Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

1/2023

Editore Associazione “Progetto giustizia penale”, c/o Università degli Studi di Milano,
Dipartimento di Scienze Giuridiche "C. Beccaria" - Via Festa del Perdono, 7 - 20122 MILANO - c.f. 97792250157
ANNO 2023 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.
Impaginazione a cura di Chiara Pavesi

Diritto penale contemporaneo – Rivista trimestrale è un periodico on line ad accesso libero e non ha fine di profitto. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione. La rivista, registrata presso il Tribunale di Milano, al n. 554 del 18 novembre 2011, è edita attualmente dall'associazione "Progetto giustizia penale", con sede a Milano, ed è pubblicata con la collaborazione scientifica e il supporto dell'Università Commerciale Luigi Bocconi di Milano, dell'Università degli Studi di Milano, dell'Università di Roma Tre, dell'Università LUISS Guido Carli, dell'Universitat de Barcelona e dell'Università Diego Portales di Santiago del Cile.

La rivista pubblica contributi inediti relativi a temi di interesse per le scienze penalistiche a livello internazionale, in lingua italiana, spagnolo, inglese, francese, tedesca e portoghese. Ogni contributo è corredato da un breve abstract in italiano, spagnolo e inglese.

La rivista è classificata dall'ANVUR come rivista scientifica per l'area 12 (scienze giuridiche), di classe A per i settori scientifici G1 (diritto penale) e G2 (diritto processuale penale). È indicizzata in DoGI e DOAJ.

La rivista può essere citata in forma abbreviata con l'acronimo: *DPC-RT*, corredato dall'indicazione dell'anno di edizione e del fascicolo.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Committee on Publication Ethics).

La rivista si conforma alle norme del Regolamento UE 2016/679 in materia di tutela dei dati personali e di uso dei cookies (clicca qui per dettagli).

Ogni contributo proposto per la pubblicazione è preliminarmente esaminato dalla direzione, che verifica l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

In caso di esito positivo di questa prima valutazione, la direzione invia il contributo in forma anonima a due revisori, individuati secondo criteri di rotazione tra i membri dell'Editorial Advisory Board in relazione alla rispettiva competenza per materia e alle conoscenze linguistiche. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore.

La direzione comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se entrambe le valutazioni sono positive, il contributo è pubblicato. Se una o entrambe le valutazioni raccomandano modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se uno o entrambi i revisori esprimono parere negativo alla pubblicazione.

La direzione si riserva la facoltà di pubblicare, in casi eccezionali, contributi non previamente sottoposti alla procedura di peer review. Di ciò è data notizia nella prima pagina del contributo, con indicazione delle ragioni relative.

I contributi da sottoporre alla Rivista possono essere inviati al seguente indirizzo mail: editor.criminaljusticenetwork@gmail.com. I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali scaricabili qui.

Diritto penale contemporaneo – Rivista trimestrale es una publicación periódica *on line*, de libre acceso y sin ánimo de lucro. Todas las colaboraciones de carácter organizativo y editorial se realizan gratuitamente y no se imponen a los autores costes de maquetación y publicación.
La Revista, registrada en el Tribunal de Milan, en el n. 554 del 18 de noviembre de 2011, se edita actualmente por la asociación "Progetto giustizia penale", con sede en Milán, y se publica con la colaboración científica y el soporte de la *Università Commerciale Luigi Bocconi* di Milano, la *Università degli Studi di Milano,* la *Università di Roma Tre*, la *Università LUISS Guido Carli*, la *Universitat de Barcelona* y la *Universidad Diego Portales de Santiago de Chile.*
La Revista publica contribuciones inéditas, sobre temas de interés para la ciencia penal a nivel internacional, escritas en lengua italiana, española, inglesa, francesa, alemana o portuguesa. Todas las contribuciones van acompañadas de un breve abstract en italiano, español e inglés.
El lector puede leer, compartir, reproducir, distribuir, imprimir, comunicar a terceros, exponer en público, buscar y señalar mediante enlaces de hipervínculo todos los trabajos publicados en "Diritto penale contemporaneo – Rivista trimestrale", con cualquier medio y formato, para cualquier fin lícito y no comercial, dentro de los límites que permite la licencia *Creative Commons - Attribuzione - Non commerciale 3.0 Italia* (CC BY-NC 3.0 IT) y, en particular, debiendo mantenerse la indicación de la fuente, el logo, el formato gráfico original, así como el autor de la contribución.
La Revista se puede citar de forma abreviada cn el acrónimo *DPC-RT*, indicando el año de edición y el fascículo.
La Revista asume el Code of Conduct and Best Practice Guidelines for Journal Editors elaborado por el COPE (*Comitte on Publication Ethics*).
La Revista cumple lo dispuesto en el Reglamento UE 2016/679 en materia de protección de datos personales (clica aquí para los detalles sobre protectión de la privacy y uso de cookies).
Todas las contribuciones cuya publicación se propone serán examinadas previamente por la Dirección, que verificará la correspondencia con los temas tratados en la Revista y el respeto de los requisitos mínimos para su publicación.
En el caso de que se supere con éxito aquella primera valoración, la Dirección enviará la contribución de forma anónima a dos evaluadores, escogidos entre los miembros del *Editorial Advisory Board*, siguiendo criterios de rotación, de competencia por razón de la materia y atendiendo también al idioma del texto. Los evaluadores recibirán un formulario, que deberán devolver a la Dirección en el plazo indicado. En el caso de que la devolución del formulario se retrasara o no llegara a producirse, la Dirección se reserva la facultad de escoger un nuevo evaluador.
La Dirección comunicará el resultado de la evaluación al autor, garantizando el anonimato de los evaluadores. Si ambas evaluaciones son positivas, la contribución se publicará. Si alguna de las evaluaciones recomienda modificaciones, la contribución se publicará después de que su autor la haya revisado sobre la base de los comentarios recibidos y de que la Dirección haya verificado que tales comentarios han sido atendidos. La contribución no se publicará cuando uno o ambos evaluadores se pronuncien negativamente sobre su publicación.
La Dirección se reserva la facultad de publicar, en casos excepcionales, contribuciones que no hayan sido previamente sometidas a *peer review*. Se informará de ello en la primera página de la contribución, indicando las razones.

Si deseas proponer una publicación en nuestra revista, envía un mail a la dirección editor.criminaljusticenetwork@gmail.com. Las contribuciones que la Dirección considere de potencial interés para la Revista se someterán al proceso de *peer review* descrito arriba. Las contribuciones que se propongan a la Revista para su publicación deberán respetar los criterios de redacción (se pueden descargar aquí).

Diritto penale contemporaneo – Rivista trimestrale is an on-line, open-access, non-profit legal journal. All of the organisational and publishing partnerships are provided free of charge with no author processing fees. The journal, registered with the Court of Milan (n° 554 - 18/11/2011), is currently produced by the association "Progetto giustizia penale", based in Milan and is published with the support of Bocconi University of Milan, the University of Milan, Roma Tre University, the University LUISS Guido Carli, the University of Barcelona and Diego Portales University of Santiago, Chile.

The journal welcomes unpublished papers on topics of interest to the international community of criminal scholars and practitioners in the following languages; Italian, Spanish, English, French, German and Portuguese. Each paper is accompanied by a short abstract in Italian, Spanish and English.

For citation purposes the journal's abbreviated reference format may be used: *DPC-RT,* indicating year of publication and issue.

The journal strictly adheres to the Code of Conduct and Best Practice Guidelines for Journal Editors drawn up by COPE (Committee on Publication Ethics).

The journal complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) (click here for details on protection of privacy and use of cookies).

All articles submitted for publication are first assessed by the Editorial Board to verify pertinence to topics addressed by the journal and to ensure that the publication's minimum standards and format requirements are met.

Should the paper in question be deemed suitable, the Editorial Board, maintaining the anonymity of the author, will send the submission to two reviewers selected in rotation from the Editorial Advisory Board, based on their areas of expertise and linguistic competence. The reviewers are provided with a feedback form to compile and submit back to the editorial board within an established timeframe. If the timeline is not heeded to or if no feedback is submitted, the editorial board reserves the right to choose a new reviewer.

The Editorial Board, whilst guaranteeing the anonymity of the reviewers, will inform the author of the decision on publication. If both evaluations are positive, the paper is published. If one or both of the evaluations recommends changes the paper will be published subsequent to revision by the author based on the comments received and verification by the editorial board. The paper will not be published should one or both of the reviewers provide negative feedback.

In exceptional cases the Editorial Board reserves the right to publish papers that have not undergone the peer review process. This will be noted on the first page of the paper and an explanation provided.

If you wish to submit a paper to our publication please email us at editor.criminaljusticenetwork@gmail.com. All papers considered of interest by the editorial board will be subject to peer review process detailed above. All papers submitted for publication must abide by the editorial guidelines (download here).

Contents

Contents

Intelligenza artificiale e diritto penale
Inteligencia artificial y derecho penal
Artificial Intelligence and Criminal Law

Criminal compliance e nuove tecnologie *

Criminal compliance *y nuevas tecnologías*

Criminal Compliance and New Technologies

Luca D'Agostino
Dottore di ricerca in diritto penale
ldagostino@luiss.it

Responsabilità da reato degli enti, Intelligenza artificiale

Responsabilidad penal personas jurídicas, Inteligencia artificial

Corporate Criminal Liability, Artificial Intelligence

Abstracts

Il contributo ha per oggetto all'analisi di una possibile automazione della compliance penale per la prevenzione di illeciti all'interno delle imprese. L'indagine mira ad esaminare i possibili benefici e i rischi derivanti dall'utilizzo di *smart technologies* (es. *big data*, intelligenza artificiale, *blockchain*) in chiave preventiva, attraverso l'integrazione di tali strumenti innovativi nei modelli organizzativi e gestionali adottati dagli enti *ex* art. 6 D. Lgs. 231/2001. Partendo dall'analisi di strumenti già esistenti (quali quelli per la *detection* di minacce, vulnerabilità e anomalie), lo studio valuta la specifica applicabilità dei nuovi ritrovati tecnologici nei processi di controllo 231. L'obiettivo è dunque quello di analizzare – *de iure condito* e sulla base dell'attuale stato della tecnica – le possibili applicazioni tecnologiche per prevenire la commissione di *corporate crimes*.

El artículo analiza la posible automatización del compliance penal para la prevención de actuaciones ilícitas en el seno de las empresas. La investigación tiene como objetivo examinar los posibles beneficios y riesgos derivados del uso de tecnologías inteligentes (por ejemplo, big data, inteligencia artificial, blockchain) de forma preventiva, a través de la integración de estas herramientas innovadoras en los modelos organizativos y de gestión adoptados por las personas jurídicas en virtud del Art. 6 del Decreto 231/2001. Partiendo del análisis de las herramientas existentes (aquellas para la detección de amenazas, vulnerabilidades y anomalías), el estudio evalúa la aplicabilidad de los nuevos medios tecnológicos en los mecanismos de prevención y control corporativos. También se pretende analizar, las posibles aplicaciones informáticas para prevenir la comisión de delitos corporativos.

The essay examines the potential automation of criminal compliance to prevent illegal activities within companies. The investigation aims to explore the potential benefits and risks associated with the utilization of smart technologies (e.g., big data, artificial intelligence, blockchain) in a proactive manner. This involves integrating these innovative tools into the organizational and management models adopted by entities under Article 6 of the Italian Legislative Decree 231/2001. By analyzing existing tools used for threat detection, vulnerability assessment, and anomaly detection, the study assesses the feasibility of implementing new technological means in corporate compliance. Furthermore, the objective is to analyze and reflect on the current state of the art regarding IT applications for preventing corporate crimes.

* Il presente contributo nasce dalla rielaborazione dei risultati della ricerca "Criminal Compliance and New Technologies", nell'ambito del progetto "Go for IT" finanziato dal Ministero dell'Istruzione e attuato dalla Fondazione CRUI.

Sumario

1. *Digital Criminal Compliance*. Opportunità e rischi dell'automazione nei processi di controllo.

Alcuni studi recenti hanno elaborato la nozione di "Digital Criminal Compliance"[1] per indicare la tendenza alla digitalizzazione della tradizionale *compliance* aziendale nella prevenzione dei reati[2]. Un concetto che, secondo alcuni, potrebbe diventare centrale nel campo del diritto penale economico. Tale disciplina – che per brevità indicheremo con l'acronimo DCC – si basa essenzialmente sull'analisi di dati ottenuti attraverso strumenti di rilevazione che, grazie all'intelligenza artificiale, sono aggregati e resi fruibili per determinate attività di monitoraggio e controllo[3].

Nonostante si parli icasticamente di una "automazione" della *compliance* penale, nella realtà si tratta di applicazioni tecnologiche di supporto a funzioni aziendali gestite dall'uomo, non sostituibili con il lavoro del *software*. Pertanto, appare preferibile definire la DCC come un *empowerment organizzativo*: la tecnologia amplifica il potenziale del sistema di gestione e permette di massimizzare i risultati delle funzioni di controllo e *internal auditing*.

La DCC si rivela certamente più efficace ed efficiente rispetto alla *compliance* soltanto "analogica", che spesso presenta debolezze riconducibili al fattore umano. Di regola i modelli organizzativi mirano a prevenire la commissione di reati attraverso la diffusione della "cultura della legalità" e la segmentazione dei processi decisionali e di controllo[4]. Questo secondo elemento porta all'irrigidimento dell'assetto organizzativo, e si pone spesso in contrasto con le dinamiche del mercato e dell'impresa[5].

Le *smart technologies* consentono di elaborare grandi quantità di dati in modo coerente, più veloce e preciso degli esseri umani; ciò porta a un significativo incremento dell'efficienza e conduce verso una progressiva semplificazione delle procedure. Inoltre, grazie all'analisi in tempo reale dei flussi di informazioni, si incentiva la leva preventiva permettendo all'ente di intervenire non appena si abbia notizia di indici di sospetto o anomalia[6]. Ciò segna una svolta significativa nella *governance* del rischio, poiché consente all'ente di reagire in un tempo in cui il reato non è ancora stato commesso.

Laddove l'illecito non possa essere prevenuto neppure da sistemi evoluti di monitoraggio attivo, il vantaggio della DCC consiste nella registrazione degli "eventi informatici" occorsi[7] che permette di svolgere una accurata analisi *ex post* per individuare i responsabili o ricostruire le modalità di commissione del reato.

Occorre tuttavia essere consapevoli anche dei rischi della DCC, e del possibile contrasto con alcune disposizioni di legge sul trattamento dei dati personali e sui diritti del lavoratore. Invero, l'utilizzo di sistemi "intelligenti" a supporto alla *compliance* penale può dar luogo – in via diretta o anche solo incidentalmente – a forme di monitoraggio del personale addetto ai

[1] Gullo (2022), p.1289 ss.
[2] Burchard (2021), p. 741 ss.
[3] L'intelligenza artificiale è qui da intendersi in senso ampio, v. *infra* § 3.2.
[4] Severino (2020), p. 531
[5] Burchard (2021), p. 746.
[6] Si segnerebbe così il passaggio da una *compliance* penale statica e "reattiva" verso un modello più dinamico e fortemente preventivo.
[7] Si consideri al riguardo il caso esemplificato al § 3.1. e l'utilizzo di SIEM per l'analisi dei dati di traffico (§ 4.2.).

processi a rischio[8]. Si pensi al controllo del traffico di mail attraverso algoritmi di *Natural Language Processing* (NLP), alla registrazione di chiamate telefoniche o telematiche, al tracciamento dei file di navigazione, o alla rilevazione delle coordinate GPS. Si tratta, come evidente, di applicazioni che presentano rischi significativi per gli individui, in grado di ledere diritti costituzionalmente tutelati.

A ben vedere, la *compliance* penale digitale[9] si differenzia da quella "analogica" non soltanto per elementi quantitativi (numero di dati raccolti e trattati, tempi di risposta e reazione etc.), ma soprattutto per elementi qualitativi (tipologia di dati analizzati, funzioni e personale coinvolto). Sarebbe dunque opportuno procedere a una valutazione preventiva di conformità normativa per evitare che, da incentivo alla legalità aziendale, la tecnologia divenga il volano di prassi illecite[10] o discriminatorie[11]. Inoltre, la DCC non dovrebbe trasmodare in una modalità "post-panottica" di esercizio del potere in funzione di *Big Data* ottenuti monitorando in modo sempre più penetrante i comportamenti dei dipendenti.

Infine, si prospettano alcuni rischi "sociali" correlati alla *compliance* digitale. Essendo questa basata sul controllo preventivo, ne potrebbe derivare una sistematica sfiducia nei confronti del personale aziendale. Dipendenti e lavoratori finiscono per essere considerati un rischio da monitorare, anziché persone dotate di indipendenza e libertà di azione[12].

1.1. RegTech *e automazione della compliance penale. Lo stato dell'arte.*

La trasformazione digitale rappresenta una delle principali sfide per la *corporate compliance*. Se si considera la *compliance* come quel metodo per l'applicazione delle regole nei processi interni, appare chiaro come l'innovazione digitale sia destinata a mutare profondamente l'assetto organizzativo e dei controlli.

