONALE ED EUROPEO

Francesco Foccillo*

SOMMARIO: 1. Introduzione. – 2. *Intelligence* e garanzie individuali nel diritto e nella giurisprudenza internazionali ed europei. – 3. Criminalità transnazionale, approccio repressivo e diritti umani. – 3.1. Diritti umani e situazioni di emergenza. – 3.2. Sicurezza, diritti umani e nuove tecnologie. – 4. Verso una *intelligence* comune nell'Unione europea? – 5. Conclusioni.

1. Introduzione

Il presente contributo si propone di esaminare, in chiave critica, le norme e la giurisprudenza internazionali ed europee riguarndanti l'utilizzo di strumenti di *intelligence* nelle attività di contrasto alla criminalità transnazionale al fine di verificarne la compatibilità con gli *standard* di tutela dei diritti umani fondamentali, anche alla luce delle recenti proposte di modifica del sistema dell'Unione europea.

La rilevanza del tema è intimamente connessa con l'attualità di fenomeni indagati. Negli ultimi anni, infatti, le problematiche connesse alla "legittimità" di azioni di *intelligence* fortemente lesive dei diritti umani, hanno richiamato l'interesse politico e dottrinale[1] e sono state portate all'attenzione dei giudici internazionali, in particolare della Corte di Strasburgo, chiamata a pronunciarsi, *inter alia*, sulla compatibilità con la Convenzione europea per la tutela dei diritti e delle libertà fondamentali (CEDU) del 1950[2] delle azioni di contrasto al terrorismo[3] e delle strategie di sorveglianza delle

Double-blind peer reviewed article.

* Dottorando in Scienze Giuridiche (*curriculum* Internazionalistico-Europeo-Comparato), Università degli Studi di Salerno. Indirizzo e-mail: ffoccillo@unisa.it.

[1] In dottrina si veda D. FLECK, *Individual and State Responsibility for Intelligence Gathering*, in *Michigan Journal of International Law*, 2007, n. 3, p. 706.

[2] A. DI STASI, *Introduzione alla Convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, Milano, 2025.

[3] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 27 settembre 1995, ricorso n. 18984/91, *McCann e altri c. Regno Unito*; Grande Camera, sentenza del 13 dicembre 2012, ricorso n. 39630/09, *El-Masri c. Ex Repubblica Jugoslava di Macedonia*; sentenza del 24 luglio 2014, ricorso n. 7511/13, *Husayn (Abu Zubaydah) c. Polonia*; sentenza del 24 luglio 2014, ricorso n. 28761/11, *Al Nashiri c. Polonia*; sentenza del 31 maggio 2018, ricorso n. 46454/11, *Abu Zubaydah c. Lituania*; sentenza del 31 maggio 2018, ricorso n. 33234/12, *Al Nashiri c. Romania*.

comunicazioni legate alla lotta alla criminalità[4] – comprese quelle effettuate tramite le tecnologie di crittografazione di ultima generazione[5] – mentre la crescente "transnazionalità" delle minacce criminali e la conseguente necessità di un'accresciuta cooperazione tra istituzioni nazionali e internazionali ha portato a vivaci discussioni riguardanti la riforma del sistema di *intelligence* dell'Unione europea.

Le criticità connesse ai fenomeni oggetto di studio si amplificano, peraltro, nelle situazioni emergenziali globali: la crisi russo-ucraina, la pandemia da COVID-19 e i disastri ambientali dovuti al cambiamento climatico hanno creato opportunità allettanti per la criminalità transnazionale, intensificando gli sforzi nazionali e internazionali per aumentare i livelli di servizi di sicurezza a discapito, spesso, delle libertà fondamentali[6].

Le stesse emergenze globali creano vulnerabilità che possono essere sfruttate dalla criminalità organizzata che utilizza *modus operandi* sempre più sofisticati, avvalendosi delle nuove tecnologie: si pensi alla impennata conosciuta dalla digitalizzazione con la pandemia da COVID-19 e al conseguente aumento di attacchi informatici, come la creazione e la diffusione di *malware*, il furto di dati personali sensibili o industriali o gli attacchi DDoS (*Distributed Denial of Service*)[7]. Parallelamente, il ricorso ad Internet o ad altri strumenti informatici soprattutto per l'accesso ai dati e alle informazioni con intercettazioni o metodi di raccolta di massa, rientra nelle moderne tecniche d'indagine delle stesse autorità di *intelligence* per il contrasto del terrorismo e della criminalità[8].

Il presente contributo intende offrire un quadro d'insieme del rapporto tra *intelligence*, diritti umani e sicurezza, esaminato, in particolare, attraverso la lente della incidenza che, sulle attività di *intelligence* (e sulla loro legittimità), possono avere anche le situazioni di emergenza e le nuove tecnologie; si tratta di profonde trasformazioni in atto nella comunità internazionale che si traducono in un intreccio di competenze e

[4] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 4 dicembre 2015, ricorso n. 47143/06, *Roman Zakharov c. Russia*; Grande Camera, sentenza del 25 maggio 2021, ricorsi n. 58170/13, 62322/14 e 24960/15, *Big Brother Watch e altri c. Regno Unito.*

[5] Emblematico è il caso di EncroChat, piattaforma di comunicazione crittografata, sul quale si è espressa la Corte di giustizia dell'Unione europea nella sentenza del 30 aprile 2024 nella causa C-670/22.

[6] A. ANTONIADIS, R. SCHÜTZE, E. SPAVENTA (eds.), *The European Union And Global Emergencies*, Londra, 2011; A.L. VALVO, *Il Nuovo Ordine Mondiale e le nuove minacce non convenzionali alla sicurezza degli Stati*, in G. SCALESE (a cura di) *Democrazia e diritti sociali. Pandemia, normazione dell'emergenza e modelli d'intervento socioeconomico e stato di necessità*, Cassino, 2012, p. 421; F. CASOLARI, *L'Unione europea e la gestione dei disastri. Considerazioni di natura sistemica a partire dalla reazione sovranazionale alla pandemia di COVID-19*, in *La Comunità Internazionale*, 2023, n. 2, p. 249; P. DE PASQUALE, A. LIGUSTRO (a cura di), *La gestione delle emergenze nel diritto dell'Unione e nel diritto internazionale. Emergenza energetica, ambientale e bellica*, vol. I, Napoli, 2024. Sull'impatto della pandemia da COVID-19 e del conflitto russo-ucraino sulla criminalità transnazionale si vedano Europol, *European Union Serious and Organised Crime Threat Assessment - SOCTA*, 2021 e United Nations Interregional Crime and Justice Research Institute, *The Conflict in Ukraine and Its Impact on Organized Crime and Security: A Snapshot of Key Trends*, 2022.

[7] Cfr. la valutazione della minaccia della criminalità organizzata su Internet (Internet Organised Crime Threat Assessment, IOCTA) del 2020 all'indirizzo https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment e altre relazioni di Europol all'indirizzo https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know.

[8] Si veda M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, in *Il Diritto dell'Unione Europea*, 2021, n. 1, pp. 93-124.

compiti ripartiti tra amministrazioni nazionali, europee e internazionali, coniugate all'articolazione in senso *multilevel* delle stesse garanzie dei diritti fondamentali della persona.

2. *Intelligence* e garanzie individuali nel diritto e nella giurisprudenza internazionali ed europei

Al fine di fornire un quadro concettuale più preciso possibile per lo studio e l'analisi e ancorare a parametri di chiarezza e precisione la trattazione, la prima parte dell'indagine è orientata a definire i concetti chiave, stabilire il contesto normativo in cui si inserisce lo studio e presentare gli orientamenti dottrinali e normativi pertinenti. In dottrina, l'*intelligence* è stata definita come il processo sistematico mediante il quale specifici tipi di informazioni importanti per le organizzazioni militari vengono richieste, raccolte, analizzate e fornite ai comandi e ai decisori a tutti i livelli, che include il prodotto di tale processo, la salvaguardia di tali informazioni attraverso attività di controspionaggio e lo svolgimento di operazioni richieste dalle autorità legali[9].

Quanto allo spionaggio, esso costituisce una attività specifica che può comprendere varie tecniche e operazioni, non tutte necessariamente illegali, ma tutte mirate all'ottenimento di informazioni sensibili. L'*intelligence* è, pertanto, un sistema più ampio che include lo spionaggio come una delle sue componenti operative[10].

La richiamata definizione di *intelligence*, pur focalizzandosi principalmente sull'*intelligence* militare (relativa alla protezione dello Stato da aggressioni esterne, minacce terroristiche e altre forme criminalità che minano l'integrità territoriale e la sovranità nazionale), trova piena estensione anche ad ambiti diversi, quali quelli della sicurezza civile (che include anche la gestione delle emergenze, quali quelle ambientali e sanitarie), penale (connessa alla repressione dei fenomeni criminali e alla tutela dell'ordine pubblico nazionale ed internazionale) e politica (concernente la stabilità e la

[9] S. RIETJENS, *Intelligence in Military Missions: Between Theory and Practice*, in *Handbook of Military Sciences*, 2025, p. 1. Cfr. sul punto anche la definizione standardizzata contenuta nel glossario NATO «*The product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers*», *NATO Glossary of Terms and Definitions*, AAP-06, 2020, p. 68. Si veda anche S. NIINISTÖ, *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness*, 2024, p. 23. Sull'*intelligence* ed il suo rapporto con la democrazia e con le nuove tecnologie si veda M. CANNATA, *Sicurezza e Intelligence, strumenti trasversali al servizio della democrazia*, in *lerispes.it*, 2026 e, sull'*intelligence* nel suo complesso, M. CALIGIURI, *Intelligence*, Roma, 2025.

[10] In questo perimetro concettuale, assume un rilievo centrale il complesso quadro normativo e di garanzia che circonda le figure asimmetriche di informatori, spie, *leakers* e *whistleblowers*, i cui statuti giuridici intersecano costantemente il confine tra doveri di riservatezza statale e tutela dei diritti fondamentali della persona**.** In dottrina si vedano: G.B. DEMAREST, *Espionage in International Law*, in *Denver Journal of International Law & Policy*, 1996, n. 2; A.J. RADSAN, *The Unresolved Equation of Espionage and International Law*, in *Michigan Journal of International Law*, 2007, n. 3 e C. FORCESE, *Spies Without Borders: International Law and Intelligence Collection*, in *Journal of National Security Law and Policy*, 2011, n. 5.

sicurezza del governo e delle istituzioni)[11]. L'*intelligence* costituisce, quindi, un fenomeno complesso che richiede un approccio di indagine necessariamente multidisciplinare e *multilevel* affinché sia esaminato adeguatamente dalla pluralità di angoli visuali interessati.

Sul piano normativo va precisato che, mentre in ambito interno, le attività di *intelligence* sono affidate generalmente ad agenzie istituite dai governi nazionali e regolate da leggi dello Stato, nel diritto internazionale si riscontra una differenza di disciplina relativa alle azioni di *intelligence* in tempo di pace e in tempo di guerra. Segnatamente, mentre queste ultime sono regolate dall'inizio del Novecento, l'unico trattato universalmente riconosciuto applicabile al tema in oggetto in tempo di pace è la Convenzione di Vienna sulle Relazioni Diplomatiche del 1961 (CVRD)[12] che non disciplina espressamente il fenomeno, ma proibisce indirettamente, in casi particolarmente specifici, alcune operazioni attraverso le disposizioni relative all'inviolabilità delle stanze della missione (articolo 22 paragrafo 1), della dimora privata dell'agente diplomatico (articolo 30 paragrafo 1), dei suoi documenti e della sua corrispondenza (articolo 30 paragrafo 2).

Il quadro normativo di riferimento in ambito europeo, in particolare in seno al Consiglio d'Europa, certamente non può prescindere dall'esame della citata Convenzione europea dei diritti dell'uomo del 1950[13] e in particolare del diritto alla vita privata e familiare e del diritto alla libertà di espressione sanciti, rispettivamente, dagli articoli 8 e 10. Alla CEDU si aggiunge la Convenzione per la protezione delle persone rispetto al trattamento automatizzato dei dati personali, nota anche come "Convenzione 108"[14], ratificata da 55 Stati e utilizzata da molti altri come modello per la nuova legislazione sulla protezione dei dati in tutto il mondo. Adottata nel 1981 e integrata nel 2018 da un protocollo di modifica (non ancora in vigore, che ne ha garantito l'adeguamento dei principi di protezione dei dati agli strumenti e alle pratiche odierni e ne ha rafforzato il meccanismo di *follow-up*[15]) la Convenzione 108 fornisce un solido quadro giuridico internazionale per la protezione dei dati personali e affronta specificamente le tematiche delle restrizioni alle garanzie individuali determinate da esigenze di sicurezza o dalla difesa nazionale.

Ai citati strumenti convenzionali si aggiunge una serie di atti di *soft law* riguardanti i servizi di sicurezza, adottati dall'Assemblea Parlamentare del Consiglio d'Europa, nel corso degli anni, quali: la Raccomandazione n. 1402 del 1999 su *Control of internal*

[11] M. WARNER, *Wanted: A Definition of "Intelligence": Understanding Our Craft*, in *Studies in Intelligence*, 2002, n. 3 e A.S. DEEKS, *Confronting and Adapting: Intelligence Agencies and International Law*, in *Virginia Law Review*, 2016, n. 3, p. 499.
[12] Convenzione di Vienna sulle relazioni diplomatiche, 1961.
[13] Sulla CEDU si veda A. DI STASI, *op. cit*.
[14] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STE no. 108), 1981.
[15] Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STCE no. 223), 2018.

security services in council of Europe member states[16], la Raccomandazione n. 1713 del 2005 su *Democratic oversight of the security sector in member states*[17], la Raccomandazione n. 1983 del 2011 su *Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations*[18], la Raccomandazione n. 2024 del 2013 su *National security and access to information*[19], la Raccomandazione n. 2067 del 2015 su *Mass surveillance*[20], la Risoluzione n. 2516 del 2023 su *Pegasus and similar spyware and secret State surveillance*[21] ed il Documento n. 16173 del 13 maggio 2025 intitolato *Draft third additional protocol to the European Convention on Mutual Assistance in Criminal Matters*[22].

Alla elaborazione degli standard giuridici di riferimento in materia hanno decisamente contribuito i criteri elaborati dalla giurisprudenza della Corte europea dei diritti dell'uomo cui già si è accennato; vanno segnalate, in particolare, le pronunce rese nei casi *Liberty e altri c. Regno Unito* del 2008[23], *El-Masri c. ex Repubblica Jugoslava di Macedonia* del 2012[24], *Husayn (Abu Zubaydah) c. Polonia*[25] e *Al Nashiri c. Polonia*

[16] Assemblea Parlamentare del Consiglio d'Europa, Raccomandazione n. 1402, *Control of internal security services in Council of Europe member states*, 1999.
[17] Assemblea Parlamentare del Consiglio d'Europa, Raccomandazione n. 1713, *Democratic oversight of the security sector in member states*, 2005.
[18] Assemblea Parlamentare del Consiglio d'Europa, Raccomandazione n. 1983, *Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations*, 2011.
[19] Assemblea Parlamentare del Consiglio d'Europa, Raccomandazione n. 2024, *National security and access to information*, 2013
[20] Assemblea Parlamentare del Consiglio d'Europa, Raccomandazione n. 2067, *Mass surveillance*, 2015.
[21] Assemblea Parlamentare del Consiglio d'Europa, Raccomandazione n. 2516, *Pegasus and similar spyware and secret State surveillance*, 2023.
[22] Assemblea Parlamentare del Consiglio d'Europa, Opinione n. 306, *Draft third additional protocol to the European Convention on Mutual Assistance in Criminal Matters*, 2025.
[23] Il caso nasce dall'installazione di una *Electronic Test Facility* da parte del Ministero della difesa del Regno Unito con l'obiettivo di intercettare diecimila telefonate simultaneamente e che è stato accusato dai ricorrenti di aver intercettato «*tutte le comunicazioni pubbliche ivi incluse, le comunicazioni telefoniche, quelle via fax ed e-mail*». La Corte ha ritenuto «*che vi sia stata una violazione dell'articolo 8 della Convenzione*» sul rispetto della corrispondenza personale (vedi Corte europea dei diritti dell'uomo, sentenza del 1° luglio 2008, ricorso n. 58243/00, *Liberty e altri c. Regno Unito*).
[24] Il caso trae origine dall'arresto e dal trattamento subito da El-Masri a Skopje dopo il suo arresto nel 2003 seguito all'accusa di essere parte di una organizzazione terroristica. La Corte ha condannato l'ex Repubblica Jugoslava di Macedonia (attualmente Macedonia del Nord dopo la riforma costituzionale del 2019) per violazioni dell'articolo 3 sulla proibizione della tortura (Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 13 dicembre 2012, ricorso n. 39630/09, *El-Masri c. Ex Repubblica Jugoslava di Macedonia*).
[25] Il caso si fondava sulle accuse di tortura formulate dal ricorrente subite in Polonia da parte della *Central Intelligence Agency* (CIA) dopo il suo arresto in Pakistan, il suo trasferimento in Polonia e la sua estradizione a Guantanamo Bay. La Polonia è stata condannata per violazione degli articoli 3, 5, 6 paragrafo 1, 8 e 13 della Convenzione (Corte europea dei diritti dell'uomo, sentenza del 24 luglio 2014, ricorso n. 7511/13, *Husayn (Abu Zubatdah) c. Polonia*).

del 2014[26], *Roman Zakharov c. Russia* del 2015[27], *Abu Zubaydah c. Lituania*[28], *Al Nashiri c. Romania* del 2018[29] e *Big Brother Watch e altri c. Regno Unito* del 2021[30] e, più recentemente, *Green Alliance c. Bulgaria*[31] e *Kanev e Bulgarian Helsinki Committee c. Bulgaria* del 2026[32].

Quanto all'Unione europea, va segnalato che, se per un verso, l'articolo 4 paragrafo 2 del TUE specifica che «*la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro*», sempre più frequenti sono le proposte di creazione di un vero e proprio servizio di cooperazione in materia di *intelligence* comune, quale quella contenuta nel Rapporto presentato nel marzo 2024 da Sauli Niinistö, ex presidente della Repubblica di Finlandia, in qualità di consigliere speciale del presidente della Commissione europea, dal titolo *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness*[33].

[26] Il caso originava dal trattamento subito dal ricorrente in Polonia dopo il suo arresto a Dubai e il suo trasferimento a Guantanamo Bay. La Polonia è stata condannata per violazione degli articoli 3, 5, 6 paragrafo 1, 8 e 13 della Convenzione e degli articoli 2 e 3 della Convenzione in combinato disposto con l'articolo 1 del Protocollo n. 6 (Corte europea dei diritti dell'uomo, sentenza del 24 luglio 2014, ricorso n. 28761/11, *Al Nashiri c. Polonia*).

[27] Il ricorrente lamentava di essere stato intercettato nelle sue comunicazioni telefoniche dalle autorità russe. La Corte ha giudicato la normativa russa come inadeguata e ha condannato la Federazione Russa per aver violato l'articolo 8 della Convenzione (Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 4 dicembre 2015, ricorso n. 47143/06, *Roman Zakharov c. Russia*).

[28] Il caso riguardava l'accusa del ricorrente di essere stato estradato illegalmente negli Stati Uniti d'America dalle autorità lituane e, di conseguenza, essere stato soggetto a maltrattamenti e detenzioni arbitrarie in un "*black site*" della CIA. La Corte ha condannato la Lituania per violazioni degli articoli 3, 5, 8 e 13 della Convenzione (Corte europea dei diritti dell'uomo, sentenza del 31 maggio 2018, ricorso n. 46454/11, *Abu Zubaydah c. Lituania*).

[29] Il caso originava da una situazione analoga a quella descritta nella nota precedente. La Corte ha condannato la Romania per violazione degli articoli 3, 5 e degli articoli 6 paragrafo 1, 2 e 3 della Convenzione in combinato disposto con l'articolo 1 del Protocollo n. 6 (Corte europea dei diritti dell'uomo, sentenza del 31 maggio 2018, ricorso n. 33234/12, *Al Nashiri c. Romania*).

[30] Il caso nasceva dalle accuse dei ricorrenti nei confronti delle autorità del Regno Unito di intercettazioni di massa delle comunicazioni, ricevimento di materiale intercettato da governi e agenzie di *intelligence* stranieri e ottenimento di dati di comunicazione dai *service provider*. La Corte ha condannato il Regno Unito per violazioni degli articoli 8 e 10 della Convenzione (Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 25 maggio 2021, ricorsi n. 58170/13, 62322/14 and 24960/15, *Big Brother Watch e altri c. Regno Unito*).