La dottrina nordamericana si interroga già da diversi anni sulle sorti della *compliance* penale dell'era del progressismo tecnologico, mettendo in evidenza il delicato equilibrio tra opportunità e rischi dell'automazione dei controlli societari[13]. Si parla in particolare di *RegTech*[14] per definire quelle tecnologie che supportano le imprese nel rispetto dei requisiti normativi, in modo da assicurare un alto grado di conformità alle regole. Secondo alcuni autori[15] il *RegTech*, non è un semplice strumento di potenziamento della *compliance*, ma un vero e proprio cambiamento di paradigma per il business del ventunesimo secolo[16]; secondo altri[17] esso rappresenta la base fondamentale e la prossima evoluzione in molti settori, tra cui in particolare quello dei servizi finanziari.

Il *RegTech* migliora la *performance* dei sistemi di gestione aziendale, automatizzando parte dei compiti attribuiti alle funzioni di *compliance* e riducendo i rischi operativi associati all'agire umano. Inoltre, permette al personale incaricato di agire in modo informato basandosi sui dati raccolti e processati dagli algoritmi[18]. Diverse applicazioni tecnologiche – quali il *machine*

[8] Sul tema, in generale, Burchard (2019), p. 1909
[9] Di recente sull'argomento v. Morgante- Fiorinelli (2022) p. 1; Nisco (2022); Mongillo (2022); Selvaggi (2019), p. 217
[10] Per trattamento illecito di dati (art. 167 D. Lgs. 196/2003) o per violazione delle disposizioni in materia di controlli a distanza dei lavoratori (art. 171 D. Lgs. 196/2003 in relazione all'art. 8 L. 300/70).
[11] Si pensi alla problematica dei *bias* algoritmici dovuti alle generalizzazioni statistiche. Tra gli esempi più noti si ricorda l'esperienza statunitense degli algoritmi predittivi per la commisurazione della pena, laddove tra le variabili rilevanti ai fini della determinazione del livello di rischio, si tiene spesso conto di fattori demografici, socioeconomici, familiari, che contribuiscono a caratterizzare come individui più pericolosi quelli appartenenti a determinate minoranze o classi sociali. L'output dell'algoritmo risulta così "contaminato" dal trend storico al trattamento deteriore e al pregiudizio nei confronti di alcune figure di criminali. Sia consentito rinviare, per richiami alla dottrina nordamericana, a D'Agostino, (2019), p. 354 ss.; Franssen -Berrendorf (2021), p.199. Il tema dei *bias* algoritmici interessa anche l'impiego per finalità di prevenzione dei reati. In dottrina si riporta l'esempio della multinazionale che intende utilizzare i dati del sistema giudiziario statunitense per individuare i dipendenti con maggiore possibilità di delinquere, che renderebbero verosimilmente più alto l'indice di pericolosità per gli individui appartenenti a talune classi sociali o minoranze razziali. Cfr. Burchard (2021), p. 746
[12] Zuboff (2019), p. 2
[13] Laufer (2017), p. 71
[14] Packin (2018), p. 193 ss.
[15] Arner *et al.* (2017), p. 373.
[16] Secondo la definizione comune, il Regtech è l'uso delle nuove tecnologie per assicurare il rispetto dei requisiti normativi in modo più efficace ed efficiente.
[17] Mohamed- Yildirim (2021), p. 153
[18] Gli strumenti tecnologici riducono la probabilità di errori umani e promuovono il miglioramento continuo dei processi organizzativi e gestionali. Il supporto alla *compliance* è caratterizzato da complesse analisi documentali e correlazioni tra dati, che grazie all'uso di strumenti e tecnologie intelligenti sono rese più performanti, facendo venir meno le inefficienze collegate al fattore umano.

learning, la crittografia, la *big data analytics* – rendono disponibili informazioni pertinenti e specifiche sulle attività della società, che in nessun altro modo sarebbe possibile ottenere[19].

É noto come l'Intelligenza Artificiale (IA)[20] abbia oggi molteplici applicazioni nella prevenzione e nel perseguimento dei reati e, in genere, nel sistema di giustizia penale[21] e nel *law enforcement*[22]. Alcune di queste, già radicate nella giudiziaria statunitense[23], pongono questioni sul fronte criminologico[24], etico e legale[25].

Di recente si è anche discusso dell'impiego dell'IA per la prevenzione dei reati, mettendo in evidenza alcune possibili criticità sul piano dei principi generali della responsabilità dell'ente[26]. La dottrina ha iniziato a interrogarsi sulla responsabilità per c.d. *algorithmic misconduct,* nei casi in cui una determinata violazione o un omesso controllo siano causati da una "scelta" del *software*. In questi casi risulterà complesso stabilire a quali condizioni l'ente debba rispondere dell'illecito, poiché si deve distinguere in base al modello di responsabilità oggettiva (*strict liability*) o di responsabilità vicaria (basato sul principio del *respondeat superior*)[27]. Mentre il primo non richiede la prova di alcun elemento soggettivo, essendo sufficiente il fatto nella sua oggettività, il secondo attribuisce rilevanza allo status psicologico del personale aziendale.

Questo secondo modello – sul quale è imperniato il sistema statunitense di responsabilità degli enti – pone alcune criticità nel caso di *algorithmic misconduct,* che gli studiosi hanno tentato di risolvere senza travolgere lo schema della responsabilità vicaria. L'ente risponderà dell'illecito a condizione che il fatto sia stato commesso attraverso informazioni "conosciute" dall'algoritmo, e quindi dalla società, per essere state prodotte o elaborate nelle attività aziendali devolute all'algoritmo stesso. Inoltre, le informazioni processate e l'output del *software* devono portare un qualche vantaggio all'ente[28].

Quando la violazione è causata dall'algoritmo, l'indagine sull'elemento psicologico diviene complessa, non essendo possibile far riferimento all'*animus* del personale aziendale incaricato di certe funzioni (ad esempio il programmatore o il responsabile IT).

Vi sono poi quei modelli di responsabilità dell'ente nei quali si valorizza la colpa di organizzazione, come nel sistema italiano disciplinato dal D. Lgs. 231/2001[29]. Secondo questo schema di responsabilità, in caso di violazione ascrivibile al *software*, l'ente sarà responsabile soltanto se la commissione dell'illecito dipende da una carenza organizzativa. Si è parlato a tal proposito dell'intelligenza artificiale come "arma a doppio taglio"[30] in grado potenziare le attività di *compliance* e, al tempo stesso, di esporre al rischio di deficit organizzativi. Sebbene, in linea di massima, l'uso della tecnologia renda i sistemi di gestione più affidabili, l'ente dovrà definire procedure e controlli specifici sul funzionamento degli strumenti informatici e sul trattamento delle eventuali anomalie[31].

La transizione digitale ha aumentato vertiginosamente la mole di dati a disposizione degli enti, che opportunamente elaborati, divengono informazioni preziose per il *decision making* aziendale. Per questo motivo l'intelligenza artificiale diviene uno strumento via via sempre più efficace per la prevenzione dei reati. Si va verso il tramonto dei processi tradizionali *human-based*, sostituiti dall'automazione nelle attività di *risk analysis*.

I *software* di IA permettono di individuare le aree critiche, attribuire un punteggio di

[19] Van Liebergen *et al.* (2016), p. 1
[20] *Amplius,* § 2.2.
[21] Ferguson (2015), p. 327; Osvald *et al.* (2018), p. 227; Gialuz (2019)
[22] United Nations Interregional Crime and Justice Research Institute's (UNICRI), *Artificial Intelligence and Robotics for law enforcement*, in unicri.it
[23] Si citano al riguardo le parole di Justice Roberts, giudice della Corte Suprema USA, che in una intervista del 2018 alla domanda se potesse immaginare un giorno in cui le macchine intelligenti saranno utilizzate per supportare il processo decisionale del giudice rispose: «*Questo giorno è già arrivato e sta mettendo a dura prova il modo in cui la magistratura fa le cose*». Cfr. Liptak (2017), citato da Burchard (2019), p. 1909.
[24] King *et al.* (2020), p. 89
[25] Vermeulen *et al.* (2021), p. 7. Gli autori affermano che l'uso legittimo dell'IA e dei *big data* nella giustizia penale dipende da una serie di fattori, tra cui la trasparenza algoritmica, l'affidabilità, la non discriminazione, la protezione dei dati, l'accesso alla giustizia, l'esistenza di rimedi effettivi.
[26] Sabia (2020), p. 179. Secondo l'autrice l'impiego dell'IA per migliorare la *compliance* aziendale e prevenire il rischio di reato è una tematica emergente, un campo di indagine ancora largamente inesplorato.
[27] Per una analisi accurata si veda Mazzacuva (2021), p. 143
[28] Diamantis (2020), p. 893 ss.
[29] Paliero (2018), p. 175 ss.
[30] Mazzacuva (2021), p. 150.
[31] Non si può infatti ignorare l'incidenza di tali strumenti nella organizzazione del lavoro e nell'assegnazione di ruoli e responsabilità all'interno dell'azienda. La dirigenza deve avere una conoscenza piena della tecnologia per poter strutturare al meglio i processi operativi; parimenti gli organismi di vigilanza dovranno comprenderne a fondo le logiche per esperire gli opportuni controlli.

rischio[32] e, grazie all'apprendimento automatico, di fare previsioni su eventi futuri. Gli enti possono così migliorare nel tempo le loro strategie di *compliance*, utilizzando la tecnologia, come detto, per l'*empowerment* organizzativo.

Altro tema discusso è il rapporto tra *digital compliance* e responsabilità da reato. Ci si è chiesti, nell'ipotesi in cui la società si affidi all'IA, se sia responsabile laddove il reato commesso rappresenti la concretizzazione di un rischio non rilevato dal *software*[33]. Facendo applicazione dei principi desumibili dall'art. 6 D. Lgs. 231/2001, l'ente andrà esente da responsabilità se, avendo adottato un modello organizzativo idoneo[34], non vi sia stata omessa o insufficiente vigilanza da parte dell'OdV.

Il vero *core* della questione rimane dunque il sindacato sull'idoneità del modello[35], attraverso il quale si esprime un giudizio sulla colpevolezza dell'ente[36]. Si dovrà compiere una valutazione relativa al caso concreto, per stabilire se l'automazione di determinate attività fosse coerente rispetto allo scopo e sia stata inserita in un processo tale da permettere l'acquisizione di informazioni e l'attivazione dei controlli da parte dell'organismo di vigilanza. L'aver acriticamente assegnato al *software* determinate funzioni – in assenza, ad esempio, di adeguata formazione del personale o di procedure specifiche di analisi dei dati – è indice sintomatico della colpa di organizzazione.

Guardando invece alle prospettive *de iure condendo* l'IA potrebbe offrire al legislatore una soluzione all'annosa questione del sindacato giudiziale, attraverso la previsione di una presunzione (relativa) di idoneità dei modelli che, in determinati ambiti, siano conformi alle *best practices* di settore[37].

Le potenzialità dei *Big Data* sono tanto maggiori quanto più grande è il flusso di informazioni[38]; grazie alle capacità computazionali e predittive degli algoritmi anche le società di grandi dimensioni possono analizzare i dati in modo accurato.

Numerosi sono tuttavia i profili critici. Secondo alcuni autori la bontà delle decisioni prese dal *software* dipende dalla quantità di dati processati in *input*[39]. Tuttavia, l'incremento di questi ultimi rende sempre più impegnativa l'attività di analisi da parte del personale umano. Spesso poi gli algoritmi di IA risultano *impenetrabili*[40], non essendo possibile determinare quanto peso abbia ogni singola variabile nella decisione finale[41]. Il problema è dunque quello della opacità del programma, che può produrre il c.d. effetto *black box*[42]. Si distinguono diversi tipi di opacità del *software*: (i) è intenzionale quando risponde a una scelta del programmatore (si pensi al *trade secret* per proteggere gli interessi economici dell'azienda); (ii) in atri casi potrebbe essere dovuta alla mancanza di competenze tecniche da parte degli utilizzatori; (iii) vi è poi l'opacità necessaria, legata alla complessità dei *software* di AI e al *deep learning*[43]. Mentre le prime due possono essere superate – scegliendo ad es. *software* non proprietari o acquisendo le opportune competenze tecniche – l'ultima è allo stato una costante ineliminabile.

[32] Si veda in argomento il paper di Deloitte, *AI and Risk Management*, *Center for regulatory strategy*, in www2.deloitte.com.

[33] Sabia (2020), p. 186 sostiene che, indipendentemente dal modello di riferimento, sia complesso attribuire la responsabilità in base alle norme esistenti. I criteri di ascrizione della responsabilità penale dell'ente potrebbero rivelarsi inadeguati di fronte alle sfide poste dalle nuove tecnologie.

[34] Sulla valutazione relativa all'idoneità del modello v. Morgante-Fiorinelli (2022), p. 13

[35] *Infra*, § 1.2.

[36] L'errore dell'algoritmo non può determinare *ex se* la responsabilità penale dell'ente, dovendosi all'opposto dimostrare l'assenza di procedure interne di valutazione e riesame. Se la società ha adottato un *compliance program* ben strutturato, prevedendo gli opportuni controlli, non dovrebbe sussistere alcuna colpa di organizzazione.

[37] La codificazione delle regole cautelari e il sindacato giudiziale sull'idoneità dei modelli sono temi assai discussi in dottrina. È autorevolmente sostenuta la tesi della "validazione" del modello attraverso la positivizzazione di protocolli cautelari, imperniati sulle *best practices* di settore. In particolare, Piergallini (2019), p. 536 ritiene che i modelli conformi allo standard del settore dovrebbero essere assistiti da una presunzione, *iuris tantum*, di idoneità preventiva, superabile dal giudice solo attraverso l'assolvimento di un onere motivazionale rafforzato. Nello stesso senso v. anche Piergallini (2015), p. 266.
A nostro modo di vedere, nella positivizzazione delle cautele, ampio spazio andrebbe riconosciuto all'impiego di strumenti tecnologici a supporto della *compliance*. Così, ad esempio, l'adozione di alcuni programmi (per la *due diligence* di terze parti o per monitorare il traffico di mail), in linea con gli standard di settore, potrebbe ragionevolmente fondare una presunzione relativa di idoneità del modello nel prevenire i reati di corruzione.

[38] Severino (2020), p. 536.

[39] Dombalagian (2016)

[40] Mozzarelli (2022), p. 259 ss.

[41] Da un punto di vista tecnico, comprendere le ragioni di una previsione basata su un numero limitato di variabili (come avviene di solito nella statistica tradizionale) è fattibile. Al contrario, le previsioni basate su Big Data e reti neurali non sono facilmente spiegabili *a posteriori*, essendo estremamente difficile ottenere informazioni sul peso di un singolo nodo nel determinare la decisione. *Amplius*, § 2.2.

[42] Sabia (2020), p. 185.

[43] Niklas (2020), p. 527.

Tra i punti deboli dei sistemi automatizzati vi sono anche la c.d. *standardizzazione dei controlli* e i malfunzionamenti derivanti da errori di programmazione o da inadeguata formazione. Il personale addetto ai sistemi non dovrà accomodarsi sugli *output* del programma, dovendo al contrario vagliare in modo critico e costruttivo la determinazione dell'algoritmo. In sostanza, l'automazione della *compliance* deve rappresentare l'occasione per dismettere le attività umane di supervisione e controllo[44].

Per superare tali criticità, una parte della dottrina ha plasmato la nozione di "controllo umano significativo"[45] per descrivere un approccio all'IA caratterizzato dal costante monitoraggio dell'uomo sui risultati della decisione algoritmica.

Altri autori ritengono necessario un intervento dei legislatori nazionali, o anche semplicemente la creazione di regole tecniche e standard di settore (es. norme ISO), per incentivare le aziende a dotarsi di strumenti digitali a supporto della *compliance*[46].

Vi è anche chi propone un approccio basato sulla *forward compliance*[47] secondo cui, per limitare i predetti rischi, l'ente dovrebbe adottare linee guida e istruzioni operative specifiche ed accurate, senza necessariamente attendere l'emanazione di una regolazione di settore. La tesi muove dal condivisibile assunto per cui qualsiasi nuova tecnologia presenta margini di rischio, e necessita l'adozione di particolari cautele. Affinché il percorso di automazione della *compliance* sia sicuro e sostenibile, gli enti dovranno interiorizzare le *smart technologies* nei processi esistenti scegliendo la soluzione che meglio riesca a conciliare le contrapposte esigenze.

Nonostante l'opinione prevalente sia favorevole al *RegTech*, non mancano voci di segno contrario. Vi è chi sostiene che la tecnologia possa ostacolare l'impegno umano nelle attività di *risk assessment* e nei processi decisionali dell'ente[48]. Si parla di *technology judgement rule* per indicare, in senso negativo, quelle scelte di *governance* basate unicamente sull'*output* algoritmico[49].

1.2. *Strumenti digitali a supporto della* compliance *231. Alcuni esempi derivanti dalle* best pratices *in materia di anticorruzione e antiriciclaggio.*

L'utilizzo di strumenti tecnologici a supporto della *compliance* aziendale si inserisce in un quadro di regole in cui è preponderante il ruolo dell'autodisciplina[50]. In molti settori il legislatore si affida al c.d. approccio basato sul rischio lasciando ai soggetti privati l'onere di individuare, in base al contesto di riferimento, le modalità concrete per l'attuazione degli obblighi di legge[51].