[31] Il caso originava dalla richiesta del ricorrente di chiedere una *review* della legislazione bulgara che permette all'agenzia di *intelligence* del paese di infiltrare agenti sotto copertura in organizzazioni private. La Corte ha condannato la Bulgaria per violazioni dell'articolo 8, vietando l'uso di "agenti sotto copertura" (*agents on cover*) infiltrati all'interno di persone giuridiche e associazioni senza garanzie legali stringenti contro l'arbitrio. La Corte ha chiarito che le esigenze di sicurezza nazionale non possono azzerare le tutele del domicilio e della riservatezza delle organizzazioni. Corte europea dei diritti dell'uomo, sentenza del 17 febbraio 2026, ricorso n. 6580/22, *Green Alliance c. Bulgaria*.

[32] Il caso originava dalla sorveglianza segreta di attivisti della società civile e dal rifiuto da parte delle autorità bulgare, dietro richiesta del ricorrente, di una richiesta di sapere quali informazioni sono state raccolte su di lui. La Corte ha Condannato la Bulgaria per violazione dell'articolo 8, introducendo l'obbligo di "trasparenza vigilata", impedendo agli Stati di opporre un segreto di Stato assoluto e automatico senza un bilanciamento proporzionato. Corte europea dei diritti dell'uomo, sentenza del 28 aprile 2026, ricorso n. 45864/22, *Kanev e Bulgarian Helsinki Committee c. Bulgaria*.

[33] S. NIINISTÖ, *op. cit.*, p. 23.

Completano la ricostruzione del quadro normativo i pertinenti strumenti di diritto derivato dell'Unione relativi, in particolare, alla tutela dei dati personali[34], alla lotta alla criminalità organizzata, alla *cybersecurity*[35], alla cooperazione giudiziaria e di polizia[36] e

[34] Direttiva 2016/680/UE del Parlamento europeo e del Consiglio sulla *relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*, del 27 aprile 2016, in GUUE L 119 del 4 maggio 2016; Regolamento 2016/679 del Parlamento europeo e del Consiglio *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*, del 27 aprile 2016, in GUUE L 119 del 4 maggio 2016; Direttiva 2002/58/CE del Parlamento europeo e del Consiglio *relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)*, del 12 luglio 2002, in GUCE 201 del 31 luglio 2002; e art. 8 della Carta di Nizza.

[35] Si vedano: Regolamento 2019/881/UE del Parlamento europeo e del Consiglio, *relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013*, del 17 aprile 2019, in GUUE L 151 del 7 giugno 2019; la Direttiva 2022/2555/UE del Parlamento europeo e del Consiglio, *relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)*, del 14 dicembre 2022, in GUUE L 333 del 27 dicembre 2022; il Regolamento 2024/2847/UE del Parlamento europeo e del Consiglio, *relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la Direttiva (UE) 2020/1828 (Regolamento sulla ciberresilienza)*, del 23 ottobre 2024, in GUUE L 2847 del 20 novembre 2024; e il Regolamento 2016/679/UE, cit.

[36] Si vedano: Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, *relativa agli attacchi contro i sistemi di informazione e che sostituisce la Decisione quadro 2005/222/GAI del Consiglio*, del 12 agosto 2013, in GUUE L 218 del 14 agosto 2013; Regolamento 2015/2219/UE del Parlamento europeo e del Consiglio, *sull'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL) e che sostituisce e abroga la Decisione 2005/681/GAI del Consiglio*, del 25 novembre 2015, in GUUE L 319 del 4 dicembre 2015; Direttiva 2016/681/UE del Parlamento europeo e del Consiglio, *sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*, del 27 aprile 2016, in GUUE L 119 del 4 maggio 2016; Direttiva 2016/1148/UE del Parlamento europeo e del Consiglio, *recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*, del 6 luglio 2016, in GUUE L 194 del 19 luglio 2016; Direttiva 2017/541/UE del Parlamento europeo e del Consiglio, *sulla lotta contro il terrorismo e che sostituisce la Decisione quadro 2002/475/GAI del Consiglio e che modifica la Decisione 2005/671/GAI del Consiglio*, del 15 marzo 2017, in GUUE L 194 del 19 luglio 2016; Regolamento 2018/1726/UE del Parlamento europeo e del Consiglio, *relativo all'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA), che modifica il Regolamento (CE) n. 1987/2006 e la Decisione 2007/533/GAI del Consiglio e che abroga il Regolamento (UE) n. 1077/2011, applicabile dall'11 dicembre 2018*, del 14 novembre 2018, in GUUE L 295 del 21 novembre 2018; Regolamento 2018/1862/UE del Parlamento europeo e del Consiglio, *sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la Decisione 2007/533/GAI del Consiglio e che abroga il Regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la Decisione 2010/261/UE della Commissione, applicabile dal 28 dicembre 2021, al più tardi*, del 28 novembre 2018, in GUUE L 312 del 7 dicembre 2018; Regolamento 2019/818/UE del Parlamento europeo e del Consiglio, *che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/81*, del 20 maggio 2019, in GUUE L 135 del 22 maggio 2019; Direttiva 1153/2019/UE del Parlamento europeo e del Consiglio, *che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati e che abroga la Decisione 2000/642/GAI del Consiglio*, del 20 giugno 2019, in GUUE L 186 dell'11 luglio 2019; Direttiva 2021/555/UE del Parlamento europeo e del Consiglio, *relativa al controllo dell'acquisizione e della detenzione di armi (codificazione)*, del 24 marzo 2021, in GUUE L 115

alla protezione delle infrastrutture critiche[37], oltre che la recente strategia per la sicurezza interna *ProtectEU*, presentata il primo aprile 2025, che definisce gli obiettivi e le azioni per i prossimi anni per garantire un'Europa più sicura e protetta, aumentando la capacità degli Stati membri di proteggere le società e le democrazie dalle minacce online e offline provenienti da terroristi, criminali e attori stranieri ostili[38].

Quanto alla giurisprudenza, il bilanciamento delle esigenze di sicurezza nazionale con la tutela delle garanzie fondamentali – in particolare il diritto alla protezione dei dati personali sancito nell'articolo 8 della Carta dei Diritti Fondamentali dell'Unione Europea – ha impegnato da tempo la Corte di Giustizia. L'interferenza tra la protezione dei dati e le azioni di *intelligence* per la sicurezza è emersa nelle note cause *Schrems I* del 2015[39] e *Schrems II* del 2020[40] (che hanno comportato l'invalidazione dei meccanismi che facilitavano il trasferimento di dati verso gli Stati Uniti) e *Privacy International*, *La Quadrature du Net*, *French Data Network e Ordre des Barreaux Francophones et Germanophone del 2020* (sulla conservazione dei dati in relazione alle norme britanniche, francesi e belghe rispettivamente[41]).

---

del 6 aprile 2021; Regolamento 2021/784/UE del Parlamento europeo e del Consiglio, *relativo al contrasto della diffusione di contenuti terroristici online, applicabile dal 7 giugno 2022*, del 20 aprile 2021, in GUUE L 17 maggio 2021; Regolamento 2022/991/UE del Parlamento europeo e del Consiglio, *che modifica il Regolamento (UE) 2016/794 per quanto riguarda la cooperazione di Europol con le parti private, il trattamento dei dati personali da parte di Europol a sostegno di indagini penali e il ruolo di Europol in materia di ricerca e innovazione*, dell'8 giugno 2022, in GUUE L 169 del 27 giugno 2022; Direttiva (UE) 2022/2555, cit.; Direttiva 2022/2557/UE del Parlamento europeo e del Consiglio, *relativa alla resilienza dei soggetti critici e che abroga la Direttiva 2008/114/CE del Consiglio*, del 14 dicembre 2022, in GUUE L 333 del 27 dicembre 2024; Direttiva 2023/977/UE, *relativa allo scambio di informazioni tra le autorità di contrasto degli Stati membri e che abroga la Decisione quadro 2006/960/GAI del Consiglio*, del 10 maggio 2023, in GUUE L 134 del 22 maggio 2023; Regolamento 2023/2131/UE del Parlamento europeo e del Consiglio, *che modifica il Regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio e la Decisione 2005/671/GAI del Consiglio per quanto riguarda lo scambio digitale di informazioni nei casi di terrorismo, applicabile a decorrere dal 31 ottobre 2023*, del 4 ottobre 2023, in GUUE L 2131 dell'11 ottobre 2023; Regolamento 2024/982/UE del Parlamento europeo e del Consiglio, *sulla consultazione e lo scambio automatizzati di dati per la cooperazione di polizia (Regolamento Prüm II), applicabile dal 25 aprile 2024; Regolamento (UE) 2025/13 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, sulla raccolta e sul trasferimento di informazioni anticipate sui passeggeri a fini di prevenzione, accertamento, indagine e azione penale riguardo ai reati di terrorismo e ai reati gravi, applicabile dal 28 gennaio 2025*, del 13 marzo 2024, in GUUE 982 del 5 aprile 2024.

[37] Si veda la Direttiva 2022/2557/UE, cit.

[38] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *ProtectEU: una strategia europea per la sicurezza interna*, Com(2025)148, 1° aprile 2025. Si vedano Y. LLEDO-FERRER, J.-H. DIETRICHT, *Building a European Intelligence Community*, in *International Journal of Intelligence and CounterIntelligence*, 2020, n. 3 e M. SCHIRIPPA, *L'organizzazione ed il controllo parlamentare delle agenzie di intelligence europee: quali spazi per una cooperazione di intelligence comunitaria?*, in *DPCE online*, 2022, n. 3.

[39] Corte di giustizia dell'Unione europea, Grande Sezione, sentenza del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*.

[40] Corte di giustizia dell'Unione europea, Grande Sezione, sentenza del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Limited, Maximillian Schrems*.