Pur non essendovi espresse disposizioni circa la doverosità di mettere in atto misure tecnologiche per mitigare il rischio di reati, può ritenersi che un tale adempimento rientri nel più ampio concetto di "best practice di settore" per assicurare l'adeguatezza in concreto dei sistemi di controllo aziendali. Da questa prospettiva l'automazione della *compliance* rappresenta una grande opportunità per gli enti, che potranno dimostrare di aver attuato controlli e procedure di mitigazione del rischio affidandosi alle più avanzate tecniche di monitoraggio e *intelligen-*

[44] Alcuni studiosi temono che gli uffici di compliance possano abbandonarsi a prassi lassiste, rimettendo tutto alle previsioni/decisioni algoritmiche. Cfr. Dombalagian (2016), p. 87.
[45] Ubertis (2020), p. 75 ss.; Sorbello (2019), p. 374 ss.
[46] Niklas (2020), p. 539.
[47] Armour (2018)
[48] Bamberger (2009), p. 669
[49] La dottrina da ultimo richiamata sostiene che i sistemi di *compliance* digitale siano sviluppati sulla base dell'interpretazione della legge fornita dal programmatore. I processi che portano alla creazione di tali sistemi nascono dalla interazione di diversi gruppi di professionisti che, spesso, comunicano tra loro in modo imperfetto.
[50] Nel sistema di responsabilità da reato degli enti si pensi ai codici elaborati dalle associazioni di categoria (le "Linee Guida") in base ai quali poter costruire, ai sensi dell'art. 6, comma 3, d.lgs. 231/2001, i modelli organizzativi e gestionali.
[51] L'approccio basato sul rischio assicura una certa flessibilità, proporzionalità e adeguatezza in concreto; in questo modo ciascun operatore dovrà valutare il rischio e adottare misure che siano adeguate e proporzionate al rischio stesso Nell'ordinamento vigente possono citarsi esempi afferenti a diversi ambiti: l'art. 6 D. Lgs. 231 /2001 indica genericamente le esigenze da considerare nella costruzione dei modelli organizzativi, senza prescrivere specifiche cautele o misure per le attività a rischio; in materia di antiriciclaggio l'art. 16, comma 1, D. Lgs. 231/2007 dispone che i soggetti obbligati debbano «*adottare i presidi e attuare i controlli e le procedure, adeguati alla propria natura e dimensione, necessari a mitigare e gestire i rischi di riciclaggio e di finanziamento del terrorismo*»; in materia di trattamento dei dati personali l'art. 12, par. 1, GDPR prevede che «*Il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*».

ce sui dati[52]. Affinché la transizione delle imprese verso il digitale sia sicura e sostenibile, è auspicabile che anche i modelli organizzativi e gestionali 231 si conformino alla progressiva informatizzazione dei processi. Il sistema di controlli dovrebbe evolvere di pari passo rispetto alle modalità di lavoro e di gestione dell'azienda[53], non potendo restare legato a dinamiche tradizionali.

Nel presente studio saranno considerati due principali benefici della *compliance* penale digitale: (i) la riduzione dei tempi di emersione degli indizi di reato e di attivazione degli opportuni controlli; (ii) il potenziamento dei canali informativi e degli elementi di valutazione a disposizione del personale incaricato di svolgere determinate funzioni. Rispetto al primo saranno considerati gli strumenti di *real time analytics*, in grado di generare *alert* automatici in caso di anomalie comportamentali o di contenuti sospetti. Il secondo vantaggio riguarda l'agire informato della società, che potrà disporre di efficienti strumenti per la *due diligence* nei confronti di terze parti, tutte le volte in cui un determinato affare possa essere considerato a rischio.

Come noto, l'esclusione della responsabilità dell'ente opera laddove l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi, secondo le cadenze prospettate agli artt. 6-7 del D. Lgs. 231/2001 a seconda che il *predicate crime* sia commesso da apicali o sottoposti. L'impiego di strumenti tecnologici rappresenta un fattore da considerare nel sindacato sull'idoneità del modello[54], poiché rafforza la tenuta complessiva del sistema di *compliance.* Il supporto offerto da tali strumenti si andrà progressivamente affermando a livello internazionale come *best practice*[55] in vari settori, fungendo da criterio guida per una efficace gestione del rischio[56]. Le buone pratiche aziendali, frutto dell'esperienza maturata negli anni, sono molto diffuse nella realtà socio-economica e, talvolta, sono cristallizzate in standard internazionali.

Si pensi, ad esempio, alla norma ISO 37001 sui sistemi di prevenzione della corruzione[57], che impone di pianificare processi di *due diligence* sui soci in affari per valutare il rischio di corruzione[58], ricorrendo a indagini sulle fonti disponibili per esaminare il coinvolgimento in atti di corruzione, condotte fraudolente, altri illeciti analoghi. I programmi di *decision intelligence* per le analisi su fonti aperte rappresentano, in questa direzione, una valida modalità di verifica delle informazioni sui fornitori.

In altri casi, l'utilizzo della tecnologia a supporto della *compliance* trova fondamento in discipline settoriali o nelle disposizioni delle autorità di vigilanza. Un esempio è dato dalle Linee Guida Confindustria che, nella parte dedicata alle modalità operative di gestione dei rischi, sottolineano la necessità di compiere *due diligence* sui fornitori qualora sia rilevato un "indicatore di sospetto"[59]. Nel settore della prevenzione del riciclaggio si possono richiamare le disposizioni della Banca D'Italia in materia di adeguata verifica del 30 luglio 2019 laddove prevedono che le informazioni per la determinazione del rischio *«possono essere tratte da ogni fonte e documento utile, tra cui fonti giornalistiche autorevoli»* (Sez. II, n. 2, lett. b), con particolare riguardo alle informazioni *«provenienti da organismi e autorità pubbliche, anche di altri paesi comunitari acquisibili anche attraverso siti web»* (Sez. V, n. 2, *sub* iii). Inoltre, gli intermediari sono tenuti a verificare la compatibilità dei dati e delle informazioni fornite dal cliente con le informazioni da essi acquisite autonomamente (Sez. VI)[60], anche per valutare la reputazione

[52] In argomento v. Gullo (2022), p. 1301 secondo cui, sul piano della valutazione giudiziale del modello, l'impiego delle nuove tecnologie potrebbe integrare quelle *best practice* condivise in grado di legittimare una presunzione relativa vincibile dal giudice con motivazione rafforzata.
[53] Per un studio sulle strategie di prevenzione e risposta ai rischi per la sicurezza informatica v. Baskerville *et al.* (2014), p. 138
[54] Di quest'avviso Gullo (2022), p. 1301; Birritteri (2019), p. 294.
[55] Sul tema delle *best pratice* v. Mongillo (2011), p. 75.
[56] Con riferimento alla colpa in organizzazione, la dottrina ha da tempo denunciato la mancanza di regole precauzionali ritenute efficaci secondo il parametro della *societas eiusdem professionis.* Pertanto, nell'effettuazione del giudizio di prevedibilità ed evitabilità del reato da prevenire ci si affida all'attività di autoregolazione societaria. In questo modo l'ente, che è il destinatario della regola cautelare, diviene anche il suo artefice.
[57] UNI ISO 37001:2016. La norma specifica i requisiti e fornisce una guida per stabilire, mettere in atto, mantenere, aggiornare e migliorare un sistema di gestione per la prevenzione della corruzione.
[58] Si vedano i paragrafi 8.1, 8.2 e l'appendice A.10.1 e seguenti.
[59] Linee Guida Confindustria per la costruzione dei modelli di organizzazione gestione e controllo, parte II, par. 4, in www.confindustria.it
[60] L'Allegato II lett. a) delle Disposizioni riporta tra i fattori di rischio elevato la presenza di indici reputazionali negativi relativi al cliente o la sussistenza di procedimenti penali noti e procedimenti per danno erariale, procedimenti per responsabilità amministrativa 231 e sanzioni amministrative, notizie negative provenienti dai media o da altre fonti informative attendibili.

del cliente e del titolare effettivo[61]. Queste fonti settoriali incoraggiano l'uso di *software* di analisi per l'indagine su fonti aperte, che permettono agli operatori finanziari di acquisire informazioni sulla clientela.

In sintesi, nell'attuale società dell'informazione sembra che le migliori tecniche di prevenzione degli illeciti non possano ignorare le potenzialità della rete e degli algoritmi, che diventeranno la base delle *best practice* cui conformarsi per l'adozione di modelli organizzativi e gestionali all'avanguardia.

Alcuni autori sostengono che l'impiego di sistemi automatizzati possa incidere anche sull'accertamento della colpa in organizzazione[62], nei casi in cui la verificazione dell'illecito sia in concreto dovuta al malfunzionamento o a difetti di programmazione dei sistemi informatici adottati[63]. In questi casi l'ente che dimostri di aver attuato le migliori misure tecnologiche di prevenzione andrà esente da responsabilità, difettando l'elemento soggettivo di ascrizione dell'illecito. Si prospettano tuttavia scenari di indubbia complessità per l'accertamento concreto della colpa di organizzazione, la cui sussistenza dipenderà dal grado di affidabilità degli strumenti informatici utilizzati e dalla corretta implementazione degli stessi nelle procedure indicate dal modello 231[64].

1.3. *Sistemi di monitoraggio e prevenzione dei reati.*

Con riferimento alla prevenzione dei reati presupposto nella responsabilità degli enti, si è parlato di "modello matematico 231" per descrivere un sistema automatizzato di presidi e controlli[65]. Tuttavia, ai fini che qui interessano, saranno prese in considerazione soltanto alcune attività di *compliance*, e precisamente quelle necessarie alla acquisizione di indizi di reato nelle aree di maggiore rischio.

Sulla scorta di tali premesse, il presente studio vuole fornire una panoramica dei possibili impieghi di sistemi evoluti di monitoraggio e tracciamento nell'utilizzo delle risorse informatiche aziendali, al fine di rilevare possibili anomalie nei comportamenti del personale coinvolto in processi a rischio di reato (**§2**). Si proseguirà con l'analisi pratico-applicativa delle concrete modalità di implementazione delle nuove tecnologie, ipotizzando alcuni casi d'uso in settori particolarmente critici (es. appalti pubblici, settore bancario, società quotate, **§3**).

Al riguardo è utile precisare che tra i numerosi strumenti automatizzati di raccolta, confronto e analisi dei dati, saranno prese in considerazione tre principali applicazioni: (i) quelle per la rilevazione di indicatori di anomalia e possibili segnali d'allarme – la c.d. *behavior analysis* – in base allo scostamento rispetto ai canoni ordinari di comportamento attesi in base ai modelli aziendali; (ii) il monitoraggio del traffico di dati all'interno all'azienda, allo scopo di individuare situazioni sintomatiche di condotte illecite; (iii) le tecniche di *decision intelligence* su fonti aperte, al fine di elaborare report e generare *alert* per responsabili di funzione circa eventuali rischi nella relazione con terze parti. Con riferimento a queste applicazioni saranno esaminati possibili benefici e rischi, concentrandosi in particolare sulla legittimità *de iure condito* dei sistemi più evoluti di monitoraggio e sulle possibili frizioni con i principi in materia di trattamento dei dati personali (**§4**).

La disamina sulle potenzialità delle *smart technologies* permette di giungere alla conclusione che, allo stato, esse sono uno strumento fondamentale di supporto alla *compliance* aziendale, purché siano implementate in modo attento e consapevole (**§5**).

2. La tecnologia a supporto delle funzioni aziendali.

Prima di procedere all'analisi casistica, occorre inquadrare le principali innovazioni tecnologiche utilizzate per lo sviluppo di strumenti a supporto della *compliance* aziendale. Essi saranno di seguito indicati anche con la locuzione sintetica "Strumenti di Monitoraggio Au-

[61] Gli operatori acquisiscono e valutano informazioni sulla reputazione del cliente e titolare effettivo (parte quarta, sezione II delle Disposizioni).
[62] Nisco (2022), p. 11.
[63] Birritteri (2019), p. 294
[64] Sul tema v. Gullo (2020), p. 283 ss.
[65] Trezza (2021), p. 2

tomatico" (SMA) in modo da mettere in evidenza la loro concreta applicazione nei processi di controllo aziendali.

Tali strumenti si basano su tecniche e *software* innovativi, quali l'*intelligence* su fonti aperte, gli algoritmi di Intelligenza Artificiale, e i sistemi a registro distribuito. I prodotti più complessi ed evoluti nascono dalla combinazione di più innovazioni tecnologiche, così da permettere la generazione di output maggiormente aggiornati ed affidabili.

2.1. *Analisi su fonti aperte e OSINT.*

L'*intelligence* è definita come l'insieme delle attività di raccolta, valutazione e analisi delle informazioni al fine di produrre "il sapere" necessario per il raggiungimento di determinati obiettivi. Essa può assumere connotati differenti, in base all'oggetto[66]. Ai fini della presente analisi rileva in particolare la *Open Source Intelligence* (OSINT), che si fonda sull'attività di analisi delle fonti "aperte", ovvero le fonti pubbliche, liberamente accessibili, non classificate[67]. Oggi Internet rappresenta un formidabile collettore di informazioni poiché, oltre a portali web di mass media (quotidiani online, siti di divulgazione, radio e televisione) e istituzioni[68], raccoglie una grossa mole di *user generated contents*. Per effetto della crescita imponente dei *social network*, si è delineato un nuovo concetto di *Social Media Intelligence* (SOCMINT)[69], per indicare le tecniche basate sulle informazioni che vengono prodotte e scambiate attraverso le piattaforme social, mediante il monitoraggio e l'analisi dei contenuti e delle reazioni condivisi dagli utenti. Dai canali social possono trarsi elementi utili per identificare gli utenti e cogliere eventuali relazioni tra individui e organizzazioni, ricostruire scenari e accertare la corrispondenza rispetto ad altre informazioni presenti nel web.

Tali tecniche assumono grande importanza per la *compliance* penale digitale poiché – come si avrà modo di approfondire[70] – la maggior parte degli strumenti di *decision intelligence* si basa sulla raccolta e l'analisi delle fonti pubbliche. Per fornire un significato ai dati dispersi nel web i risultati della ricerca sono rielaborati da appositi programmi o algoritmi di intelligenza artificiale.

Va peraltro rimarcato come gli orizzonti dell'OSINT stiano divenendo sempre più estesi in ragione del *favor* legislativo per l'apertura dei dati pubblici. La Direttiva 2019/1024/UE (c.d. direttiva sugli *Open Data*) promuove l'utilizzo di dati aperti e favorisce il loro riutilizzo, a fini commerciali e non commerciali, con particolare riguardo alle informazioni detenute da pubbliche amministrazioni, da organismi di diritto pubblico e imprese pubbliche[71]. Si vuole in tal modo accrescere l'offerta di dati pubblici, rendendoli più facilmente disponibili per le imprese[72], assicurando disponibilità di fonti dinamiche e in tempo reale.

Con il D. Lgs. 200/2021 il legislatore italiano ha provveduto a dare attuazione alla Direttiva, predisponendo un sistema di regole volte a incentivare la divulgazione dei dati pubblici[73]

[66] Si distingue, ad esempio, tra *Human Intelligence* (HUMINT) che ha per oggetto le fonti umane e si basa sulla raccolta delle informazioni da soggetti in possesso di informazioni rilevanti per il caso; *Imagery Intelligence* (IMINT), vale a dire l'attività di raccolta informazioni attraverso l'elaborazione e l'analisi di immagini aeree provenienti da satelliti, aerei spia, droni etc.; *Measurement and Signature Intelligence* (MASINT), riferita all'analisi scientifica e tecnica di tracce chimiche, spettrografiche e radiologiche riferite a vettori e sistemi strategici militari; *Signals Intelligence* (SIGINT), basata sull'intercettazione e l'analisi delle comunicazioni sia tra esseri umani, sia tra macchine intelligenti. Cfr. Sagliocca (2017) p. 171

[67] Nel dettaglio l'OSINT è quella disciplina dell'*intelligence* che si occupa della ricerca, raccolta e analisi di dati e informazioni disponibili in fonti aperte, legalmente accessibili al pubblico.

[68] Basti pensare alla quantità di documenti di istituzioni pubbliche reperibili online (es. atti parlamentari, rapporti dell'esecutivo, conferenze stampa, atti giudiziari, pubblicazioni accademiche, atti di convegni, relazioni annuali, albi professionali, documenti programmatici etc).

[69] Massaro *et al.* (2017), p. 425

[70] *Infra* § 4.1.

[71] Secondo la Commissione europea l'adozione della Direttiva era necessaria per rinnovare il quadro giuridico in considerazione delle rilevanti evoluzioni delle tecnologie per la condivisione dei dati e per stimolare ulteriormente l'innovazione digitale, promuovendo nello stesso tempo, la concorrenza e la trasparenza nel mercato dell'informazione pubblica.

[72] Secondo quanto si legge nella Relazione tecnica al D. Lgs. 200/20212 (camera.it) l'intervento normativo sancisce il principio generale secondo cui i dati pubblici e quelli finanziati con fondi pubblici dovrebbero essere riutilizzabili a fini commerciali o non commerciali, perseguendo anche la finalità di renderle più facilmente disponibili per le start-up e le piccole e medie imprese, aumentando l'offerta di dati dinamici e di set di dati con un impatto economico particolarmente elevato e promuovendo la concorrenza e la trasparenza nel mercato dell'informazione.

[73] Il decreto delegato è intervenuto apportando rilevanti modifiche al D. Lgs. 24 gennaio 2006 , n. 36, che già conteneva alcune disposizioni sul riutilizzo di dati pubblici. La citata Relazione tecnica al D. Lgs. 200/2021 riporta alcune statistiche degne di nota sul totale dei dati di tipo aperto resi disponibili nel Catalogo Nazionale (che ammontano a 46.1442), messi a disposizione da 559 pubbliche amministrazioni.

entro limiti ben definiti per categorie particolari di documenti[74]. Benché la finalità principale della normativa sia quella di incentivare il riutilizzo dei dati a beneficio della concorrenza, le imprese potranno utilizzare il *dataset* pubblico anche per rafforzare i sistemi interni *compliance* e le procedure di controllo attraverso l'*intelligence* su fonti pubbliche.

2.2. Machine learning *e intelligenza artificiale.*

Secondo una nota definizione l'Intelligenza Artificiale consiste in *«una scienza e un insieme di tecniche computazionali che vengono ispirate dal modo in cui gli esseri umani utilizzano il proprio sistema nervoso e il proprio corpo per sentire, imparare, ragionare e agire»*[75]. Nel linguaggio comune spesso si utilizza tale concetto per indicare forme di apprendimento automatizzato. Giova pertanto effettuare alcuni chiarimenti concettuali, partendo dalla differenza tra IA e robotica. Mentre la prima si riferisce alla riproduzione di alcune funzioni tipiche della mente umana, la seconda si riferisce alla sostituzione del lavoro corporale dell'uomo[76] con dispositivi meccanici che, nelle applicazioni più evolute, riescono anche a interagire con il mondo esterno (c.d. macchine intelligenti)[77].

Va parimenti tracciata una distinzione tra intelligenza artificiale e algoritmi. Si suole definire "algoritmo" quell'insieme di istruzioni ordinate, funzionali alla produzione di un determinato risultato. In informatica viene indicato come quel procedimento per risolvere un problema attraverso un numero finito di passi elementari, chiari e non ambigui, in un tempo ragionevole[78]. Nel descrivere il funzionamento di un algoritmo viene spesso richiamato il Teorema di Bohm-Jacopini[79] che individua tre strutture principali di elaborazione dei dati: sequenziale, alternativa e iterativa. Nella prima le istruzioni di assegnazione o di calcolo sono eseguite una dopo l'altra; nella seconda vi è una condizione che determina la scelta tra due strutture diverse da eseguire ("se la condizione è vera esegui la struttura 1, altrimenti la struttura 2"). La struttura iterativa invece è costituita dalla ripetizione di un *task* fino a che non è soddisfatta una determinata condizione ("ripeti struttura finché la condizione è vera").

Già queste semplici nozioni aiutano a comprendere come l'algoritmo e l'apprendimento automatico siano concetti non sovrapponibili[80]. Certo, anche l'algoritmo (specie se molto complesso) può essere considerato una forma di intelligenza artificiale, in quanto riproduce alcune categorie logiche della mente umana; ma non tutti gli algoritmi sono anche algoritmi di *machine learning*.

L'apprendimento automatico è quella branca dell'intelligenza artificiale che raccoglie un insieme di metodi e statistiche per migliorare progressivamente la *performance* di un algoritmo. Tecnicamente si suole parlare di apprendimento "supervisionato" quando al *software* vengono forniti esempi in forma di possibili *input* e rispettivi *output* desiderati con l'obiettivo di estrarre una regola generale che associ l'*input* all'*output* corretto. A esso si contrappone l'apprendimento "non supervisionato" dove l'algoritmo è impostato per trovare una struttura negli input forniti, senza che gli input vengano etichettati in alcun modo[81]. Infine nell'apprendimento "semi-supervisionato" si fornisce un *dataset* incompleto per allenare il *software*, cioè un insieme di dati per l'allenamento tra i quali ci sono dati senza il rispettivo *output* desiderato.

Con riferimento a queste forme di apprendimento automatico si è sviluppato il concetto di "rete neurale" per descrivere quei sistemi di elaborazione che, nel trattamento delle infor-

Con l'estensione dell'ambito soggettivo anche alle imprese pubbliche, la platea è destinata ad aumentare notevolmente poiché, dalle ultime rilevazioni dell'ISTAT, le società partecipate sarebbero circa 8.510, delle quali circa 6.085 sono imprese attive operanti nel settore dell'industria e dei servizi.

[74] L'art. 3 del D. Lgs. 36/2006, come modificato dall'art. 1 D. Lgs. 200/2021, elenca i documenti esclusi dall'ambito di applicazione del decreto tra cui quelli detenuti per finalità che esulano dall'ambito dei compiti istituzionali della PA, quelli nella disponibilità di imprese pubbliche non prodotti nella prestazione di servizi di interesse generale o connessi ad attività direttamente esposte alla concorrenza, quelli esclusi dall'accesso ai sensi dell'articolo 24 L. 7 agosto 1990, n. 24 o ai sensi dell'articolo 5-*bis* D. Lgs. 14 marzo 2013, n. 33 etc.

[75] *Artificial Intelligence and life in 2030, One hundred year study on Artificial Intelligence,* Stanford University, 2016, 5, in ai100.stanford.edu/2016-report.

[76] Secondo alcuni robotica deriva dal ceco *robota* che significa "lavoro forzato"; altri ritengono sia una flessione del sostantivo latino *vis-roboris* (forza, energia).

[77] Sul tema di recente v. Minneci *et al.* (2021)

[78] Per approfondimenti sugli algoritmi si rinvia al saggio di Laura (2019)

[79] Bianchini (2007) p. 23

[80] Gillespie (2014), p. 167 ss.

[81] Mozzarelli (2022), p. 266

mazioni, presentano alcune analogie con l'intelligenza naturale tra cui quella di ponderare i fattori di ingresso per giungere a un *output*[82]. Si deve al filosofo Searle[83] la distinzione tra IA debole e forte: la prima svolge alcune funzioni semplici dell'intelletto umano, mentre la seconda è dotata di una capacità cognitiva assimilabile a quella umana.

Ai fini del presente studio, si farà riferimento alla nozione giuridica di Intelligenza Artificiale contenuta nell'art. 3 della Proposta di Regolamento 2021/0106 (COD). É considerato "sistema di intelligenza artificiale" quel software sviluppato secondo uno o più degli approcci elencati *«che sia in grado di generare risultati come contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagisce alla luce degli obiettivi definiti dall'uomo»*. L'allegato I della Proposta indica tre gruppi di tecnologie: (a) approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, tra cui l'apprendimento profondo (*deep learning*); (b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti; (c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione. Si tratta di una nozione molto elastica, che attrae nell'ambito dell'IA tutte le applicazioni, i servizi, e i dispositivi che riflettono le categorie di ragionamento della mente umana.

Nella materia penalistica l'intelligenza artificiale solleva numerosi interrogativi sul fronte del diritto penale sostanziale (imputabilità, rilevanza causale del danno provocano da sistemi intelligenti, rischio consentito, rapporto di autoria tra agente e fatto di reato)[84] e processuale (utilizzo di algoritmi predittivi per la commisurazione della pena o per determinare la pericolosità sociale di un individuo)[85]. Alcuni autori hanno trattato il tema dalla prospettiva della prevenzione attiva dei reati (c.d. *predictive policing*), facendo riferimento a particolari applicazioni progettate per coadiuvare le forze dell'ordine[86]. Sulla medesima scia si colloca l'oggetto di questo studio, che effettua una ricognizione delle potenzialità offerte dall'IA per la prevenzione dei reati nelle organizzazioni complesse[87], attraverso applicazioni che potremmo definire di *predictive compliance*.

2.3. *Tecnologia a registro distribuito* (Distributed Ledger Technology – DLT).

Le tecnologie a registro distribuito (*Distributed Ledger Technology* o anche DLT) costituiscono una classe di tecnologie complesse fondate sulla combinazione di diverse tecniche informatiche. Tra esse la specie più nota è quella comunemente denominata *blockchain.* Quest'ultima nasce dalla combinazione di due tecnologie diverse, la crittografia asimmetrica e i protocolli di comunicazione *peer-to-peer*, all'interno di una rete interconnessa di elaboratori[88].

Pur racchiudendo soluzioni tecnologiche molto diverse tra loro, le *blockchain* presentano una serie di proprietà comuni riassumibili in quattro principali caratteristiche: (i) la *resilienza* (c.d. *tamper resistance*), poiché ogni nodo reca in sé copia di tutte le transazioni precedenti, sicché, non esistendo alcun singolo punto di fallimento, il sistema è in via generale impossibile o comunque difficile da compromettere nella sua interezza; (ii) la *tendenziale irreversibilità e non ripudiabilità* delle transazioni, che una volta iscritte nel *ledger*, non possono essere modificate se non con il concorso di una maggioranza qualificata di nodi; (iii) l'*immediatezza e automaticità delle transazioni*, che sono processate istantaneamente e automaticamente dai nodi

[82] La rete neurale è costituita da unità elaborative che presentano collegamenti di varia intensità. Partendo dalle unità di input il calcolo si propaga in parallelo nella rete fino alle unità di output, che forniscono il risultato. La rete non viene programmata con istruzioni *ex ante* sull'output, ma addestrata mediante una serie di esempi che consentono l'affinamento dell'output nel tempo. Si parla a tal proposito di *deep learning* per indicare l'insieme di tecniche basate su reti neurali complesse, che permettono l'affinamento della ponderazione, affinché l'informazione finale sia il più possibile completa e affidabile.
[83] Searle (1980), p. 417
[84] Sul tema sia pur con diversità di prospettive v. Consulich (2018), p. 195 ss.; Basile (2019), p. 24 ss.; Borsari (2020); Ubertis, (2020), p. 75.
[85] Nella letteratura straniera v. Burchard (2019b), p. 3 ss.; Starr (2014), p. 809; Kehl *et al.,* (2017). Nella dottrina italiana v. Gialuz (2019); Maugeri (2021); Manes (2020).
[86] Bennett Moses e Chan (2018), p. 806.; Birritteri (2019), p. 291.
[87] Sull'utilizzo dell'IA nella prevenzione della corruzione v. di recente De Simone (2022), p. 51.
[88] Gambino e Bomprezzi (2019), p. 623

validatori; (iv) l'*attribuzione univoca dell'informazione*, assicurata dall'utilizzo della crittografia asimmetrica[89].

Richiamando in estrema sintesi il funzionamento della più nota *blockchain*, quella di Bitcoin, essa si basa sulla marcatura temporale delle transazioni, raggruppate progressivamente in blocchi per formare una vera e propria catena. Le nuove transazioni sono trasmesse a nodi della rete che, previa verifica della validità del trasferimento, si attivano per trovare un numero casuale che possa risolvere una predeterminata funzione algebrica.

Le caratteristiche sin qui esaminate sono proprie della *blockchain* c.d. pubblica in cui manca un titolare del sistema: il connotato essenziale è la decentralizzazione dell'infrastruttura in una pluralità di nodi gestiti da soggetti diversi[90]. Nei sistemi totalmente decentralizzati nessun utente ha privilegi sugli altri, o può controllare le informazioni che vengono memorizzate nei registri, modificarle o eliminarle. Nei sistemi pubblici la fiducia nella rete sembra giustificarsi proprio in virtù della disintermediazione negli scambi, che rappresenta un fattore di garanzia contro i possibili abusi da parte dell'autorità centrale.

Nell'ottica dell'automazione della *compliance* penale, assume particolare rilevanza l'archiviazione di dati informatici sui sistemi DLT, che assicura la certezza della data, l'identificazione univoca del firmatario della transazione, e la tendenziale immodificabilità del registro. Si tratta di una delle caratteristiche di maggior pregio della tecnologia a registro distribuito, tanto che il legislatore vi ha fatto espresso riferimento nella L. 11 febbraio 2019, n. 12 di conversione del D.L. 14 dicembre 2018, n. 135. L'art. 8-*ter* definisce le DLT[91] e pone le basi per attribuire valore legale alle registrazioni di dati informatici in *blockchain*. Si prevede che la memorizzazione di un documento informatico su un registro distribuito produca gli «*effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014*»[92], purché siano rispettati gli standard tecnici fissati dall'Agenzia per l'Italia Digitale[93].

Nel contesto qui in esame, appaiono evidenti i vantaggi delle DLT nella gestione dei dati all'interno dell'ente[94], non solo per la possibilità di "notarizzare" alcune informazioni rilevanti (es. conferimento di deleghe, comunicazioni ufficiali agli organi di controllo etc.) senza ricorrere a soggetti terzi, ma anche per potenziare il controllo dei responsabili sulle diverse procedure previste dal modello organizzativo (es. tracciamento dei passaggi intermedi per l'approvazione di una autorizzazione di spesa).

3. Prevenzione dei reati *ex* D. Lgs. 231/2001. Individuazione di possibili casi d'uso.

Possiamo ora esaminare da vicino le potenzialità offerte dalle *smart technologies* per la prevenzione di reati all'interno delle organizzazioni complesse. La casistica d'uso che segue è stata elaborata sulla falsariga degli elementi ricavabili da modelli organizzativi e gestionali 231 pubblicati sui siti web di importanti società nazionali. Prendendo spunto dai sistemi interni di controllo (es. flussi informativi verso l'OdV, gestione dei flussi finanziari etc.) nelle aree ritenute a rischio di reato, si è delineato uno scenario ipotetico di applicazione degli SMA nelle

[89] Si suole definire la *blockchain* come un registro tendenzialmente inalterabile, poiché nessuno dei nodi dispone – né potrà mai ragionevolmente disporre – di una potenza computazionale sufficiente a imporre un "monopolio" sul processo di verifica delle transazioni. La decentralizzazione diviene così un presidio contro il c.d. attacco del 51%, che si verificherebbe laddove uno o più soggetti, avendo il controllo della maggioranza dei nodi, potessero falsificare *ex post* le registrazioni, decidere unilateralmente quali trasferimenti validare o eludere i presidi contro il *double spending*. Tale caratteristica è propria delle reti pubbliche ad accesso libero, in cui chiunque può mettere a disposizione le proprie risorse per entrare a far parte del *network*.

[90] L'accesso alla rete può essere *permissionless* o *permissioned:* nel primo caso chiunque può prendere parte alla rete, semplicemente scaricando il *software* base e mettendo a disposizione un *hardware* connesso al sistema; nel secondo caso sono previste delle particolari condizioni per il rilascio dell'autorizzazione da parte di una autorità che verifica il rispetto delle condizioni di accesso e definisce il ruolo di ciascun partecipante.

[91] La disposizione definisce le DLT come quelle «*tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili*».

[92] La materia è oggi disciplinata dal Regolamento 910/2014/UE che, in un'ottica di armonizzazione delle legislazioni nazionali, individua i requisiti e gli effetti giuridici della validazione temporale elettronica. Circa gli effetti giuridici della validazione temporale il Regolamento prevede che ad essa «*non possano essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali*». Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora, e di integrità dei dati ai quali tale data e ora sono associate.

[93] Ad oggi si resta ancora in attesa della pubblicazione della normativa secondaria dell'AgID sui requisiti tecnici che le DLT debbono possedere in fini indicati dall'art. 8-*ter* D.L. 135/2018. Per approfondimenti v. Piselli e D'Agostino (2019), p. 13

[94] De Simone, (2022), p. 67 ss.

procedure descritte dai modelli organizzativi.

3.1. *Gestione di sistemi informatici di pubblica utilità e appalti pubblici.*

Il primo *case study* riguarda la gestione di un sistema informatico utilizzato da una Centrale di committenza per lo svolgimento di procedure a evidenza pubblica. Gli operatori economici che intendono partecipare alle gare acquisiscono tutte le informazioni utili e accedono al sistema di deposito delle domande di partecipazione direttamente dalla piattaforma messa a disposizione da una società terza.