[41] Corte di giustizia dell'Unione europea, Grande Sezione, sentenza del 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs e Igwan.net c. Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées* e *Ordre des barreaux francophones et germanophone*,

In queste ultime decisioni, il Giudice di Lussemburgo ha statuito che l'articolo 15, paragrafo 1, della Direttiva 2002/58/CE (volta a garantire la riservatezza delle comunicazioni elettroniche e a vietare l'archiviazione dei dati sul traffico e sulla localizzazione[42]) non osta a una normativa nazionale che imponga ai fornitori il ricorso all'analisi automatizzata e alla raccolta in tempo reale di tali dati. Ciò purché la misura sia tassativamente circoscritta a situazioni di minaccia grave, reale, attuale o prevedibile per la sicurezza nazionale, e sottoposta al controllo effettivo di un giudice o di un'autorità amministrativa indipendente. Parimenti, la raccolta in tempo reale deve limitarsi ai soggetti nei cui confronti sussista un valido motivo di sospetto circa il coinvolgimento in attività terroristiche, restando subordinata a un vaglio preventivo volto ad accertare la stretta necessità della misura[43].

La Corte ha adottato tale soluzione interpretando la Direttiva alla luce delle garanzie della Carta sancite dall'articolo 7 (rispetto della vita privata e familiare), dall'articolo 8 (protezione dei dati personali), dall'articolo 11 (libertà di espressione e di informazione) e dall'articolo 52, paragrafo 1 (che fissa le condizioni di legittimità per qualsiasi limitazione dei diritti, basandole sui criteri di stretta necessità e proporzionalità)[44].

Questo orientamento giurisprudenziale delinea la necessità di un rigoroso bilanciamento che rifiuta l'adozione di deroghe indiscriminate, inserendosi nel solco già tracciato dalle fondamentali pronunce rese dalla Corte nei casi *Digital Rights Ireland*[45] e *Tele2 Sverige*[46]. In tali sentenze, infatti, il giudice europeo aveva sancito che

---

Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX c. Conseil des ministres.

[42] Direttiva 2002/58/CE, cit.

[43] Corte di giustizia dell'Unione europea, sentenza del 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, cit., punto 229.

[44] *Id.*

[45] Corte di giustizia dell'Unione europea, Grande Sezione, sentenza dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung e altri*, riguardante la conservazione di dati relativi a comunicazioni elettroniche da parte delle autorità irlandesi. Nella sentenza la Corte invalida la direttiva 2006/24/CE del Parlamento europeo e del Consiglio, *riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, cit., poiché, al punto 37, la Corte ha constatato che «*l'ingerenza che la direttiva 2006/24 comporta nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta si rivela essere […] di vasta portata e va considerata particolarmente grave. Inoltre, il fatto che la conservazione dei dati e l'utilizzo ulteriore degli stessi siano effettuati senza che l'abbonato o l'utente registrato ne siano informati può ingenerare nelle persone interessate […] la sensazione che la loro vita privata sia oggetto di costante sorveglianza*» in quanto in violazione dell'articolo 8 (3) della Carta di Nizza.

[46] Corte di giustizia dell'Unione europea, Grande Sezione, sentenza del 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB c. Post- och telestyrelsen* e *Secretary of State for the Home Department c. Tom Watson, Peter Brice e Geoffrey Lewis*, sull'accusa da parte delle autorità svedesi nei confronti di Tele2 Sverige AB riguardante la conservazione dei dati da parte del *service provider*. Nella sentenza, al punto 112, la Corte specifica che l'articolo 15 (1) della Direttiva 2002/58/CE (del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009), alla luce degli articoli 7, 8, 11 e 52 (1) della Carta di Nizza «*deve essere interpretato nel senso che esso osta ad una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi*

l'archiviazione generalizzata dei metadati genera un'ingerenza congiunta: da un lato, lede il diritto al rispetto della vita privata poiché consente di ricavare proiezioni dettagliate sulle abitudini e sulle relazioni dei singoli; dall'altro, viola la libertà di espressione a causa dell'effetto dissuasivo che la costante tracciabilità statale produce sulla libertà di comunicazione dei consociati. Esigendo il rispetto dei medesimi parametri per le attività di *intelligence*, le decisioni del 2020 confermano che la deroga ai diritti fondamentali non può risolversi nella compressione di tali tutele fondamentali, che restano subordinate al citato principio di proporzionalità[47].

3. Criminalità transnazionale, approccio repressivo e diritti umani

Dall'esame del richiamato quadro normativo e giurisprudenziale emerge che uno dei principali rischi per la sicurezza (nazionale ed internazionale) è costituito dai crimini transnazionali che non conoscono confini e rappresentano una minaccia significativa per i cittadini, le imprese, le istituzioni e l'economia nel suo complesso[48]. Comunemente, il quadro giuridico per contrastare i crimini transnazionali viene applicato attraverso meccanismi prevalentemente repressivi, espressione di un *criminal justice approach*, che caratterizza i principali strumenti normativi sul punto, quali la Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale (Convenzione di Palermo) del 2000[49] (cui si deve la definizione dei reati di natura transnazionale contenuta nell'articolo

all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica». In dottrina si veda M. NINO, *op. cit.*

[47] *Supra*, note 45 e 46.

[48] Si veda la valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità dell'Unione europea (European Union Serious and Organised Crime Threat Assessment, SOCTA dell'UE) del 2021. EUROPOL, *EU SOCTA 2021*, 12 aprile 2021: https://www.europol.europa.eu/activities-services/mainreports/european-union-serious-and-organised-crime-threat-assessment. La SOCTA dell'UE è un'analisi completa della minaccia rappresentata dalla criminalità organizzata, che identifica le aree di criminalità a priorità elevata ed è elaborata ogni quattro anni da Europol sulla base dei contributi forniti dagli Stati membri. Si veda anche la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025*, COM(2021) 170 final, 19 aprile 2021.

[49] L'UNTOC, adottata con la Risoluzione dell'Assemblea generale delle Nazioni Unite 55/25, del 15 novembre 2000, è entrata in vigore il 29 settembre 2003 ed è stata successivamente integrata da tre protocolli, che disciplinano specifiche aree e forme d'espressione della criminalità organizzata, ovvero: 1) il Protocollo sulla prevenzione, soppressione e persecuzione del traffico di esseri umani, in particolar modo donne e bambini, adottato con la Risoluzione dell'Assemblea generale delle Nazioni Unite 55/25, del 15 novembre 2000 ed entrato in vigore il 25 dicembre 2003; 2) il Protocollo contro il traffico di migranti via terra, mare e aria, adottato con la Risoluzione dell'Assemblea generale delle Nazioni Unite 55/25, del 15 novembre 2000 ed entrato in vigore il 28 gennaio 2004; e 3) il Protocollo contro la fabbricazione e il traffico illeciti di armi da fuoco, loro parti e componenti e munizioni, adottato con la Risoluzione dell'Assemblea generale delle Nazioni Unite 55/255, del 31 maggio 2001 ed entrato in vigore il 3 luglio 2005. Per un commento si veda M.A. ACCILI SABBATINI, A. BALSAMO, *Verso un nuovo ruolo della Convenzione di Palermo nel contrasto alla criminalità transnazionale*, in *Diritto Penale Contemporaneo*, 2018, n. 12.

3)[50], il Trattato sul Funzionamento dell'Unione europea (TFUE) e in particolare gli articoli 82, 83 (sulla competenza penale dell'UE in materia processuale e sostanziale[51]) e 86 (sulla istituzione della Procura europea (EPPO) per combattere i reati gravi che ledono gli interessi finanziari dell'Unione[52]) e le numerose Convenzioni adottate in seno al Consiglio d'Europa, tra cui la Convenzione sulla criminalità informatica del 2001[53], la Convenzione sulla lotta contro la tratta di esseri umani del 2005[54], la Convenzione di Nicosia contro il traffico illecito di beni culturali del 2017[55] e la recente Convenzione sulla protezione dell'ambiente attraverso il diritto penale (2025)[56].

Alla proliferazione normativa (internazionale ed europea) diretta a prevenire e sanzionare i crimini transnazionali per garantire la sicurezza nazionale ed internazionale non ha corrisposto, però, l'adozione di un sistema omogeneo di tutela dei diritti umani delle persone interessate, a diverso titolo, dalle misure di contrasto alla criminalità. Nel perseguimento degli obiettivi di sicurezza contro i reati transnazionali, il diritto internazionale ed europeo lascia apparentemente ampio margine alle autorità nazionali a discapito dell'applicazione uniforme di principi e valori generali, come le garanzie connesse allo Stato di diritto (sostanziale[57]). L'esame della prassi evidenzia, peraltro, che la disomogeneità tra i differenti sistemi giuridici nazionali – in relazione, sia alla

[50] Ai sensi dell'articolo 3, par. 2 UNTOC, un reato è di natura transnazionale se: a) è commesso in più di uno Stato; b) è commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo ha luogo in un altro Stato; c) è commesso in uno Stato, ma coinvolge un gruppo criminale organizzato che svolge attività criminali in più di uno Stato; d) è commesso in uno Stato, ma produce effetti sostanziali in un altro Stato.

[51] N. PERŠAK, *Criminalising Hate Crime and Hate Speech at EU Level: Extending the List of Eurocrimes Under Article 83(1) TFEU*, *Criminal Law Forum*, 2022, n. 33; A. ORIOLO, A. R. CASTALDO, A. DI STASI, M. NINO (a cura di), *Criminalità transnazionale e Unione europea*, Napoli, 2024.

[52] Regolamento 2017/1939/UE del Consiglio, *relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea ("EPPO")*, del 12 ottobre 2017, in GUUE L 283 del 31 ottobre 2017. Per un commento sull'atto si vedano N. PARISI, *La Procura europea: un tassello per lo spazio europeo di giustizia penale*, *Studi sull'Integrazione Europea*, 2013, n. 8; S. ALLEGREZZA, *Statuto e poteri del Pubblico ministero europeo*, in *I nuovi orizzonti della giustizia penale europea*, Milano, 2015; P. FERRUA, R. GAMBINI, M. SALVADORI (a cura di), *La Nuova Procura Europea. Indipendenza, Coordinamento tra Stati e tutela dei diritti dell'uomo*, Napoli, 2016; L. BACHMAIER WINTER (ed.), *The European Public Prosecutor's Office. The Challenges Ahead*, Cham, 2018; W. GEELHOED, L. H. ERKELENS, A. W.H. MEIJ (eds.), *Shifting Perspectives on the European Public Prosecutor's Office*, Berlino, 22018; A. ORIOLO, *The European Public Prosecutor's Office (EPPO): A Revolutionary Step in Fighting Serious Transnational Crimes*, in *ASIL Insights*, 2018, n. 4.

[53] M. O'NEILL, *The Transnational Crime of Human Trafficking, A Human Security Approach*, Abingdon-on-Thames, 2023.