All'esito delle attività di *risk assessment* tale società ha ritenuto che alcuni processi interni – e in particolare quelli relativi alle attività di supporto tecnico e manutenzione della piattaforma – siano particolarmente esposti al rischio di reato. Nel dettaglio, si è ritenuto concreto il rischio di commissione dei seguenti delitti: (a) frode informatica a danno dello Stato o di altro ente pubblico (art. 24 D. Lgs. 231/2001 in relazione all'art. 640-*ter* c.p.), poiché i dipendenti addetti al supporto sono dotati dei privilegi di amministratore di sistema e possono intervenire sulle informazioni pubblicate sulla piattaforma, modificandole a propria discrezione. Si teme in particolare che vi possa essere un intervento senza diritto sui dati relativi alle coordinate per i pagamenti (es. spese per la partecipazione, versamento di cauzioni provvisorie alle Stazioni appaltanti), al fine di ottenere un profitto; (b) accesso abusivo a sistema informatico (art. 24-*bis* D. Lgs. 231/2001 in relazione all'art. 615-*ter* c.p.) con riferimento alle informazioni e ai segreti commerciali contenuti nelle offerte tecniche formulate dagli operatori economici in sede di gara. Difatti il Sistema gestisce anche procedure per l'acquisto di servizi informatici, che potenzialmente rientrano nel business della Società concessionaria. Si teme quindi un accesso non autorizzato finalizzato ad acquisire informazioni commerciali (es. soluzioni tecniche, *know-how* etc.) da poter riutilizzare a vantaggio della società in altre gare pubbliche; (c) danneggiamento informatico (art. 24-*bis* D. Lgs. 231/2001, in relazione agli artt. 635-*bis* ss. c.p.), falso informatico (art. 24-*bis* D. Lgs. 231/2001, in relazione all'art. 491-*bis* c.p.) e frode informatica a danno dello Stato o di altro ente pubblico, relativamente al rischio di cancellazione o alterazione di dati dal Sistema per favorire alcuni partecipanti (es. imprese con cui sussistono buoni rapporti commerciali o di collaborazione).

Ciò posto, la società vorrebbe dotarsi di alcuni applicativi che consentano di rilevare anomalie e segnalarle ai competenti organi di controllo. In particolare, con riferimento alle ipotesi *sub* (a), un sistema di *alert* nel caso in cui, durante una sessione, siano in qualsiasi modo modificati o alterati parametri relativi a spese e pagamenti (importi, coordinate bancarie, termini di pagamento, e altre informazioni economicamente rilevanti). Inoltre, per agevolare l'emersione di eventuali condotte illecite, l'applicativo dovrebbe poter effettuare un controllo automatizzato e un *matching* con le comunicazioni effettuate all'interno dell'azienda (es. rilevare che nei giorni precedenti, in un messaggio di posta si discuteva di modificare un importo o una coordinata bancaria)[95].

Quanto all'ipotesi *sub* (b), si ipotizza l'impiego di un *software* in grado di riconoscere per parole chiave le procedure e le offerte in qualche modo connesse e collegate al business della società, esposte al rischio di accesso abusivo. In tal caso l'applicativo dovrebbe limitare l'accesso a utenze predeterminate (es. ai soli responsabili incaricati) e tenere traccia di eventuali copie o *download* di documenti dalla piattaforma.

Infine, avuto riguardo ai reati *sub* (c), si prospetta l'utilizzo di un applicativo "intelligente" che possa segnalare agli organi di controllo della società l'avvenuta registrazione nel Sistema (oppure la presentazione di un'offerta) di un'impresa potenzialmente affiliata o comunque nota alla Società. Il *software* dovrebbe essere in grado di associare la denominazione dell'impresa all'elenco dei fornitori oppure alle registrazioni contabili della Società, ovvero di consultare fonti aperte (es. motori di ricerca, *web crawling*, etc.) per trovare dei collegamenti tra due o più aziende (es. si riesce a riconoscere che l'impresa partecipante alla gara fa parte di un gruppo affiliato etc.). L'applicativo dovrebbe anche consentire di segnalare eventuali scambi di messaggi, in entrata o in uscita, con indirizzi riconducibili all'impresa affiliata nei giorni precedenti o successivi rispetto alla registrazione nella piattaforma.

[95] Un tale applicativo potrebbe essere utile anche per far emergere possibili dinamiche corruttive nel caso in cui l'intervento senza diritto sui dati di pagamento sia stato oggetto di trattative illecite con un funzionario pubblico.

3.2. Compliance *nel settore bancario-creditizio.*

Un secondo caso d'uso riguarda da vicino il settore bancario-finanziario. Nel modello organizzativo e gestionale di una Banca sono individuate alcune attività a rischio di reato, tra cui le seguenti: (a) corruzione attiva (art. 25 D. Lgs. 231/2001, in relazione all'art. 321 c.p.), poiché la società intrattiene rapporti economici con molti Comuni ed enti pubblici, gestendo fondi per centinaia di milioni di Euro. Si ritiene particolarmente concreto il rischio che i dirigenti della società possano pagare tangenti per ottenere una proroga nell'affidamento dei servizi; (b) ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza (art. 25-*ter* D. Lgs. 231/2001 in relazione all'art. 2638 c.c.) con riferimento in particolare alla mancata comunicazione mensile dei dati relativi ad alcune operazioni alla Banca D'Italia; (c) riciclaggio (art. 25-*octies* in relazione agli artt. 648-*bis* e seguenti c.p.), finanziamento del terrorismo (art. 25-*quater* in relazione all'art. 270-*quinquies.1* c.p.) o delitti di criminalità organizzata (art. 24-*ter* D. Lgs. 231/2001) nell'instaurazione di relazioni di affari con nuovi clienti.

Visti gli esiti dell'ultima valutazione dei rischi, la Banca vorrebbe integrare alcuni SMA nei processi aziendali per facilitare l'emersione di prassi o flussi finanziari a rischio di reato. Segnatamente, avuto riguardo al rischio di corruzione attiva *sub* a), un sistema in grado di individuare attraverso tecniche di OSINT o sulla base di istruzioni predeterminate, i nominativi dei vertici amministrativi (dirigenti, alti funzionari) e politici (sindaci, presidenti etc.) di enti pubblici con cui la Banca intrattiene rapporti economici. Il sistema dovrebbe monitorare le comunicazioni che intercorrono tra la Banca e gli indirizzi istituzionali dei funzionari coinvolti, in modo da segnalare eventuali anomalie (ad es. uno scambio di mail tra indirizzi con richieste di incontro o di appuntamento).

Con riferimento alla prevenzione del reato *sub* (b), un SMA in grado di segnalare le anomalie comportamentali rispetto alle procedure ordinarie seguite dalla Banca e alle tempistiche individuate dalla legge. Tale sistema dovrebbe prevedere *alert* e segnalazioni automatizzate qualora, ricevuta una richiesta qualificata da un indirizzo istituzionale, l'organizzazione non segua il pattern di comportamento atteso (es. non si osservino le procedure previste dal modello o vi siano comunicazioni sintomatiche della volontà di occultare certe informazioni).

Infine, rispetto al rischio di commissione dei reati *sub* (c), si vorrebbe implementare un sistema in grado di estrapolare dati da fonti *open source* per calcolare un punteggio di rischio associato alla persona fisica o giuridica che richiede di entrare in affari con la Banca. Nella specie, il *software* dovrebbe essere in grado di: sintetizzare in un report le notizie disponibili online sul cliente, relativi a possibili coinvolgimenti in atti illeciti (es. legami con la criminalità organizzata, indagini per fatti di riciclaggio); confrontare le risposte fornite dal cliente in sede di acquisizione di informazioni AML con le notizie disponibili online (es. sul profilo di rischio o sulla professione del cliente); fornire un *alert* ogniqualvolta, successivamente alla instaurazione della relazione d'affari, sopravvengano nuove notizie sulla posizione del cliente[96].

L'applicativo dovrebbe avere due funzionalità essenziali: la generazione di report reputazionali *one-shot* prima di entrare in affari con il cliente; il monitoraggio periodico alla ricerca di nuove informazioni online. Con riferimento a questa seconda funzione, il nominativo del cliente inserito in "black-list" sarà oggetto di successivi controlli automatizzati; il sistema provvederà ad inviare in tempo reale un *alert* non appena risulteranno disponibili in rete informazioni potenzialmente rilevanti.

3.3. *Società quotate, redazione di bilanci e conflitti di interessi.*

Si è infine ipotizzato il caso di una società quotata, facente parte di un gruppo, il cui modello organizzativo e gestionale – adottato ai sensi dell'art. 6 del D. Lgs. 231/2001 – individua alcuni processi a rischio di reato tra cui: (a) quelli collegati all'ufficio acquisti, con particolare riferimento ai delitti di falso in bilancio (art. 25-*ter* D. Lgs. 231/2001 in relazione agli artt.

[96] Le analisi reputazionali saranno attivate soltanto in casi specifici (es. quando vengono richieste operazioni superiori a un certo ammontare) o quando si abbia motivo di ritenere che l'attività esercitata dal Cliente presenta il rischio di interferenze illecite.
Per *software* di questo tipo si veda ad es. il sistema CERICO, offerto da Dow Jones Risk & Compliance; oppure il software World Check della Thomson-Reuters che comparano dati provenienti da svariati fonti pubbliche al fine di valutare i rischi legali e reputazionali che l'impresa può correre intraprendendo una certa operazione. Sul tema, anche per riferimenti alla letteratura statunitense v. Birritteri (2019), p. 295.

2621 e seguenti c.c.) e corruzione (art. 25 D. Lgs. 231/2001, in relazione all'art. 321 c.p.), stante la verificazione in passato di fenomeni di *overpricing* e di *downpricing* (stipulazione di contratti e iscrizione a bilancio di prezzi per acquisiti molto superiori rispetto alla media del mercato); (b) quelli relativi alle deliberazioni del CdA su particolari materie, limitatamente al reato di omessa comunicazione del conflitto di interessi (art. 25-*ter* D. Lgs. 231/2001 in relazione all'art. 2629-*bis* c.c.), tenuto conto del consistente numero e della frequente alternanza dei membri del CdA (che durano in carica tre anni e che spesso, in passato, hanno ricoperto posizioni analoghe in primarie società nazionali).

La società intende automatizzare parte dei compiti di controllo attribuiti all'OdV e ai revisori contabili e dotarsi di strumenti di analisi preventiva di possibili rischi. Nella specie, con riferimento ai reati *sub* (a) utilizzare un applicativo integrato nel gestionale in uso, che possa confrontare in modo automatico e in tempo reale i prezzi di acquisto con il prezzo medio di mercato desumibile da listini, mercuriali o tariffari (specialmente per acquisti standardizzati). A tal fine si prevede che per ogni acquisto debba essere compilato un *form* in formato *excel* nel quale sono riportate quantità e prezzi di acquisto. L'applicativo dovrà pertanto estrarre questi dati e confrontarli con quelli desumibili da fonti aperte e inviare un *alert* ai responsabili in caso di anomalie.

Quanto al reato *sub* (b), la società vorrebbe sfruttare le potenzialità dell'OSINT per rivelare l'esistenza di potenziali conflitti di interessi nelle relazioni con terze parti. Il *software* dovrà essere in grado di rivelare l'esistenza di pregressi rapporti (professionali, imprenditoriali, amicali etc.) tra gli amministratori o i componenti del Consiglio di Gestione e terzi fornitori o controparti contrattuali. Tra i criteri rivelatori del "conflitto di interessi" saranno considerati anche i precedenti professionali del vertice aziendale in una data materia (es. se l'operazione riguarda l'acquisto di autovetture, si potrà fornire al *software* una istruzione per verificare un *linkeability* tra l'amministratore e il settore automotive). In sostanza l'analisi verterà tanto su rapporti personali diretti (associazione per soggetto), quanto su legami indiretti (associazione per oggetto).

4. Applicazione delle nuove tecnologie ai casi d'uso considerati.

I casi d'uso sopra esemplificati rappresentano soltanto alcune possibili applicazioni dei SMA per l'automazione della *compliance* penale. Le soluzioni tecnologiche ivi descritte non sono strettamente legate a tali contesti, e possono essere applicate per la prevenzione di reati anche in ambiti e settori economici diversi.

Poiché i *software* di raccolta e analisi dei dati non sono stati sviluppati per offrire supporto alla *compliance* penale, ci si interroga sul possibile impiego di tali programmi al fine prevenire la commissione di reati all'interno dell'azienda[97]. La soluzione affermativa dipende, in buona misura, dalla capacità dell'ente di riadattare gli applicativi di uso comune (es. SIEM, sistemi di *Data Classification* etc.) per favorire i controlli sui processi a rischio di reato. Si tratta di un'attività complessa che richiede competenze tecniche adeguate per mettere in funzione e supervisionare l'utilizzo dei sistemi. Si dovranno inoltre individuare i *cluster* di dati rilevanti ai fini della elaborazione di un *output*, e predisporre le dotazioni *hardware* (sistemi, *workstation*, *server* etc.) e di connessione (es. intranet aziendale) necessarie per l'utilizzo degli applicativi.

Nel prosieguo, gli strumenti di supporto alla *compliance* sono analizzati in base alle diverse tipologie di *software* utilizzabili.

4.1. Software *di* decision intelligence *e OSINT.*

L'imponente mole di dati reperibile online rappresenta un vero e proprio patrimonio informativo che gli enti possono impiegare a supporto della *compliance* penale. I programmi di analisi su fonti aperte sono stati elaborati per agevolare la raccolta di informazioni sulle controparti contrattuali (c.d. *due diligence* di terze parti) in modo da rendere più consapevole la decisione di entrare in affari con determinati soggetti. Più in generale di parla di *decision*

[97] Morgante e Fiorinelli (2022), p. 8

intelligence (o *decision support*) per descrivere quei *software* in grado di mettere in relazione due o più chiavi semantiche ordinando i risultati della ricerca secondo impostazioni predefinite[98]. Il principale scopo di tali programmi è quello di comporre un quadro conoscitivo per assumere scelte consapevoli nella gestione societaria.

Di regola questi software eseguono uno *scraping*[99] delle risorse del web, passando in rassegna i risultati forniti dai motori di ricerca, ordinati secondo filtri e criteri specifici. Ciò consente di cogliere la relazione tra due o più elementi testuali e di rendere intellegibile la correlazione tra essi; talvolta si utilizza la trasposizione in grafi[100] per illustrare in modo figurato l'associazione logica tra i risultati e consentire la c.d. *link analysis*.

Gli applicativi più evoluti permettono di eseguire ricerche per chiavi semantiche non soltanto su fonti aperte ma anche su database privati (es. archivi e risorse informatiche dell'azienda)[101], e di porre eventualmente in relazione i relativi risultati. La ricerca può avere ad oggetto dati strutturati o non strutturati[102] come emerge dalla casistica d'uso sopra esemplificata[103].

Per la raccolta e l'analisi delle informazioni si utilizzano tecniche di intelligenza artificiale applicate all'analisi semantica e multimediale, mediante algoritmi di *data mining* molto avanzati. Questi aggregano i dati in modo massivo, offrendo agli analisti un quadro generale ottenuto dalla correlazione di una pluralità di fonti e la visualizzazione di relazioni complesse tra le chiavi di ricerca. I programmi più avanzati si servono del *machine learning* anche per raffinare i risultati della query escludendo falsi negativi e falsi positivi dalla correlazione semantica[104].

Una volta elaborato il sistema di correlazione tra i dati, gli applicativi in esame permettono di analizzare i trend in tempo reale, aggiornandosi in base ai nuovi dati inseriti nel database o rintracciati online. L'analisi dinamica e continuativa delle fonti si rivela fondamentale per i processi di controllo aziendali poiché consente di generare automaticamente segnali di anomalia[105]. I modelli organizzativi dovrebbero prevedere specifiche procedure di riesame degli *alert*, attivando gli opportuni presidi nel caso in cui la segnalazione risulti attendibile.

La nota di maggior pregio degli strumenti in esame consiste nella possibilità di costruire ricerche "mirate" per argomento selezionando una o più categorie da una lista predefinita. Alcuni *software* prodotti da società americane sono stati sviluppati per la *due diligence* in determinati ambiti disciplinari attraverso la previa selezione di tutte le parole chiave e le forme flesse di uso comune in tali ambiti. Sarà dunque sufficiente inserire il nome di una persona fisica o di un ente per ottenere, all'esito della *query*, ogni possibile correlazione tra questi e i settori considerati[106]. Le imprese potranno così prevenire l'instaurazione di rapporti con soggetti coinvolti in affari illeciti e verificare la veridicità di quanto dichiarato da clienti e fornitori.

Sul versante giuridico emergono tuttavia alcune criticità collegate al trattamento dei dati personali, laddove il sistema attribuisca alle persone fisiche una classificazione di rischio[107]. Se-

[98] Alcuni applicativi permettono di fare ricerche non soltanto in pagine del *surface web*, ma persino nella parte "oscura" (il c.d. *dark web*) della rete.

[99] Lo *scraping* è una tecnica che consiste nel prelevare dati dal web. Il processo di estrazione è automatizzato grazie all'uso di un software che, dopo aver visitato un sito per ottenere dati, compila un database e analizza i risultati. Si pensi, ad esempio, ai siti che mettono a confronto i prezzi di alcuni prodotti (es. viaggi, assicurazioni etc.) mediante *web scraping* dei portali di vendita online.

[100] Il grafo in informatica descrive una figura geometrica (bidimensionale o tridimensionale), costituita da un insieme finito di punti, detti nodi (o vertici), e da segmenti o archi che congiungono coppie di nodi.

[101] Alcune piattaforme disponibili sul mercato si basano su tecniche OSINT e SOCMINT per integrare i dati ricavabili da fonti aperte con le informazioni dei database aziendali. Il matching tra i dati è effettuato impartendo le istruzioni fondamentali al software e dettando criteri specifici. A tal fine è indispensabile il ruolo dell'analista dei dati nell'impostare il sistema a seconda delle specifiche esigenze.

[102] Con "dati strutturati" si suole indicare quelli organizzati secondo schemi e tabelle (es. un file excel). Sono invece "non strutturati" i dati privi di schema (come quelli contenenti testi a carattere narrativo o file multimediali).

[103] Nel caso del software che mette in relazione i tabulati dell'ufficio acquisti con i listini prezzi ufficiali (v. *supra* §3.3 lett. a) i dati saranno disponibili in forma strutturata. Diversamente, per la valutazione del punteggio di rischio associato a determinate operazioni (v. § 3.2. lett. c) e in genere in tutti i casi di due diligence di terze parti si tratta di dati non strutturati.

[104] Ipotizzando una ricerca sull'affiliazione commerciale (v. § 3.1., lett. c) tra l'impresa Alfa e Beta, l'utilizzo del *machine learning* permette di non inquinare la ricerca con risultati in cui "Alfa" e "Beta" sono utilizzati in altri contesti lessicali. Il Natural Language Processing (NLP) indica gli algoritmi di IA in grado di analizzare il linguaggio naturale per comprenderne il contenuto, estrapolarne il significato, tradurlo in altra lingua etc., a partire da dati o documenti forniti in input. Si parla anche di linguistica computazionale per indicare lo studio del linguaggio naturale in modo da elaborare programmi eseguibili dalle macchine.

[105] Così, nei casi pocanzi esemplificati il sistema genera un *alert* quando sopravvengono notizie su un cliente ritenuto a rischio (v. § 3.2. lett. c) o sui rapporti tra un apicale della banca e un cliente coinvolto in una operazione economicamente molto rilevante.

[106] Per valutare il coinvolgimento di un socio in affari in traffici illeciti si potrà spuntare la categoria "criminalità organizzata" per ottenere l'associazione del nominativo a parole chiave come mafia, art. 416-*bis,* concorso esterno, scambio elettorale, boss, intimidazione, misura di prevenzione, DIA, etc.

[107] Sul tema del rating reputazionale, sia pur prospettive diverse, v. Sciascia (2021), p. 317 ss.; Ammannati e Greco (2021), p. 290

condo una recente sentenza di legittimità[108], gli strumenti di calcolo del rating reputazionale delle persone fisiche sono illegittimi in assenza di specifico ed espresso consenso dell'interessato. Nello specifico la Cassazione ha affrontato il caso di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali concernenti persone fisiche e giuridiche, col fine di contrastare fenomeni basati sulla creazione di profili artefatti o inveritieri e di calcolare, invece, in maniera imparziale la reputazione dei soggetti censiti, in modo da consentire a eventuali terzi una verifica di reale credibilità. Nell'accogliere il ricorso proposto dall'Avvocatura dello Stato, la Corte ritiene che il problema alla base del calcolo del rating è costituito dalla validità del consenso che si assume prestato al momento della registrazione. Non potrebbe dirsi valida l'adesione a un sistema automatizzato, che si avvale di un algoritmo per la valutazione oggettiva di dati personali, laddove non siano resi conoscibili gli schemi con cui il software si esprime né i fattori considerati.

Nel giudizio di merito il Tribunale di Roma[109] aveva riconosciuto l'illegittimità del rating reputazionale riferito a soggetti che non avevano prestato il consenso per accedere al servizio, i cui nominativi potevano desumersi dai documenti inseriti nella piattaforma.

Nell'applicare tali principi alla raccolta di dati ricavabili da fonti aperte e alle attività di OSINT, emergono sostanziali differenze rispetto al caso affrontato dalla Corte. *In primis* perché il trattamento ha ad oggetto unicamente dati pubblicati sul web accessibili a chiunque finché l'interessato non eserciti i propri diritti (es. limitazione o cancellazione); in secondo luogo perché la maggior parte dei programmi non elabora un punteggio reputazionale, limitandosi a mettere in correlazione notizie, link e immagini. Pur non essendo dubitabile che l'impiego di tali *software* possa dar luogo a un "trattamento" in senso tecnico-giuridico[110], è altrettanto vero che esiste una base giuridica che legittima le operazioni[111].

4.2. *SIEM e analisi dei dati di traffico.*

L'analisi dei dati di traffico viene spesso utilizzata in chiave preventiva di possibili attacchi informatici ai danni dell'impresa; essa rappresenta una misura di *cybersecurity* particolarmente efficace per tenere traccia di tentativi di intrusione da parte di IP sconosciuti o per sventare minacce cibernetiche di vario genere.

In informatica si parla di *Security Information and Event Management* (SIEM)[112] per indicare quei *software* di monitoraggio in tempo reale degli eventi di rete, in grado di correlare, segnalare e reagire in modo automatico a determinati accadimenti. Il programma tiene traccia, all'interno di un registro, di tutti i dati di traffico al fine di rilevare possibili minacce alla sicurezza della rete aziendale. I prodotti più diffusi sul mercato prevedono l'installazione del SIEM all'interno di un *server* centralizzato nel quale confluiscono tutti i dati di traffico generati dalla rete locale[113]. I dati raccolti e processati non riguardano il contenuto delle comunicazioni informatiche, ma soltanto gli estremi delle comunicazioni intercorse[114]; nel registro degli eventi si tiene traccia dei log e degli indirizzi IP, dell'ora e della data della connessione ed eventualmente della quantità di dati scambiati. Dopo la fase di raccolta e acquisizione, il sistema procede al c.d. *arricchimento* dei dati, ricavando informazioni sulla localizzazione geografica dell'IP e sulla reputazione ad esso attribuitagli da fonti autorevoli.

[108] Cass. Civ., Sez. I, 25 maggio 2021 n. 14381 in *Media Laws*, 16 giugno 2021, con nota di Paolucci (2021); e in Federalismi.it, 11 agosto 2021, con nota di G. Lo Sapio (2021).
[109] Tribunale di Roma, Sez. I, 4 aprile 2018, n. 5715.
[110] L'art. 4, par 1, n. 2 GDPR definisce il "trattamento" come «*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*».
[111] Da rinvenirsi, a seconda dei casi, nel consenso dell'interessato (si pensi ai dati spontaneamente condivisi sui *social network*), nell'esistenza di un obbligo legale al quale è soggetto il titolare del trattamento (es. obblighi di identificazione della cliente e segnalazione delle operazioni sospette in base alla normativa antiriciclaggio), nel perseguimento del legittimo interesse dell'impresa o di terzi, O nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (cfr. sulle condizioni di liceità del trattamento, art. 6 GDPR).
[112] L'acronimo nasce dalla crasi di SIM (*Security Information Management*) e SEM (*Security Event Management*) per definire quei programmi che presentano entrambe le funzionalità (gestione della sicurezza delle informazioni e gestione degli eventi informatici).
[113] Le attività in entrata e in uscita tra i *device* all'interno della rete aziendale sono duplicate attraverso una porta SPAN (*Switched Port Analyzer*), che produce una copia *mirror* del traffico di rete per inviarlo al server SIEM di destinazione.
[114] Ai fini della normativa privacy "dato relativo al traffico" è «*qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione*» (art. 1, comma 1, lett. h D. Lgs. 196/2003).

Gli eventi sono classificati per tipologie e associati in base a regole di correlazione predefinite, ferma la possibilità di impartire istruzioni personalizzate a fronte di esigenze specifiche. Tali regole rendono fruibile il registro degli eventi che, anche in organizzazioni di ridotte dimensioni, conta migliaia di attività al giorno.

Laddove il SIEM dovesse individuare attività anomale, verrà emessa una notifica per segnalare la presenza di una possibile minaccia[115]. I programmi più evoluti attribuiscono un punteggio di rischio (es. in scala decimale) agli eventi di rete, così da far emergere immediatamente le attività maggiormente pericolose. Grazie all'uso del *machine learning* il SIEM perfeziona la regola di giudizio "allenandosi" su un database di eventi-tipo, nel quale gli analisti hanno valutato casi analoghi. Tra i principali indici di rischio si tiene conto della reputazione dell'indirizzo IP in base alla sua provenienza geografica, al numero di "visite" e alla prossimità temporale delle richieste di accesso[116]. Per rilevare anomalie il sistema tiene traccia di tutte le attività intercorse nei giorni precedenti, di modo che un evento considerato "neutro" sarà valutato come una potenziale minaccia laddove venga rilevato un pattern anomalo di comportamento.

Di regola i SIEM sono utilizzati per prevenire attacchi informatici mediante il blocco automatico delle attività sospette, respingendo ad es. le richieste di accesso e connessione ritenute sospette, o per rilevare la presenza di *malware*. Si tratta ora di comprendere se, ed eventualmente in che misura, applicativi di questo genere possano coadiuvare la prevenzione di reati commessi nell'esercizio dell'impresa. Attuando una sorta di capovolgimento di prospettiva, si dovrà chiarire se i SIEM siano in grado di fornire una qualche utilità nel caso di illecito commesso nell'interesse o a vantaggio dell'ente.

A ben vedere, l'analisi dei dati di traffico permette di rilevare anomalie anche nelle comunicazioni in uscita o interne all'azienda. Il sistema tiene traccia delle autenticazioni attraverso le periferiche di rete, individuando eventuali accessi non autorizzati o violazioni delle politiche interne all'impresa. Poiché la correlazione tra eventi si basa su criteri predefiniti, l'utilizzo dei SIEM nei sistemi di controllo *ex* D. Lgs. 231/2001 appare sicuramente plausibile dal punto di vista tecnico. Il sistema andrà customizzato per mettere in evidenza gli eventi ritenuti di interesse per la prevenzione di determinati reati presupposto.

Riprendendo la casistica d'uso pocanzi delineata, si pensi al sistema informatico per la presentazione delle domande di partecipazione a gare pubbliche[117]. L'ente che gestisce la piattaforma può utilizzare un SIEM per raccogliere i dati di traffico e registrare i log delle utenze dotate dei diritti amministrativi. Saranno così segnalati eventi che, sulla base delle istruzioni fornite, presentino indici di anomalia: tentativi ripetuti di accesso, attività in orari non abituali, autenticazione con account mai utilizzati in una determinata *workstation* etc. Per arricchire ulteriormente le informazioni ricavate dai log, esiste la possibilità di integrare i dati di traffico con sistemi di *Data Classification* e *Data Loss Prevention*[118]. La classifica dovrà tener conto degli esiti della valutazione dei rischi e attribuire particolare valore ai dati che presentano collegamenti più stretti con i reati presupposto indicati dal modello 231. Nel caso esemplificato, il sistema potrà "etichettare" in automatico i dati relativi ai pagamenti e quelli relativi alle offerte tecniche presentate per la fornitura di servizi informatici[119], avvisando i responsabili delle funzioni di controllo in caso di attività anomale. Ciò consente di prevenire efficacemente accessi abusivi e frodi informatiche commessi a vantaggio dell'ente nei processi ritenuti a più alto rischio.

[115] Gli avvisi sono recapitati tramite la dashboard del programma oppure utilizzando servizi di posta elettronica o telefonia.

[116] Così, ad esempio, sarà attribuito un punteggio di rischio elevato alle connessioni che provengono da un IP straniero sconosciuto che, nell'arco di pochi minuti, ha inoltrato decine di richieste di accesso. Parimenti, l'indice di rischio sarà via via più elevato se a cadenza periodica l'IP sospetto continua a tentare accessi ai server aziendali.

[117] Si veda § 3.1.

[118] Per *Data Classification* si intende quel processo volto a individuare i dati sensibili all'interno di un database, al fine di determinare i controlli di sicurezza necessari in base all'importanza delle informazioni. I sistemi di *Data Classification* effettuano ricerche testuali complesse (frasi, composti di parole e vocaboli polisenso) grazie ad algoritmi di NPL, indicizzando i dati sensibili in base ai risultati della *query*. La *Data Loss Prevention* indica quei sistemi che identificano e proteggono i dati aziendali (in uso o archiviati), al fine di prevenire l'uso non autorizzato e la trasmissione di informazioni riservate.

[119] I sistemi di classifica del dato sono basati su elementi testuali "inequivocabili" riconosciuti come sensibili a livello aziendale. Così, nel caso addotto ad esempio, una coordinata IBAN o le specifiche tecniche di un software presentano alcuni elementi semantici distinguibili dalla mole di dati presenti nella piattaforma.

4.3. *Domini aziendali e flusso di comunicazioni.*

Il SIEM non consente di vagliare il contenuto delle comunicazioni informatiche, ma soltanto di analizzare il traffico di rete che transita per i server aziendali. Per questo motivo esso non è in grado, ad esempio, di monitorare il contenuto delle e-mail scambiate all'interno dell'organizzazione[120]. Il controllo sui messaggi di posta rappresenta un efficace strumento di prevenzione, specialmente nei casi in cui l'*iter criminis* si articoli in più fasi e richieda una previa concertazione tra il personale aziendale. Astrattamente lo si potrà impiegare per qualsiasi processo a rischio di reato, purché vi siano degli elementi testuali inequivocabili – o quantomeno discriminanti – che lascino presagire l'imminente commissione di un reato. A tal fine si dovranno stabilire regole rigide sui processi comunicativi all'interno dell'azienda, privilegiando l'utilizzo della posta aziendale per tutte le comunicazioni lavorative in luogo degli account personali.

Dal punto di vista tecnico il monitoraggio è eseguito grazie ad algoritmi di NPL[121] che, una volta impostati e collegati con la casella gestita dal *service provider* di posta[122], sono in grado di "comprendere" il significato dei messaggi e segnalare eventuali contenuti sospetti. Ciò permette di irrobustire i processi di controllo, facilitando l'emersione di condotte illecite e l'invio di segnalazioni tempestive ai responsabili di funzione.

Alcuni prodotti utilizzano l'intelligenza artificiale per ottenere metriche e attribuire un punteggio di rischio ai messaggi scambiati all'interno dell'azienda, in modo da indirizzare il controllo umano verso le comunicazioni ritenute più pericolose. Il grado di affidabilità dell'*output* dipende dalle istruzioni di partenza e dal peso attribuito ai diversi fattori. Di regola gli algoritmi sono impostati per associazioni semantiche di parole o di altri elementi del messaggio[123], e funzionano in modo dinamico. L'indice di rischio non è legato al messaggio in sé, ma tiene conto delle possibili attività sospette rilevate nei giorni precedenti[124]. Il segnale di *alert* sarà generato soltanto laddove la valutazione algoritmica superi una certa soglia, predeterminata in base alle specifiche esigenze e al contesto in cui il software è impiegato.

Nonostante i numerosi vantaggi, devono essere considerati anche gli aspetti critici relativi alla riservatezza di alcune comunicazioni aziendali e alla *privacy* degli individui[125]. Il monitoraggio attivo delle mail rischia di sovvertire gli schemi di *governance* della società, in quanto anche i messaggi più delicati sulla gestione dell'impresa (es. una conversazione tra amministratori) potrebbero astrattamente essere "intercettati", con conseguente alterazione gli equilibri societari e del delicato rapporto tra organi di amministrazione e funzioni di controllo. Per non considerare quelle comunicazioni che, per loro natura, devono restare strettamente segrete per evitare che altri all'interno dell'azienda possano trovare occasione per commettere un reato (si pensi alla circolazione di informazioni privilegiate, quanto alla responsabilità *ex* art. 25-*sexies* D. Lgs. 231/2001). Trattandosi di un rischio concreto, si è dell'avviso che l'ambito di applicazione dei sistemi in esame dovrebbe essere circoscritto ai soli processi a più alto rischio[126], previa adozione delle cautele necessarie per impedire che si addivenga a forme di controllo generalizzato[127].

Venendo al secondo aspetto, si dovrà chiarire se il monitoraggio del traffico di mail possa ritenersi legittimo in base al diritto vigente. Circa il controllo a distanza dell'attività dei lavoratori la giurisprudenza più recente ha chiarito che l'art. 171 D. Lgs. 196/2003 non è

[120] Si vedano al riguardo i casi d'uso individuati in precedenza v. §3.1. lett. a) e lett. c); § 3.2. lett. a)
[121] Sul *Natural Language Processing* v. *supra* §4.1.
[122] Alcuni applicativi dialogano direttamente con il gestionale di posta elettronica attraverso interfacce di programmazione; altri invece leggono il contenuto delle mail archiviate in un database. In entrambi i casi l'elaborazione dei dati avviene in tempo reale, così da generare immediatamente *alert* in caso di anomalie.
[123] Ad esempio, nel caso esemplificato, vocaboli afferenti a "denaro" o "pagamenti" rispetto all'indirizzo del destinatario del messaggio (riconosciuto come istituzionale) o alle parole "Comune", "funzionario" etc.
[124] Così, nel caso in cui vi sia stato uno scambio tra colleghi per discutere dell'impugnazione di un provvedimento negativo di aggiudicazione, il sistema attribuirà al messaggio un profilo di rischio basso. Il punteggio diventerà via via più alto se nei giorni successivi un apicale dovesse scrivere alla Stazione appaltante parlando di denaro o altri vantaggi economici.
[125] Per un approfondimento del tema in chiave giuslavoristica v. Alagna (2018), p. 339 ss.
[126] Sarebbe opportuno limitare il monitoraggio del traffico di mail a uno o più indirizzi (dedicati alla gestione di determinati affari) in relazione alla tipologia di reato che si vuole prevenire.
[127] L'ente dovrà dotarsi di discipline specifiche (codici di condotta, istruzioni operative, accordi di riservatezza) per garantire che l'accesso al software sia dato al solo personale incaricato e nei limiti delle funzioni attribuite. Salvi gli obblighi di comunicazione previsti dal modello (es. flussi informativi all'organismo di vigilanza), le informazioni apprese nell'esercizio di tali funzioni dovrebbero essere considerate riservate e soggette a cancellazione dopo un tempo massimo di *retention*.

configurabile[128] laddove la sorveglianza – anche in assenza di accordo sindacale *ex* art. 4 L. 300/1970 o di autorizzazione dell'Ispettorato del lavoro[129] – sia strettamente funzionale alla tutela dell'azienda e non si declini in un «*significativo controllo sull'ordinario svolgimento dell'attività lavorativa*»[130], e il sistema sia riservato all'accertamento di gravi condotte illecite dei dipendenti. La pronuncia richiama l'orientamento della Corte di Strasburgo secondo cui tali forme di sorveglianza sono legittime purché vi sia il rischio di commissione di illeciti da parte dei dipendenti, i controlli siano limitati allo scopo di impedire i reati, e lo strumento sia proporzionato[131]. Si è dell'avviso che la facoltà riconosciuta al datore di lavoro di effettuare controlli difensivi renda pienamente legittima, alle condizioni previste dalla legge, anche la sorveglianza attiva nei processi a rischio di reato. Trattandosi di controlli finalizzati a prevenire la commissione di illeciti e di evitare conseguenze negative per l'impresa, appare irrilevante la finalità soggettiva perseguita dall'agente (danno per la società o interesse dell'ente).