[54] M.A. VATIS, *The Council of Europe Convention on Cybercrime*, in *Proceedings of a Workshop on Deterring Cyberattacks Informing Strategies and Developing Options for U.S. Policy*, 2010.

[55] A. ORIOLO, *Reati contro il patrimonio culturale, criminalità transnazionale e ordinamento italiano: l'adeguamento agli standard della Convenzione di Nicosia*, in *Quaderni SIDI*, 2022, n. 9, pp. 287-304.

[56] D. BERTRAM, *The First Ecocide Treaty?*, in *EJIL:Talk*, 2025.

[57] Mentre nella sua caratterizzazione formale, il principio dello Stato attiene al modo (procedimento) in cui la legge è promulgata (dall'organo competente nel rispetto delle norme) e amministrata (attraverso un sistema giudiziario indipendente) e alla sua chiarezza (tale da guidare correttamente la condotta di un individuo nella pianificazione della propria vita), nella sua concezione sostanziale tale principio comporta (anche) che la legge debba essere "giusta", ovvero incorporare gli ideali di giustizia, equità e rispetto dei diritti fondamentali. P. CRAIG, *Formal and Substantive Conceptions of the Rule of Law: An Analytical Framework*, in *Public Law*, 1997.

individuazione stessa delle garanzie da tutelare in quanto diritti fondamentali degli individui, sia alla interpretazione del contenuto e della portata di tali diritti, sia, infine, alla scelta dei parametri da utilizzare nel bilanciamento tra queste garanzie (individuali) ed altri interessi (più generali), quale quello della sicurezza[58] – si traduce anche nell'assenza di criteri univoci cui ancorare la protezione dei diritti dei singoli nel contrasto ai crimini transnazionali.

Sicché, parte della dottrina ha esaminato anche l'efficacia di un differente approccio nel contrasto ai crimini transnazionali incentrato sui diritti degli individui e sulla loro capacità di rivendicarne il rispetto, la protezione e la promozione imposti agli Stati dalle norme internazionali ed europee anche nella lotta ai *cross-border crimes*[59]: il c.d. *human rights-based approach*[60].

Tale approccio postula che i diritti fondamentali dell'individuo non costituiscano meri vincoli negativi o eccezioni all'esercizio dei poteri sovrani, bensì i criteri direttivi, intrinseci e inderogabili che devono strutturare ogni azione pubblica, inclusa la tutela della sicurezza dello Stato. In questa prospettiva, la sicurezza nazionale non è configurata come un valore confliggente con le garanzie individuali, ma come uno strumento funzionale alla protezione delle libertà stesse.

Tuttavia, la tenuta di questo approccio fondato sulla preminenza dei diritti umani rischia di subire una progressiva e profonda compromissione dinanzi a due dinamiche tra loro interconnesse, destinate a ridefinire i confini della sovranità statale: la gestione delle situazioni di emergenza e l'avvento delle nuove tecnologie.

3.1. Diritti umani e situazioni di emergenza

Ai diritti umani nelle situazioni di emergenza è dedicato l'articolo 4 del Patto delle Nazioni Unite sui diritti civili e politici (ICCPR) del 1966, che prevede deroghe alle garanzie individuali (approfondite nei cosiddetti Principi di Siracusa[61]), per i casi di "pericolo pubblico eccezionale", senza però ledere alcuni diritti fondamentalismi quali il diritto alla vita, al divieto di tortura e schiavitù, alla libertà di pensiero, di coscienza e di

[58] N. DE BOER, *Addressing Rights Divergences under the Charter: Melloni*, in *Common Market Law Review*, 2013, n. 50.
[59] A. PETERS, *Corruption as a Violation of International Human Rights*, in *European Journal of International Law*, 2018, n. 4.
[60] R. HEMSLEY, *Human Rights & Corruption States' Human Rights Obligation to fight Corruption*, in *Journal of Transnational Legal Issues*, 2018, n. 1; O. MERKELE, *Mainstreaming gender and human rights in anti-corruption programming*, 2018; A. PETERS, cit.
[61] Consiglio economico e sociale delle Nazioni Unite, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, E/CN.4/1985/4, Annex, 1985.

religione[62]. Analogamente, l'articolo 15 della CEDU[63] prevede deroghe alle garanzie individuali presenti anche nell'articolo G della Carta sociale europea del 1996[64], nell'articolo 26 della Convenzione sui diritti umani e la biomedicina (Convenzione di Oviedo) del 1997[65] e nell'articolo 11 della citata Convenzione 108 del Consiglio d'Europa[66]. Quanto all'Unione europea, limitazioni generali all'esercizio dei diritti garantiti dalla Carta dei diritti fondamentali, ai sensi dell'articolo 52, «*devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà*», possono essere apportate solo «*laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*», nel rispetto del principio di proporzionalità[67].

Tra i pericoli pubblici in grado di determinare una limitazione delle garanzie individuali va senza dubbio citata l'emergenza sanitaria[68]: la recente pandemia da

---

[62] «*1. In caso di pericolo pubblico eccezionale, che minacci l'esistenza della nazione e venga proclamato un atto ufficiale, gli Stati Parti del presente Patto possono prendere misure le quali deroghino agli obblighi imposti dal presente Patto, nei limiti in cui la situazione strettamente lo esiga, e purché tali misure non siano incompatibili con gli altri obblighi imposti agli Stati medesimi dal diritto internazionale e non comportino una discriminazione fondata unicamente sulla razza, sul colore, sul sesso, sulla lingua, sulla religione o sull'origine sociale. 2. La suddetta disposizione non autorizza alcuna deroga agli articoli 6, 7, 8 (paragrafi 1 e 2), 11, 15, 16 e 18*». Si veda Comitato per i diritti umani delle Nazioni Unite, *General comment no. 29, States of emergency (article 4): International Covenant on Civil and Political Rights*, CCPR/C/21/Rev.1/Add.11, 31 agosto 2001.

[63] Il testo dell'articolo 15 riprende quello del progetto di articolo 4 del Progetto di patto delle Nazioni Unite relativo ai diritti umani, che è divenuto in seguito l'articolo 4 del Patto internazionale relativo ai diritti civili e politici. Si veda la pagina 10 e l'allegato I ai lavori preparatori sull'articolo 15 (*document DH (56)4* disponibile sul sito web della Biblioteca della Corte di Strasburgo: www.echr.coe.int/Library). Anche la Convenzione americana relativa ai diritti umani contiene una clausola derogatoria (l'articolo 27). Invece, non ve ne sono nella Carta africana dei diritti dell'uomo e dei popoli.

[64] «*1. I diritti ed i principi enunciati nella parte I, quando saranno effettivamente attuati, e l'esercizio effettivo di tali diritti e principi come previsto nella parte II, non potranno essere oggetto di restrizioni o di limitazioni non specificate nelle parti I e II ad eccezione di quelle stabilite dalla legge e che sono necessarie, in una società democratica, per garantire il rispetto dei diritti e delle libertà altrui o per proteggere l'ordine pubblico, la sicurezza nazionale, la salute pubblica o il buon costume. 2 Le restrizioni apportate, in virtù della presente Carta, ai diritti ed agli obblighi ivi riconosciuti possono essere applicate solo per gli scopi per i quali sono stati previste*». Carta sociale europea (riveduta) (STE no. 163), 1996.

[65] «*1 L'esercizio dei diritti e le disposizioni di tutela contenute nella presente Convenzione non possono essere oggetto di altre restrizioni all'infuori di quelle che, previste dalla legge, costituiscono delle misure necessarie, in una società democratica, alla sicurezza pubblica, alla prevenzione delle infrazioni penali, alla protezione della salute pubblica o alla protezione dei diritti e libertà altrui. 2 Le restrizioni di cui all'alinea precedente non possono essere applicate agli articoli 11, 13, 14, 16, 17, 19, 20 e 21*». Convenzione per la protezione dei diritti dell'uomo e della dignità dell'essere umano nei confronti dell'applicazioni della biologia e della medicina: Convenzione sui diritti dell'uomo e la biomedicina (STE no. 164), 1997.

[66] Articolo 11 Protezione più estesa: «*Nessuna delle disposizioni del presente capitolo sarà interpretata come limitante o altrimenti recante pregiudizio alla facoltà di ciascuna Parte di accordare alle persone interessate una protezione più vasta di quella prevista dalla presente Convenzione*».

[67] Si vedano T. TRIDIMAS, *The Principle of Proportionality*, in R. SCHÜTZE, T. TRIDIMAS (eds.), *Oxford Principles Of European Union Law: The European Union Legal Order: Volume I*, Oxford, 2018; R. PALLADINO, *Il principio di proporzionalità nel diritto dell'Unione europea. Natura, funzioni e controllo*, Bari, 2024.

[68] L.O GOSTIN, E. A. FRIEDMAN, S. HOSSAIN, J. MUKHERJEE, S. ZIA-ZARIFI, C. CLINTON, U. RUGEGE, P. BUSS, M. WERE, A. DHAI, *Human rights and the COVID-19 pandemic: a retrospective and prospective analysis*, in *The Lancet*, 2023, n. 10371. Sul tema si vedano anche: N. SUN, *Applying Siracusa: A Call for*

COVID-19 ha portato all'esame della Corte di Strasburgo numerosi casi di violazione delle disposizioni convenzionali dovute alla gestione "statale" del pericolo pandemico relativi, in particolare, alla lamentata violazione degli articoli 3[69], 5[70], 6[71], 8[72], 9[73] e 11[74] della CEDU.

Anche la Corte di giustizia dell'Unione europea si è pronunciata sulle restrizioni alla libertà di movimento[75], all'accesso alle istituzioni europee[76] e alla protezione dei dati e alla privacy, connesse alle misure di tutela della salute pubblica adottate durante l'emergenza sanitaria[77].