Il monitoraggio delle mail pone anche l'ulteriore questione della violazione del c.d. domicilio informatico del lavoratore. Alcune pronunce hanno ritenuto configurabile il reato di cui all'art. 615-*ter* c.p. nel caso di accesso abusivo alla posta elettronica del dipendente[132]; ma si trattava di casi in cui l'agente aveva utilizzato senza consenso la password per introdursi in una area riservata personale.

Quando la casella di posta è gestita direttamente dell'organizzazione, le mail in entrata e in uscita transitano – e risultano visibili – agli indirizzi aziendali dotati di particolari privilegi. Si pensi ad esempio all'account di segreteria che, per ragioni connesse all'organizzazione del lavoro, può visualizzare tutti i messaggi di posta scambiati dai membri dell'organizzazione. Per quanto la casella di posta di ciascun utente sia protetta da password, al gestore del dominio aziendale è attribuito *by design* il potere di amministrare tutti gli *account* collegati e di supervisionare il contenuto dei messaggi. Ciò pare sufficiente a ritenere legittimo l'utilizzo di software che, analizzando il traffico di mail aziendali, supportino le funzioni di controllo e prevenzione di reati. L'affermazione trova conforto anche nella giurisprudenza della Corte EDU che – pronunciandosi in un caso riguardante i controlli del datore di lavoro sulle e-mail inviate e ricevute dai dipendenti tramite l'account di posta aziendale[133] – ha ritenuto insussistente la violazione dell'art. 8 della Convenzione, purché l'ordinamento nazionale preveda misure e garanzie per evitare abusi.

Infine, per quel che riguarda i dati personali dei destinatari dei messaggi, esterni all'impresa, si ritiene le operazioni di trattamento siano legittime perché effettuate nel perseguimento del legittimo interesse dell'impresa (art. 6 GDPR). I terzi – di fatto consapevoli di corrispondere con un indirizzo gestito dall'azienda – non potranno vantare una illimitata aspettativa di *privacy*, potendo ben prefigurarsi che i messaggi siano gestiti in modo centralizzato dall'azienda (es. attraverso l'inoltro automatico a altre caselle di posta in caso di assenza del lavoratore) o soggetti a controlli di vario tipo. Sarebbe comunque opportuno, per dovere di trasparenza, che le *policy* aziendali imponessero di inserire una informativa preimpostata in calce alle mail, al fine di avvisare i terzi che l'*account* con cui interagiscono è gestito direttamente dall'ente e che

[128] La disposizione, come modificata dal D. Lgs. 101/2018, prevede che per le violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori prevede che si applichino le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300 (arresto o ammenda, contravvenzione oblabile *ex* art. 162-*bis* c.p.).

[129] L'art. 23 del D. Lgs. 151/2015 (c.d. *Jobs Act*) è intervenuto sull'art. 4 dello Statuto dei lavoratori, aggiungendo, accanto agli impianti audiovisivi, il riferimento ad altri strumenti «*dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori*». Il secondo comma precisa che l'accordo sindacale non è necessario per gli strumenti «*utilizzati dal lavoratore per rendere la prestazione lavorativa*». Alla luce della novella è si dovrà chiarire se il tracciamento nell'uso della rete aziendale ricada nell'ambito applicativo del primo ovvero del secondo comma dell'art. 4.

[130] Cass. Pen., Sez. III, 14 dicembre 2020, n. 3255 in *Sistema Penale*, 16 febbraio 2021, con nota di Birritteri (2021).

[131] Corte EDU, Grande Camera, Lopez Ribalda e altri c. Spagna, 17 ottobre 2019, in *Rivista Labor,* 22 novembre 2019, con traduzione di F. Perrone.

[132] Si veda, anche per più ampi richiami giurisprudenziali, Cass. Sez. V Pen. 31 marzo 2016, n. 13057 secondo cui la casella di posta «*non è altro che uno spazio di memoria di un sistema informatico destinato alla memorizzazione di messaggi, o informazioni di altra natura (immagini, video, ecc.), di un soggetto identificato da un account registrato presso un provider del servizio. E l'accesso a questo "spazio di memoria" concreta, chiaramente, un accesso al sistema informatico, giacche' la casella non e' altro che una porzione della complessa apparecchiatura – fisica e astratta destinata alla memorizzazione delle informazioni. Allorche' questa porzione di memoria sia protetta – come nella specie, mediante l'apposizione di una password – in modo tale da rivelare la chiara volontà dell'utente di farne uno spazio a se' riservato ogni accesso abusivo allo stesso concreta l'elemento materiale del reato di cui all'articolo 615/ter cod. pen.*».

[133] Corte EDU, Grande Camera, Barbulescu c. Romania, 5 settembre 2017 «*[…] the Court takes the view that the Contracting States must be granted a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer may regulate electronic or other communications of a non-professional nature by its employees in the workplace. Nevertheless, the discretion enjoyed by States in this field cannot be unlimited. The domestic authorities should ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, is accompanied by adequate and sufficient safeguards against abuse*» (§ 119, 120).

i messaggi scambiati potrebbero essere letti anche da personale diverso rispetto al destinatario.

5. Conclusioni.

La disamina sulle potenzialità offerte dalle *smart technologies* permette di giungere alla conclusione che, nella moderna società dell'informazione, esse sono uno strumento fondamentale di supporto alla *compliance* aziendale.

La tecnologia migliora la *performance* dei sistemi di gestione, automatizzando parte dei compiti attribuiti alle funzioni di controllo e riducendo i rischi operativi associati all'agire umano. Inoltre permette al personale incaricato di agire in modo informato basandosi sui dati raccolti e processati dagli algoritmi. Diverse applicazioni tecnologiche – quali il *machine learning*, la crittografia, l'analisi di *Big Data* – rendono disponibili informazioni pertinenti e specifiche sulle attività della società, che in nessun altro modo sarebbe possibile ottenere.

Dal punto di vista dei principi generali della responsabilità dell'ente, si è dell'avviso che la *digital compliance* sia un fattore positivo nella valutazione del modello organizzativo e gestionale adottato *ex* artt. 6 e 7 D. Lgs. 231/2001, potendo contribuire a rafforzare l'apparato di regole in chiave preventiva.

Peraltro, il supporto offerto da tali strumenti si andrà progressivamente affermando a livello internazionale come *best practice* in vari settori, fungendo da criterio guida per una efficace gestione del rischio. A tal riguardo, è da accogliere con favore la tesi di una maggiore positivizzazione delle regole cautelari per gli enti mediante un sistema che, valorizzando le *best practices* di settore, introduca una presunzione relativa di idoneità del modello[134].

Tuttavia, affinché il percorso di automazione della *compliance* sia sicuro e sostenibile, si dovrà svolgere una accurata analisi del caso concreto, valutando i possibili rischi derivanti dall'applicazione di certe tecnologie (es. l'intelligenza artificiale, con il suo alto grado di opacità). L'ente dovrà inoltre avere cura di definire il ruolo del personale "umano" nelle attività "digitalizzate", supervisionando in modo critico e costruttivo le determinazioni dell'algoritmo.

Tra le innovazioni tecnologiche sopra esaminate, certamente i programmi di *decision intelligence* su fonti aperte assumono particolare rilevanza per la semplicità con cui possono essere acquisiti e integrati nei processi aziendali. Gli enti potranno prevedere, nei propri modelli organizzativi, che il compimento di determinate operazioni a rischio di reato sia preceduto da una specifica *due diligence* mediante OSINT, o che situazioni particolari siano "monitorate" in tempo reale dall'algoritmo. Ciò consentirà di elaborare report e generare *alert* per responsabili di funzione circa eventuali rischi nella relazione con terze parti. Tali strumenti presentano anche il pregio di una piena conformità con la normativa in materia di *privacy*, laddove non siano utilizzati per la profilazione o per finalità non consentite.

Anche i SIEM e gli strumenti per il monitoraggio del traffico di dati (e delle mail) all'interno all'azienda si rivelano di grande utilità per prevenire la commissione di alcuni *corporate crimes*. Tuttavia, affinché tali software possano assolvere adeguatamente al compito di supportare la *compliance*, l'ente dovrà adattarli e/o customizzarli sulla base delle proprie esigenze. Si profilano, inoltre, alcuni rischi per la *privacy* dei lavoratori che, sebbene non ostativi al monitoraggio dei dati, dovrebbero richiedere quantomeno un'analisi di impatto preventivo.

In definitiva, la trasformazione digitale è un processo inarrestabile che investe, anzi deve investire, anche i modelli organizzativi e gestionali 231. Il sistema di *governance* e di controlli non può restare ancorato a logiche tradizionali, ma deve evolvere di pari passo rispetto alle nuove modalità di comunicazione e lavoro.

Bibliografia

Alagna, Ilenia Maria (2018): "Big data e People Analytics: nuove sfide e opportunità per liberare valore", *Ciberspazio e diritto*, 2018, vol. 19, p. 339 ss.

[134] *Amplius*, § 1.1

Ammannati Laura e Greco Gian Luca (2021): "Piattaforme digitali, algoritmi e "big data": il caso del "credit scoring", *Rivista Trimestrale di Diritto dell'Economia*, 2, p. 290 ss.

Armour, John (2018): The Case for "Forward Compliance", *The British Academy Review*, 1 november 2018, in www.thebritishacademy.ac.uk

Arner, Douglas W, Barberis Janos, e Buckley Ross (2017): "FinTech, RegTech and the Reconceptualization of Financial Regulation", *Northwestern Journal of International Law & Business*, vol. 37, 3, p. 373

Bamberger, Kenneth A. (2009): "Technologies of Compliance: Risk and Regulation in a Digital Age", *Texas Law Review*, vol. 88, p. 669 ss.

Baskerville, Richard, Spagnoletti, Paolo e Kim, Jongwoo (2014): "Incident-centered information security: Managing a strategic balance between prevention and response", *Information & Management*, vol. 51, 1, p. 138 ss.

Bennett Moses, Lyria e Chan, Janet (2018): "Algorithmic prediction in policing: assumptions, evaluation, and accountability", *Policing and Society,* vol. 28, 7, p. 806 ss.

Bianchini, Francesco (2007): "L'IA e il linguaggio fra storia ed epistemologia", in Bianchini, Francesco, Gliozzo, Alfio, e Matteuzzi Maurizio (editor), *Instrumentum vocale: intelligenza artificiale e linguaggio*, Bologna

Birritteri, Emanuele (2019): "Big Data Analytics e compliance anticorruzione. Profili problematici delle attuali prassi applicative e scenari futuri", *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2, p. 294 ss.

Birritteri, Emanuele (2020): "Controllo a distanza del lavoratore e rischio penale", nota a Cass. Pen., Sez. III, 14 dicembre 2020, n. 3255, *Sistema Penale*, 16 febbraio 2021

Basile, Fabio (2019): "Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine", *Diritto Penale Uomo*, 29 settembre 2019

Borsari, Riccardo (2020): "Intelligenza Artificiale e responsabilità penale: prime considerazioni", *Discrimen,* 14 febbraio 2020

Burchard, Christoph (2021): "Digital Criminal Compliance", in Engelhart, Marc, Kudlich, Hans, und Vogel, Benjamin (editor), *Digitalisierung, Globalisierung und Risikoprävention. Festschrift für Ulrich Sieber*, Berlin, p. 741

Burchard, Christoph (2019a): "Künstliche Intelligenz als Ende des Strafrechts? Zur algorithmischen Transformation der Gesellschaft" , *Normative Orders Working Paper*, in www.publikationen.ub.uni-frankfurt.de

Burchard, Christoph (2019b): "L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società", *Rivista italiana di diritto e procedura penale*, 4, p. 1909 ss.

Consulich, Federico (2018), "Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato", *Banca, borsa e titoli di credito,* 2, p. 195 ss.

D'Agostino, Luca (2019): "Gli algoritmi predittivi per la commisurazione della pena. A proposito dell'esperienza statunitense nel c.d. evidence-based sentencing", *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2, p. 354 ss.

Dombalagian, Onnig H. (2016): "Preserving Human Agency in Automated Human Compliance, in Tulane University School of Law Public Law and Legal Theory", *Working Paper Series Working Paper n. 11/2016,* in brooklynworks.brooklaw.edu

Diamantis, Mihailis E. (2020): "The Extended Corporate Mind: When Corporations Use AI to Break the Law", *North Carolina Law Review,* vol. 98, 4, p. 893 ss.

Ferguson, Andrew Guthrie (2015): "Big Data and predictive reasonable suspicion", *University of Pennsylvania Law Review*, Vol. 163, p. 327;

Franssen, Vanessa, and Berrendorf, Alyson (2021): "The Use of AI Tools in Criminal Courts: Justice Done and Seen to Be Done?", *Revue Internationale de Droit Pénal,* vol. 92, 1, p. 199 ss.

Gambino, Alberto Maria, e Bomprezzi, Chantal (2019): "Blockchain e protezione dei dati personali", *Diritto dell'informazione e dell'informatica,* 3, p. 623

Gialuz, Mitja (2019): "Quando la giustizia penale incontra l'Intelligenza Artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa", *Diritto penale contemporaneo,* 29 maggio 2019

Gillespie, Tarleton (2014): "The Relevance of Algorithms", in Gillespie, Tarleton, and Boczkowski, Pablo J. (editor), *Media Technologies: Essays on Communication, Materiality, and Society,* MIT Press, p. 167 ss.

Gullo, Antonio (2022): "Compliance", in Piergallini, Carlo, Mannozzi, Grazia, Perini, Chiara, Scoletta, Marco, Sotis, Carlo, e Consulich Federico, (editor), *Studi in onore di Carlo Enrico Paliero*, Milano, p.1289 ss.

Gullo, Antonio (2020): "I modelli organizzativi", in Lattanzi, Giorgio, e Severino, Paola (editor), *Responsabilità da reato degli enti,* vol. I, *Diritto sostanziale*, Torino, p. 283 ss.

Kehl, Danielle, Guo, Priscilla, and Kessler, Samuel (2017): "Algorithms in the Criminal Justice System: Assessing the use of Risk Assessments in Sentencing", *Responsive Communities Initiative, Berkman Klein Center for Internet and Society, Harvard Law School*, in dash.harvard.edu

King, Thomas, Aggarwal, Nikita, Taddeo, Mariarosaria, and Floridi, Luciano (2020): "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions", *Science and Engineering Ethics,* 26, p. 89-120

Laufer, William S. (2017): "The missing account of progressive corporate criminal law", *New York Journal of Law and Business*", vol. 14, 1, p. 71 ss.

Laura, Luigi (2019): *Breve e universale storia degli algoritmi*, Luiss University Press

Liptak, Adam (2017): "Sent to prison by a Software Program's secret algorithms", *New York Times*, May 1st 2017

Lo Sapio, Germana (2021): "Rating reputazionale, consenso valido e comprensione dell'algoritmo alle prese con l'era digitale", *Federalismi.it*, 11 agosto 2021, nota a Cass. Civ., Sez. I, 25 maggio 2021 n. 14381

Manes, Vittorio (2020): "L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia", *Discrimen,* 15 maggio 2020

Massaro, Alessandro, Icardi, Simone, e Mele, Fabio: (2017): "La Social Media Intelligence nell'era dei social network", *Ciberspazio e diritto,* 2, p. 425 ss.

Mazzacuva, Francesco (2021): "The Impact of AI on Corporate Criminal Liability: Algorithmic Misconduct in the Prism of Derivative and Holistic Theories", *Revue Internationale de Droit Pénal,* vol. 92, 1, p. 143 ss.