La criminalità transnazionale prospera anche e soprattutto in contesti di conflitto armato favorendo i traffici illeciti di esseri umani armi, droga, beni culturali, specie protette e il terrorismo che da tali traffici trae le principali fonti di finanziamento. Con la globalizzazione dei conflitti e la comune caratteristica transnazionale delle citate minacce criminali, i servizi di *intelligence* possono spesso ricorrere a risorse specializzate o ad accessi specifici per acquisire dati, in violazione dei diritti dei singoli. In tali casi, la sorveglianza da parte dei servizi di *intelligence* differisce in diversi modi dalla

---

a General Comment on Public Health Emergencies, in *Health and Human Rights Journal*, 2020, n. 1; M. KJAERUM, M. F. DAVIS, A. LYONS (eds.), *COVID-19 and Human Rights*, Londra, 2021; D. A. GOZDECKA, *Human Rights During the Pandemic: COVID-19 and Securitisation of Health*, in *Nordic Journal of Human Rights*, 2021, n. 3. Sull'applicazione dei Principi di Siracusa nell'ambito delle emergenze sanitarie prima della pandemia di COVID-19 si veda: K.W. TODRYS, E. HOWE, J.J. AMON, *Failing Siracusa: governments' obligations to find the least restrictive options for tuberculosis control*, in *Public Health Action*, 2013, n. 1. Sull'applicazione dei Principi di Siracusa nell'ambito delle emergenze sanitarie prima della pandemia di COVID-19 si vedano: K.W. TODRYS, E. HOWE, J.J. AMON, *op. cit.*; L. FORMAN, *The fragile relationship between the amended International Health Regulations and human rights law*, in *The International Journal of Human Rights*, 2025, n. 7. Si veda anche: L. FORMAN, J. BUENO DE MESQUITA, L. BOTTINI FILHO, B. M. MEIER, M. SIRLEAF, *How Did Human Rights Fare in Amendments to the International Health Regulations?*, in *The Journal of Law, Medicine & Ethics*, 2024; G. CAGGIANO, *COVID-19. Competenze dell'Unione, libertà di circolazione e diritti umani in materia di controlli delle frontiere, misure restrittive della mobilità e protezione internazionale*, in *I Post di AISDUE*, 2020; D. THYM, J. BORNEMANN, *Schengen and Free Movement Law During the First Phase of the Covid-19 Pandemic: Of Symbolism, Law and Politics*, in *European Papers*, 2020, n. 3; H. VAN EIJKEN, J. RIJPMA, *Stopping a Virus from Moving Freely: Border Controls and Travel Restrictions in Times of Corona*, *Utrecht Law Review*, 2021, n. 3.

[69] Corte europea dei diritti dell'uomo, sentenza dell'11 marzo, ricorso n. 6865/19, *Feilazzoo c. Malta*.

[70] Corte europea dei diritti dell'uomo, sentenza del 13 giugno 2023, ricorso n. 53114/20, *Khokhlov c. Cipro*.

[71] Corte europea dei diritti dell'uomo, sentenza dell'8 febbraio 2022, ricorso n. 19937/20, *Q e R c. Slovenia*.

[72] Corte europea dei diritti dell'uomo, sentenza del 19 dicembre 2023, ricorso n. 14139/21, *Narbutas c. Lituania*; sentenza del 16 maggio 2024, ricorsi nn. 512/21, 57755/21, 59365/21, 61086/21, 17889/23, *riuniti Crăciun e altri c. Romania*.

[73] Corte europea dei diritti dell'uomo, sentenza dell'11 ottobre 2022, ricorso n. 29443/20, *Constantin-Lucian Spînu c. Romania*.

[74] Corte europea dei diritti dell'uomo, sentenza del17 ottobre 2024, ricorso del n. 49363/20, *Central Unitaria de Traballadores/AS c. Spagna*.

[75] Corte di giustizia dell'Unione europea, Grande Sezione, sentenza del 5 dicembre 2023, causa C-128/22, *Nordic Info BV c. Belgische Staat*.

[76] Corte di giustizia dell'Unione europea, sentenza del 27 aprile 2022, cause riunite T-710/21, T-722/21 and T-723/21, *Robert Roos e a. c. Parlamento europeo*.

[77] Corte di giustizia dell'Unione europea, sentenza del 5 ottobre 2023, causa C-659/22, *UC c. Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)*; Grande Sezione, sentenza del 5 dicembre 2023, causa 6-863/21, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos c. Valstybinė duomenų apsaugos inspekcija*; sentenza del 28 novembre 2024, causa C-169/23, *Nemzeti Adatvédelmi és Információszabadság Hatóság c. UC*.

sorveglianza nelle forze dell'ordine o nelle operazioni di sicurezza interna più tradizionali. Non si inizia necessariamente con un sospetto nei confronti di una o più persone in particolare: l'obiettivo è spesso *trovare* un pericolo piuttosto che indagare su un pericolo noto (approccio *target-free* o *intelligence-led*[78]). L'azione penale non è, quindi, lo scopo principale della raccolta di informazioni che vengono conservate e utilizzate in una serie di modi che possono incidere sui diritti umani[79].

3.2. Sicurezza, diritti umani e nuove tecnologie

Il tema dei rapporti tra sicurezza e nuove tecnologie risultava degno di nota già agli estensori della Convenzione di Palermo del 2000 che, all'articolo 27 paragrafo 3, impegna gli Stati parte a «*cooperare con i propri mezzi per fronteggiare il crimine organizzato transnazionale perpetrato attraverso l'uso della moderna tecnologia*», riconoscendo al paragrafo 1 dell'articolo 20 il ricorso a «*tecniche speciali di investigazione, quali la sorveglianza elettronica*» e, all'articolo 29, lo sviluppo di programmi di formazione del personale. Similmente, l'articolo 4 paragrafo 9 del II Protocollo addizionale del 2001 alla Convenzione europea di assistenza giudiziaria in materia penale del 1959[80] ha introdotto la possibilità di effettuare, tramite i mezzi di telecomunicazione, le comunicazioni relative all'assistenza giudiziaria.

Nel diritto dell'Unione europea sono numerose le disposizioni in materia di assistenza giudiziaria tra gli Stati membri e uso della tecnologia nel contrasto alla criminalità (transnazionale in generale e cibernetica in particolare), riguardanti, ad esempio, la produzione e la conservazione delle prove elettroniche[81], lo scambio automatizzato di dati per la lotta ai reati transfrontalieri[82], le definizioni dei limiti riguardanti le intercettazioni

[78] Sul tema si vedano: W. DE LINT, *Intelligence in Policing and Security: Reflections on scholarship*, in *Policing and Society*, 2006, n. 1; E.F. MCGARRELL, J.D. FREILICH, S. CHERMAK, *Intelligence-Led Policing as a Framework for Responding to Terrorism*, in *Journal of Contemporary Criminal Justice*, 2007, n. 2 e J. H. RATCLIFFE, *Intelligence-Led Policing*, III ed., Abingdon-on-Thames, 2026.

[79] European Commission for Democracy Through Law (Venice Commission), *Report on the Democratic Oversight of Signals Intelligence Agencies*, Study N. 719/2013, 15 dicembre 2015, par. 3.

[80] Secondo Protocollo addizionale alla Convenzione europea di assistenza giudiziaria in materia penale, 2001.

[81] Regolamento 2023/1543/UE, *relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali e Direttiva (UE) 2023/1544, del 12 luglio 2023, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali*, del 12 luglio 2023, in GUUE L 191 del 28 luglio 2023. Sul tema si veda S. BUSILLO, *Conservazione e produzione della prova digitale nella nuova disciplina europea: il potenziale disallineamento con i principi espressi dalla giurisprudenza di settore*, in questa *Rivista*, 2023, n. 3.

[82] Decisione 2008/615/GAI del Consiglio *sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera*, del 23 giugno 2008, in GUUE L 210 del 6 agosto 2008 e il Regolamento 2024/982/UE, cit.

e i dati personali[83]; questioni che, si è detto, sono state al centro di numerose pronunce della Corte di giustizia[84].

In questo perimetro, emerge come coordinata strutturale ed elemento di indiscutibile rilievo la nascita dei nuovi ambiti di operatività delle attività criminali legati alle c.d. *cognitive weapons*, caratterizzate dalla "criminalizzazione digitale" dei media e della comunicazione attraverso l'*hate speech* e azioni di *disinformation* e *misinformation*[85].

Si evidenzia, parimenti, lo stretto nesso normativo esistente tra la digitalizzazione della giustizia penale e l'uso di algoritmi predittivi da parte delle stesse autorità informative, ambiti che si configurano come elementi di spiccata complessità sul terreno della tutela delle garanzie individuali[86].

4. Verso una *intelligence* comune nell'Unione europea?

In forza delle limitazioni all'azione in materia di sicurezza previste dall'articolo 4, paragrafo 2, del TUE, l'Unione non dispone (ancora) di un'agenzia di *intelligence* operativa sul modello di quelle degli Stati membri.

In Italia, ad esempio, i servizi di *intelligence* sono organizzati in due agenzie distinte: l'Agenzia informazioni e sicurezza interna (AISI) e l'Agenzia informazioni e sicurezza esterna (AISE), facenti parte del Sistema di informazione per la sicurezza della Repubblica (SISR) e coordinate dal Dipartimento delle informazioni per la sicurezza (DIS) ai sensi della Legge 3 agosto 2007, n. 124[87].

L'istituzione più vicina a un'agenzia di *intelligence* civile europea è l'*EU Intelligence and Situation Centre* (INTCEN[88]), istituito nella sua veste attuale come evoluzione del

[83] Direttiva 2002/58/CE, cit.; Regolamento (UE) 2016/679, cit.; Regolamento (UE) 2022/991, cit.

[84] Si vedano, tra le altre: Corte di giustizia dell'Unione europea, Grande Sezione, sentenza dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd*; Grande Sezione, sentenza del 2 ottobre 2018, causa C-207/16, *Ministerio Fiscal*; Grande Sezione, sentenza del 6 marzo 2021, causa C-746/18, *Prokuratuur*.

[85] Si vedano: I. IGLEZAKIS, *The Legal Regulation of Hate Speech on the Internet*, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU, T. PRASTITOU (eds.), *EU Internet Law Regulation and Enforcement*, Berlin, Heidelberg, New York, 2017, pp. 367-383; M. GREGOR, P. MLEJNKOVÁ, *Explaining the Challenge: From Persuasion to Relativisation*, in M. GREGOR, P. MLEJNKOVÁ (eds.), *Challenging Online Propaganda and Disinformation in the 21st Century*, Cham, 2021, pp. 3-41; A. GAETA, V. LOIA, F. ORCIUOLI, A. PASCUZZO, Information Disorder, Cognitive Weapons *e crimini transnazionali: scenari, sfide e possibili soluzioni*, in A. ORIOLO, A.R. CASTALDO, A. DI STASI, M. NINO (a cura di), *Criminalità transnazionale e Unione europea*, *op. cit*., pp. 703-715.

[86] Sul tema si vedano: A. ZAVRŠNIK, *Algorithmic justice: Algorithms and big data in criminal justice settings*, in E*uropean Journal of Criminology*, 2019, n. 5; A. ZAVRŠNIK, *Criminal justice, artificial intelligence systems, and human rights*, in *ERA Forum*, 2020, n. 20; S. BRAYNE, A. CHRISTIN, *Technologies of Crime Prediction: The Reception of Algorithm in Policing and Criminal Courts*, in *Social Problems*, 2021, n. 3; M. G. ZAKARIA, *AI Applications in the Criminal Justice System: The Next Logical Step or Violation of Human Rights*, in *Journal of Law & Emerging Technologies*, 2020, n. 2.

[87] Sulla riforma del 2007 si veda T. F. GIUPPONI, *Servizi di informazione e segreto di Stato nella legge n. 124/2007*, in *Studi in onore di Luigi Arcidiacono - Vol. IV*, Torino, 2011, pp. 1677-1751.

[88] La base normativa per l'istituzione dell'INTCEN è la Decisione 2010/427/UE del Consiglio *che fissa l'organizzazione e il funzionamento del servizio europeo per l'azione esterna*, del 26 luglio 2010, in GUUE

Centro congiunto di situazione (SITCEN[89]) e del Joint *Situation Centre* (JSC), nuclei originari sorti nel 2002[90]. L'INTCEN fa parte della Capacità unica di analisi dell'*intelligence* (SIAC) del Servizio europeo per l'azione esterna (SEAE), insieme alla Direzione dell'*intelligence* dello Stato maggiore dell'UE (EUMS INT), sotto la diretta autorità dell'Alto rappresentante per gli affari esteri e la politica di sicurezza[91].

L'INTCEN, a differenza delle agenzie nazionali, non raccoglie direttamente le informazioni tramite operazioni sul campo, ma le riceve da queste ultime, da organizzazioni non governative (ONG), da report diplomatici e da fonti aperte (OSINT). Esso ha il compito di fornire analisi di *intelligence*, preallarme (*early warning*) e consapevolezza della situazione (*situational awareness*) all'Alto rappresentante, al Consiglio, alla Commissione e ai decisori politici dell'Unione, basandosi sul principio del "need-to-know[92]" e sulla Decisione del Consiglio 2013/488/UE sulle norme di sicurezza per la tutela delle informazioni classificate UE[93]. Le analisi prodotte sono secretate e classificate come "informazioni classificate UE" (ICUE) su quattro livelli di segretezza in base all'articolo 2 della medesima decisione[94].

L 201del 3 agosto 2010. Risposta data dall'Alto Rappresentante/Vicepresidente Borrell per conto della Commissione europea alla domanda E-001243/2021.

[89] Consiglio dell'Unione europea, *Documento 9984/2/04 Rev 2 Confidentiel UE/EU Confidential su Counter-Terrorism: Intelligence Cooperation within an EU Framework*, par. 4.1. Il documento in questione è stato declassificato parzialmente il 24 ottobre 2012 grazie a una *freedom of information request*. Si vedano anche EU INTELLIGENCE NEWS DESK, *European Union Intelligence and Situation Centre (EU INTCEN): A Comprehensive Analysis*, in *EUIntelligence.com*, 2023 e P.P. SEYFRIED, *A European Intelligence Service? Potentials and Limits of Intelligence Cooperation at EU Level*, in *Federal Academy for Security Policy: Security Policy Working Papers*, 2017, n. 20.

[90] HOUSE OF LORDS, *European Union – Seventh Report: Appendix 5*, 2003.

[91] Risposta congiunta data dall'Alto Rappresentante/Vicepresidente Ashton per conto della Commissione europea alle domande E-006018/12, E-006020/12, 2012. La struttura è stata accusata di non essere abbastanza integrata, con le due agenzie che lavorerebbero come "silos paralleli" senza una reale integrazione, D. CATTLER, *The EU's Intelligence Debate: Capability First, Structures Last*, in *Rahvusvaheline Kaitseuuringute Keskus International Centre for Defence and Security*, 2025.

[92] In generale il principio del *need-to-know* si basa sul fornire informazioni confidenziali se e solo se la persona ha le adeguate autorizzazioni e *security clearance* ed ha la necessità di essere al corrente di queste informazioni per poter condurre il proprio compito, si veda U.S. DEPARTMENT OF DEFENSE, *DOD Dictionary of Military and Associated Terms*, 2017. Nel caso dell'*intelligence* europea i membri del Parlamento europeo possono presentare richiesta per ricevere briefing da parte dell'INTCEN solo dopo che le autorità nazionali del proprio Stato abbiano loro fornito una Personal Security Clearance. Risposta data dall'Alto Rappresentante/Vicepresidente Borrell, cit.

[93] Decisione 2013/488/UE del Consiglio *sulle norme di sicurezza per proteggere le informazioni classificate UE*, del 23 settembre 2013, in GUUE L 274 del 15 ottobre 2013.

[94] I livelli descritti al paragrafo 2 dell'articolo 4 sono: «*a) TRÈS SECRET UE/EU TOP SECRET: informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'Unione europea o di uno o più Stati membri; b) SECRET UE/EU SECRET: informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gravemente gli interessi fondamentali dell'Unione europea o di uno o più Stati membri; c) CONFIDENTIEL UE/EU CONFIDENTIAL: informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gli interessi fondamentali dell'Unione europea o di uno o più Stati membri; d) RESTREINT UE/EU RESTRICTED: informazioni e materiali la cui divulgazione non autorizzata potrebbe essere pregiudizievole per gli interessi dell'Unione europea o di uno o più Stati membri*». La segretezza dei report dell'INTCEN è stata criticata, *inter alia*, in C. JONES, *Secrecy reigns at the EU's Intelligence Analysis Centre*, in *Statewatch journal*, 2013, p. 4.

Un'applicazione recente di questo coordinamento analitico è il progetto di raccordo strategico tra l'INTCEN e il Centro di coordinamento della ciberdifesa dell'UE (EUDCC), formalizzato nella Comunicazione congiunta sulla politica di ciberdifesa del 2022[95]. La funzione dell'INTCEN è, però, rigidamente limitata al supporto informativo e strategico, escludendo le tradizionali attività esecutive o di infiltrazione delle agenzie nazionali, come ribadito nel 2021 dall'allora Alto rappresentante Josep Borrell in sede di risposta a un'interrogazione parlamentare[96]. Nonostante ciò, la prassi cooperativa del Centro ha permesso di uniformare e strutturare i canali di collegamento e i protocolli di scambio tra gli Stati membri.

Mentre nell'ambito della cooperazione giudiziaria e di polizia l'Unione si è dotata di strutture operative quali Europol[97] ed Eurojust[98], il comparto dell'*intelligence* mostra, peraltro, un minor grado di integrazione. Le mutate condizioni della sicurezza internazionale hanno tuttavia alimentato, negli ultimi decenni, diverse proposte di riforma strutturale. Già prima dell'istituzione del SITCEN, l'ipotesi di una politica di *intelligence* comune veniva considerata fonte di vantaggi operativi ed economici per le istituzioni comunitarie[99], scontrandosi però con storiche resistenze intergovernative (si pensi alla posizione contraria del Regno Unito espressa nel report della *House of Lords* del 2003-2004)[100]. Per superare lo stallo normativo, nel giugno 2004 l'Alto rappresentante Javier Solana presentò un progetto di cooperazione al Consiglio Giustizia e Affari interni. Il piano Solana, divenuto la base dell'assetto attuale, demandò al SITCEN la produzione di analisi macro-strategiche a supporto dei decisori politici di Bruxelles, incrementando la base informativa delle istituzioni ma salvaguardando l'esclusività operativa delle agenzie nazionali sul terreno[101].

La discussione ha subìto un'accelerazione a causa dell'ondata di attentati terroristici che ha colpito il territorio europeo nello scorso decennio[102]. Dinanzi a minacce transnazionali, il SEAE ha promosso una maggiore condivisione delle informazioni tra i servizi nazionali e gli organi centrali[103], sollecitando un sostegno strutturale a favore dell'INTCEN[104]. Un'analoga necessità di scambio informativo è emersa nelle conclusioni del Consiglio relative alla gestione della sicurezza interna durante la pandemia da

[95] Commissione europea, Comunicazione congiunta al Parlamento europeo e al Consiglio "*La politica di ciberdifesa dell'UE*" (JOIN/2022/49 final), 2022.
[96] Risposta data dall'Alto Rappresentante/Vicepresidente Borrell, cit.
[97] Regolamento UE 2016/794, cit.
[98] Regolamento UE 2018/1727/UE del Parlamento europeo e del Consiglio, *che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) e che sostituisce e abroga la decisione 2002/187/GAI del Consiglio*, del 14 novembre 2018, in GUUE L 295 del 21 novembre 2018.
[99] A. POLITI, *Perché è necessaria un'intelligence policy europea?*, in *Per Aspera Ad Veritatem*, 1998, n. 10.
[100] D. BLUNKETT, *Letter from Rt Hon David Blunkett MP, Home Secretary, Home Office to the Chairman*, 2004.
[101] Summary of remarks by Javier SOLANA, EU High Representative for the CFSP, *on Terrorism and Intelligence Co-operation*, 2004.
[102] P.P. SEYFRIED, *op. cit.*, p. 1.
[103] SERVIZIO EUROPEO PER L'AZIONE ESTERNA, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy*, 2016, p. 21.
[104] SERVIZIO EUROPEO PER L'AZIONE ESTERNA, *op. cit.*, p. 52.

COVID-19[105]. Nel 2024, la Commissione europea ha pubblicato il citato Report Niinistö che evidenzia l'incidenza delle minacce ibride (*hybrid attacks*) e suggerisce di incrementare l'uso dell'*intelligence* strategica nei processi decisionali dell'Unione[106]. Il report propone il rafforzamento della SIAC e lo sviluppo, d'intesa con gli Stati membri, di un servizio europeo di cooperazione tra agenzie di *intelligence* pienamente sviluppato (*fully-fledged*), finalizzato alla protezione delle infrastrutture critiche dai rischi di sabotaggio[107]. Niinistö raccomanda, inoltre, di connettere la dimensione interna ed esterna della sicurezza, promuovendo una cultura comune della *counter-intelligence* e valutando l'uso pubblico sussidiario di *intelligence* declassificata per accrescere la prontezza della popolazione di fronte alle minacce asimmetriche. La reazione degli Stati membri è tracciata nella nota della Presidenza del Consiglio al Comitato dei rappresentanti permanenti (Coreper) del 6 dicembre 2024. Il documento accoglie favorevolmente il potenziamento della SIAC, pur ribadendo la riserva di competenza nazionale prevista dall'art. 4, par. 2, del TUE[108]. Tale orientamento è stato recepito dalla Commissione nella strategia *ProtectEU*, la quale individua nella SIAC il punto di accesso unico (*single entry point*) per i flussi informativi degli Stati membri, qualificando la collaborazione come un dovere strategico[109].

Sulla falsariga del Report Niinistö, l'11 novembre 2025 il *Financial Times* ha rivelato l'avvio di un progetto della Commissione europea volto a istituire una nuova unità di *intelligence* incardinata nel proprio Segretariato Generale. L'iniziativa rispondeva all'esigenza di colmare il divario tra le ampie responsabilità politiche della Commissione nella gestione delle minacce ibride e le sue limitate capacità di analisi informativa autonoma, prevedendo il distacco di funzionari dai servizi nazionali[110]. La proposta ha tuttavia sollevato resistenze interistituzionali all'interno del SEAE, dove alti funzionari hanno espresso contrarietà paventando il rischio di una duplicazione funzionale o di uno svuotamento delle prerogative dell'INTCEN[111]. In assenza di commenti ufficiali da parte delle istituzioni dell'Unione[112], le indiscrezioni giornalistiche successive hanno evidenziato una parabola negoziale: il progetto originario di una cellula autonoma in seno alla Commissione è stato prima ridimensionato e poi accantonato, confluendo infine in

[105] Si veda Consiglio dell'Unione europea, *Relazione della Commissione al Parlamento Europeo e al Consiglio sull'esercizio del potere di adottare atti delegati conferito alla Commissione a norma della direttiva 2014/68/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di attrezzature a pressione*, Documento 14291/20, 2020.
[106] S. NIINISTÖ, *op. cit*, p.8.
[107] *Id.*, p. 108.
[108] Comunicazione della Presidenza del Consiglio al Comitato dei rappresentanti permanenti "*Presidency report on Council deliberations related to the report on strengthening Europe's civilian and military preparedness and readiness*", 6 dicembre 2024.
[109] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *ProtectEU*, cit., par. 2.
[110] H. FOY, *EU to set up new intelligence unit under Ursula von der Leyen*, in *Financial Times*, 2025.
[111] H. FOY, *op. cit*.
[112] Come descritta da Cattler: "*Brussels' proposal for an EU-level intelligence 'cell' has created headlines but not answers*". D. CATTLER, *op. cit*.

una proposta di riforma e potenziamento strutturale dell'INTCEN guidata dallo stesso SEAE[113].

Il dibattito sull'evoluzione dell'INTCEN e sulla nascita di un'*intelligence fully-fledged* solleva interrogativi cruciali sulla tenuta dello Stato di diritto. Se da un lato la centralizzazione europea potrebbe standardizzare le procedure di trattamento dei dati sotto l'egida della Carta di Nizza, dall'altro la creazione di un apparato informativo sovranazionale rischia di generare un pericoloso vuoto di controllo giurisdizionale, lasciando irrisolto il cronico conflitto tra l'esigenza di sicurezza e la tutela delle garanzie individuali**.**

5. Conclusioni

Le sfide alla sicurezza nello scenario globale e multilivello contemporaneo presentano oggi caratteri transnazionali complessi, che spaziano dalle emergenze sanitarie alle minacce ibride, sino ai sabotaggi informatici e alle guerre cognitive perpetrati da attori statali e non statali. Questi fenomeni mettono a dura prova non soltanto l'ordinamento dell'Unione europea, ma l'intero sistema di cooperazione internazionale. La proliferazione di trattati globali e di strumenti promossi in seno al Consiglio d'Europa dimostra il tentativo di strutturare risposte giuridiche uniformi superiori ai confini dei singoli Stati. Tuttavia, la spinta all'integrazione e alla condivisione informativa deve costantemente confrontarsi con il principio della sovranità statale e, nel contesto specifico dell'UE, con il principio di attribuzione sancito dall'articolo 4, paragrafo 2, del TUE, il quale riserva la tutela della sicurezza nazionale alla competenza esclusiva di ciascuno Stato membro.

L'analisi condotta evidenzia che il tradizionale *criminal justice approach*, di stampo prevalentemente repressivo, si rivela insufficiente se non coordinato con lo *human rights-based approach*, il quale impone di considerare i diritti fondamentali come parametri intrinseci e inderogabili dell'azione pubblica, inclusa la tutela della sicurezza. Questo bilanciamento subisce però forti tensioni durante le situazioni di emergenza, in cui l'attivazione delle clausole di deroga previste dal diritto internazionale (dall'articolo 4 dell'ICCPR a livello globale, sino all'articolo 15 della CEDU a livello regionale) rischia di giustificare una contrazione sproporzionata delle libertà individuali. La prassi legata alla gestione della pandemia da COVID-19 e dei recenti conflitti geopolitici mostra come il ricorso a regimi eccezionali tenda a consolidare limitazioni dei diritti che dovrebbero rimanere temporanee, indebolendo le garanzie dello Stato di diritto sia nei singoli ordinamenti nazionali sia nello spazio giuridico internazionale.

[113] A. ROUSSI, J. BARIGAZZI, *Von der Leyen softens plan for intelligence cell*, in *Politico*, 9 febbraio 2026. A. IZAMBARD, *Von der Leyen abandons planned EU Commission intelligence unit*, in I*ntelligenceonline.com*, 30 marzo 2026. A. ROUSSI, *EU's intelligence hub eyes bigger role in security overhaul*, in *Politico*, 27 maggio 2026.

Le criticità si amplificano con l'impiego delle nuove tecnologie su scala globale. Il superamento delle barriere territoriali nell'intercettazione dei flussi informatici e la transizione a strategie di sorveglianza di tipo *target-free* o *intelligence-led* – unite all'uso di algoritmi predittivi per neutralizzare minacce asimmetriche e *cognitive weapons* (quali disinformazione e *hate speech*) – determinano il rischio di controlli informativi generalizzati. Sul punto, sebbene il quadro internazionale soffra di una frammentazione normativa dovuta alla natura parziale di strumenti come la Convenzione 108 sulla protezione dei dati, la giurisprudenza delle corti sovranazionali ha cercato di porre argini precisi.

Da un lato, la Corte europea dei diritti dell'uomo, con pronunce fondamentali da *Liberty* a *Big Brother Watch*, ha delineato gli standard minimi per evitare gli abusi legati alla sorveglianza di massa. Dall'altro, la giurisprudenza della Corte di Giustizia nelle cause riunite *La Quadrature du Net* e *Ordre des barreaux* ha fissato un limite chiaro: l'accesso e il trattamento dei dati personali da parte dei servizi di informazione sono subordinati ai criteri di proporzionalità e stretta necessità, vietando forme di sorveglianza di massa indiscriminate in assenza di una minaccia grave, reale, attuale o prevedibile per la sicurezza nazionale.

In questo complesso quadro multilivello si inserisce il dibattito sulla possibile istituzione di un'*intelligence* comune europea. L'attuale architettura della SIAC e dell'INTCEN svolge funzioni puramente analitiche, prive di poteri operativi sul campo e dipendenti dalle informative fornite dagli Stati membri. Le recenti proposte di riforma, dal *Report* Niinistö del 2024 alla strategia *ProtectEU* fino ai progetti di cooperazione strutturata emersi nel 2025, delineano la transizione verso un modello di coordinamento avanzato. Tuttavia, l'eventuale centralizzazione delle funzioni informative a livello europeo non risolve il conflitto tra esigenze di sicurezza e tutela dei diritti fondamentali, ma ne sposta l'applicazione sul piano sovranazionale. Se da un lato l'inquadramento sotto l'egida della Carta di Nizza offre parametri di standardizzazione formale, dall'altro la creazione di un apparato informativo centralizzato rischia di generare un *deficit* di controllo giurisdizionale.

In assenza di un organo giudiziario europeo specializzato o di una commissione parlamentare permanente dotata di effettivi poteri ispettivi sul segreto delle ICUE, l'integrazione rischia di determinare una compressione delle garanzie individuali priva di adeguati contro-poteri democratici, lasciando irrisolto il problema della tutela del cittadino di fronte agli apparati di sicurezza sia all'interno del blocco eurounitario, sia nell'interazione con i sistemi informativi globali.

ABSTRACT: Il contributo analizza il rapporto tra le attività di *intelligence* e la tutela dei diritti fondamentali all'interno di un sistema giuridico multilivello nel contrasto alla criminalità transnazionale. L'indagine esamina, in particolare, i limiti del modello repressivo rispetto a un approccio orientato ai diritti umani. A tal fine lo studio muove

dall'esame delle norme e della giurisprudenza in ambito internazionale ed europeo in materia di legittimità delle possibili deroghe ed eccezioni ai diritti umani per esigenze di sicurezza; successivamente esso illustra le prospettive di riforma dell'architettura informativa eurounitaria alla luce del Report Niinistö e delle recenti iniziative negoziali relative all'INTCEN, evidenziando il rischio di un *deficit* di controllo giurisdizionale sovranazionale a danno delle garanzie individuali.

KEYWORDS: Criminalità transnazionale – Diritti umani – *Intelligence* – INTCEN – Sicurezza.

INTELLIGENCE, HUMAN RIGHTS, AND SECURITY: CRITICAL ISSUES AND PERSPECTIVES WITHIN THE INTERNATIONAL AND EUROPEAN FRAMEWORKS

ABSTRACT: This paper analyzes the relationship between *intelligence* activities and the protection of fundamental rights within a multilevel legal system in the context of countering transnational crime. Specifically, the study examines the limitations of the repressive model in comparison to a human rights-based approach. To this end, the research begins by investigating international and European norms and jurisprudence concerning the legitimacy of potential derogations and exceptions to human rights for security purposes. Subsequently, it illustrates the prospects for reforming the European information architecture in light of the Niinistö Report and recent regulatory initiatives concerning the INTCEN, highlighting the risk of a supranational judicial oversight deficit to the detriment of individual guarantees.

KEYWORDS: Human Rights – INTCEN – *Intelligence* – Security – Transnational Crime.