Maugeri, Anna Maria (2021): "L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali", *Archivio Penale,*1, p. 2 ss.

Minneci, Ugo, Ammannati, Laura, Canepa, Allegra, e Greco, Gianluca (2021): *Algoritmi, Big Data, piattaforme digitali. La regolazione dei mercati in trasformazione,* Giappichelli

Mohamed, Hazik, and Yildirim, Ramazan (2021): "RegTech and Regulatory Change Management for Financial Institutions", in Hamdan, Allan, Hassanien, Aboul Ella, and Razzaque, Anjum (editor), *The Fourth Industrial Revolution: Implementation of Artificial Intelligence for Growing Business Success*, Studies in Computational Intelligence, p. 153 ss.

Mongillo, Vincenzo (2011): "Il giudizio di idoneità del Modello di Organizzazione ex d.lgs. 231/2001: incertezza dei parametri di riferimento e prospettive di soluzione", *La responsabilità amministrativa delle società e degli enti*, 3, p. 75 ss.

Mongillo, Vincenzo (2022): "Presente e futuro della compliance penale", *Sistema Penale,* 11 gennaio 2022

Morgante, Gaetana, e Fiorinelli, Gaia (2022): "Promesse e rischi della compliance penale digitalizzata", *Archivio Penale Web,* 2

Mozzarelli, Michele Cesare Maria (2022): "Digital Compliance: The Case for Algorithmic Transparency", in Centonze, Francesco, e Manacorda, Stefano (editor), *Corporate Compliance on a Global Scale. Legitimacy and Effectiveness,* Springer

Niklas, Jędrzej (2020): "Human Rights-Based Approach to AI and Algorithms", in Barfield Woodrow (editor), *The Law of Algorithms*, p. 527 ss.

Nisco, Attilio (2022): "Riflessi della compliance digitale in ambito 231", *Sistema Penale*, 14 marzo 2022

Oswald, Marion, Grace, Jamie, Urwin, Sheena, and Barnes, Geoffrey (2018): "Algorithmic risk assessment policing models: lessons from the Durham HART model and "Experimental" proportionality", *Information and Communications Technology Law*, p. 227

Packin, Nizan Geslevich (2018): "RegTech, Compliance and Technology Judgment Rule", *Chicago Kent Law Review*, vol. 93, 1, p. 193-218

Paolucci, Federica (2021): "Consenso, intelligenza artificiale e privacy", *Media Laws*, 16 giugno 2021, con nota a Cass. Civ., Sez. I, 25 maggio 2021 n. 14381

Paliero, Carlo Enrico (2018): "La colpa di organizzazione tra responsabilità collettiva e responsabilità individuale", *Rivista trimestrale di diritto penale dell'economia*, 1-2, p. 175 ss.

Piergallini, Carlo (2015): "Autonormazione e controllo penale", *Diritto penale e processo*, 3, p. 266 ss.

Piergallini, Carlo (2019): "Premialità e non punibilità nel sistema della responsabilità degli enti", *Diritto penale e processo,* 4, p. 530 ss.

Piselli, Riccardo, e D'Agostino, Luca (2019): "La definizione di tecnologia a registro distribuito e di smart contract nella legge di conversione del "Decreto semplificazioni". Un primo commento critico", in Nuzzo, Antonio (editor), *Blockchain e autonomia privata – Fondamenti giuridici,* Luiss University Press, 2019, p. 13-22

Sabia, Rossella (2020): "Artificial Intelligence and Environmental Criminal Compliance", *Revue Internationale de Droit Pénal*, 1, p. 179 ss.

Sagliocca, Antonio (2017): "Open Source Intelligence e Deep Web: scenari moderni delle investigazioni digitali", *Ciberspazio e diritto*, 1, p. 171 ss.

Sciascia, Giuseppe (2021): "Reputazione e potere: il social scoring tra distopia e realtà", *Giornale di diritto amministrativo*, 3, p. 317 ss.

Searle, John R. (1980): "Minds, brains, and programs", *Behavioral and Brain Sciences*, 3, p. 417-457

Selvaggi, Nicola (2019): "Dimensione tecnologica e compliance penale: un'introduzione", in Lupària, Luca, Marafioti, Luca, e Paolozzi, Giovanni, (editor), *Dimensione tecnologica e prova penale,* Giappichelli, p. 217 ss.

Severino, Paola (2020): "Intelligenza artificiale e diritto penale", in Ruffolo, Ugo (editor), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, p. 531 ss.

Sorbello, Pietro (2019): "Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto", *Diritto penale contemporaneo – Rivista trimestrale,* 2, p. 374 ss.

Starr, Sonja B. (2014): "Evidence -based Sentencing and the Scientific Rationalization of Discrimination", *Stanford Law Review*, vol. 66, p. 809 ss.

Trezza, Remo (2021): "L'Intelligenza Artificiale come ausilio alla standardizzazione del modello 231: vantaggi possibili e rischi celati", *Giurisprudenza Penale*, 1-*bis,* 2 ss.

Ubertis, Giulio (2020): "Intelligenza artificiale, giustizia penale, controllo umano significativo", *Diritto penale contemporaneo – Rivista trimestrale*, 4, p. 75 ss.

Van Liebergen, Bart (2016): "RegTech in financial services: technology solutions for compliance and reporting", 22th march 2016, *Institute of International Finance Publications*, in www.iif.com

Vermeulen, Gert, Peršak, Nina, e Recchia, Nicola (2021): "Capabilities and limitations of ai in criminal justice", *Revue Internationale de Droit Pénal,* vol. 92, 1, p. 7 ss.

Zuboff, Shoshana (2019), *Il capitalismo della sorveglianza,* Luiss University Press (trad. Paolo Bassotti)

La responsabilità penale del produttore di sistemi di intelligenza artificiale*

La responsabilidad penal del fabricante de sistemas de inteligencia artificial

The Criminal Liability of Artificial Intelligence System Manufacturers

Beatrice Fragasso
Dottoressa di ricerca in Diritto penale
beatrice.fragasso@unimi.it

Intelligenza artificiale, Nesso causale, Colpa

Inteligencia artificial, Nexo causal, Culpa

Artificial Intelligence, Causation, Negligence

Abstracts

Il contributo esamina i problemi ascrittivi della responsabilità penale in capo al produttore di sistemi di intelligenza artificiale (i.a.), per gli eventi lesivi derivanti dall'impiego di questi ultimi. L'obiettivo è di verificare se i tradizionali regimi di responsabilità penale – che hanno come presupposto la commissione di fatti penalmente rilevanti da parte di persone fisiche – siano adeguati al nuovo contesto tecnologico, in cui algoritmi caratterizzati da autonomia, interattività e opacità possono porre in essere condotte imprevedibili per gli stessi produttori.
Da un lato, l'interposizione dell'imperscrutabile decision making algoritmico tra la condotta del produttore e l'evento lesivo rende problematico l'accertamento del nesso di causalità, stante l'assenza, attualmente, di leggi scientifiche di copertura in grado di spiegare il comportamento dei dispositivi intelligenti. Dall'altro lato, la crisi del modello nomologico-deduttivo sembrerebbe ripercuotersi, a cascata, sull'accertamento della colpa in capo al produttore, al quale soltanto con gravi forzature potrebbe essere rimproverato il verificarsi di un evento lesivo concretamente imprevedibile. Preso atto delle criticità applicative del tradizionale diritto penale d'evento, il contributo vaglierà, infine, l'opportunità di fare ricorso a tecniche di anticipazione della tutela penale.

El artículo examina los problemas de atribución de responsabilidad penal al fabricante de sistemas de inteligencia artificial (IA) por los daños resultantes de su uso. El objetivo es determinar si los regímenes tradicionales de responsabilidad penal, que se basan en la comisión de conductas punibles por parte de personas físicas, son adecuados para el nuevo contexto tecnológico, en que algoritmos caracterizados por su autonomía, interactividad y opacidad, pueden llevar a cabo conductas impredecibles incluso para los propios fabricantes. Por un lado, la interposición de procesos de toma de decisión algorítmicos, muchas veces inescrutables, entre la conducta del fabricante y el daño dificulta el establecimiento de la relación de causalidad, dado que actualmente no existen leyes científicas que expliquen el comportamiento de los dispositivos inteligentes. Por otro lado, la crisis del modelo nomológico-deductivo parece repercutir, en cascada, en la determinación de la culpabilidad del fabricante, pues dicho modelo solamente podría aceptar la imputación de un resultado lesivo imprevisible a través de interpretaciones forzadas. Dado el reconocimiento de las dificultades de aplicación del derecho penal tradicional basado en el resultado, el artículo evaluará, finalmente, la oportunidad de recurrir a técnicas de anticipación de la protección penal.

*Testo, rivisto e corredato di note, della relazione tenuta al Corso "Intelligenza artificiale, diritto e processo" organizzato dalla Scuola Superiore della Magistratura e dalla Fondazione Vittorio Occorsio (Napoli, 20-22 marzo 2023).

The article aims to address the issue of criminal liability for manufacturers in relation to harms caused by Artificial Intelligence systems (hereinafter 'AI systems'). Such incidents can challenge existing liability frameworks that are based on human actions. As AI systems become more autonomous and capable of learning new skills and adapting to their environment, they may act in ways that the designers and developers cannot anticipate. The involvement of the manufacturer in the inscrutable algorithmic decision-making (referred to as the 'black box') raises concerns about establishing causation since there is no scientific understanding of how AI systems behave. Additionally, the culpability of the producer and user is a matter of debate. While the general unpredictability of AI systems may be foreseeable, establishing criminal negligence would require foreseeability of the specific harm that occurs in each individual case. Due to the challenges associated with assigning criminal liability for AI-related harms, this article concludes by exploring the potential introduction of new negligence offenses focusing on the improper design, operation, and testing of AI applications.

Sommario

1. Premessa.

Il cambiamento che l'intelligenza artificiale (d'ora in avanti, i.a.) sta portando nelle nostre vite è epocale. Già oggi, molti sistemi di i.a. hanno dimostrato di essere più accurati, nello svolgere le attività loro delegate, degli esseri umani: si pensi, ad esempio, all'attività di riconoscimento biometrico, che i sistemi di i.a. sono in grado di svolgere in modo più efficace (oltre che rapido) rispetto agli esseri umani[1]; si pensi, ancora, alle *self driving cars*, che, secondo alcune stime, se adottate da gran parte degli utenti della strada, potrebbero ridurre del 90% gli incidenti stradali[2] – oltre che liberare uomini e donne da un'attività spesso percepita come noiosa e stressante. Se la diffusione dell'intelligenza artificiale in ogni aspetto della vita quotidiana promette di arrecare grandi benefici alla società, essa, tuttavia, apre anche una serie di interrogativi sul piano politico, etico, economico, e, per quanto qui interessa, giuridico.

La questione, per quanto concerne i profili strettamente penalistici, può essere riassunta in poche battute: la (parziale) perdita di controllo dell'operatore umano (dell'utilizzatore, così come del produttore, del programmatore, dello sviluppatore, etc.) sul processo decisionale e sul comportamento dell'algoritmo potrebbe scardinare i classici meccanismi imputativi del diritto penale, comportando un'attenuazione, se non un totale annullamento, delle istanze punitive.

Chi risponde, allora, se un veicolo a guida autonoma attraversa un incrocio con il semaforo rosso e investe un pedone, cagionandone la morte?[3] Sono individuabili dei soggetti personalmente responsabili per le notizie false fornite da Chat GPT[4] e per le manipolazioni del mercato realizzate da algoritmi di *trading* finanziario?[5]

Il diritto penale – fondato sul *mancato dominio*, da parte dell'agente, di un *fatto offensivo effettivamente dominabile*[6] – rischia di risultare inadeguato laddove tale *dominio* si venga a perdere e "autore" immediato del reato risulti essere proprio una macchina.

Il problema del c.d. *responsibility gap*[7] è avvertito anche dalle istituzioni europee, che in diverse occasioni – riferendosi, in realtà, soprattutto a profili civilistici, di responsabilità extracontrattuale – hanno evidenziato come i "comportamenti emergenti"[8] delle macchine "intelligenti" possano comportare un intollerabile vuoto di tutela nei confronti delle persone danneggiate. Già nel 2017, ad esempio, nella Risoluzione sul diritto civile e la robotica del Parlamento europeo (2015/2103(INL))[9], si poteva leggere, tra i considerando, che «più i robot sono autonomi, meno possono essere considerati come meri strumenti nelle mani di altri at-

[1] Vd. il report di ID R&D (2022).
[2] Vd. il report di McKinsey & Company (2015).
[3] Ci sono diversi *database online* che raccolgono e classificano gli incidenti che hanno coinvolto veicoli a guida autonoma; tra i più aggiornati vd. il sito *Autonomous Vehicle Crashes* (www.avcrashes.net), che dà anche la possibilità di visualizzare i dati attraverso una mappa interattiva. In data 2 maggio 2023, il sito contava 630 incidenti, realizzatisi tra il 14 ottobre 2014 e il primo maggio 2023.
[4] Come noto, ChatGPT è un modello di i.a. "generativo", liberamente accessibile *online*, che, attraverso algoritmi di apprendimento automatico, genera risposte agli *input* scritti forniti dall'utente. Già in diversi casi è stata riscontrata la comunicazione di notizie false da parte del sistema, vd. Cassens Weiss (2023); Khatsenkova, Huet (2023).
[5] Con l'espressione "*algorithmic trading*" ci si riferisce a sistemi informatici che sono in grado di effettuare autonomamente ordini di acquisto sulle piattaforme di *trading*: l'algoritmo decide la tempistica, il prezzo e la quantità dell'ordine; nella maggior parte dei casi, può addirittura avviare l'ordine in assenza di intervento umano. In diverse occasioni si sono già verificati fenomeni di improvvise turbative dei prezzi dei titoli finanziari, dovuti all'agire contestuale di "sciami" di algoritmi di *trading* (c.d. *Flash Crash*); in argomento vd. Scopino (2020); Consulich (2018a).
[6] Così Fiorella (1988), p. 1289.
[7] Di *responsibility gap* si è parlato, inizialmente, soprattutto in dottrina. Vd., in particolare, i lavori seminali di Matthias (2004); Sparrow (2007); Wallach, Allen (2009), p. 198 ss. Recentemente si vedano le acute riflessioni di Cappellini (2023).
[8] Sul concetto di "*emergent behaviors*" – utilizzato in letteratura per descrivere i comportamenti "autonomi" dei sistemi di i.a. – vd., per tutti, Calo (2015), p. 532 ss.
[9] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)).

tori (quali il fabbricante, l'operatore, il proprietario, l'utilizzatore, ecc.)»[10] e che l'attuale quadro giuridico potrebbe rivelarsi non idoneo «a coprire i danni causati dalla nuova generazione di robot, in quanto questi possono essere dotati di capacità di adattamento e di apprendimento che implicano un certo grado di imprevedibilità nel loro comportamento, dato che imparerebbero in modo autonomo, in base alle esperienze diversificate di ciascuno, e interagirebbero con l'ambiente in modo unico e imprevedibile»[11].

Posto che l'ipotesi – pur avanzata in dottrina – di una responsabilità penale diretta del dispositivo intelligente[12] non sembra condivisibile, a meno di non voler trasfigurare completamente i connotati del diritto penale[13], ci pare che la riflessione sui *reati da intelligenza artificiale* dovrebbe coinvolgere, da un lato, la sfera dell'utilizzatore del sistema di i.a., e, dall'altro, quella del "produttore". In questa sede, nell'attenerci al tema assegnatoci dagli organizzatori del Corso, ci concentreremo esclusivamente su quest'ultimo aspetto.

Premettiamo fin da ora che, per comodità espositiva, in questa relazione si farà sempre riferimento alla figura del "produttore", intendendo tuttavia includere, in tale espressione, tutte quelle persone che, a vario titolo, contribuiscono ai processi di *sviluppo, progettazione e commercializzazione* dei dispositivi intelligenti. Va da sé, ovviamente, che l'individuazione del soggetto personalmente responsabile – tra coloro che fanno parte del ciclo *lato sensu* produttivo – incontrerà difficoltà specifiche, determinate dal problematico accertamento: (*i*) della specifica *causa* dell'evento lesivo (es. difetto di programmazione o di addestramento o di installazione, etc.); (*ii*) della persona responsabile all'interno delle organizzazioni complesse.

1.1. *La necessità di una nozione "penalisticamente orientata" di intelligenza artificiale.*

Nell'ambito di questo Corso sono già ampiamente emerse le complessità del rapporto tra sistema penale e intelligenza artificiale. Concludiamo queste giornate con molti spunti di riflessione, ma quasi nessuna certezza – se non, forse, con una sola: che non esistono, ad oggi, definizioni unanimemente condivise di i.a. L'hanno sottolineato tutti i relatori e anche questo intervento partirà da qui.

Una definizione destinata ad avere importanti ripercussioni è sicuramente quella fornita dalla proposta di Regolamento sull'intelligenza artificiale presentata nel 2021 dalla Commissione Europea (c.d. *AI Act*)[14], che definisce il sistema di i.a. come «un *software* sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare *output* quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono» (art. 3, lett. a)[15]. Si tratta, com'è evidente, di una definizione molto ampia, e che per questo motivo è stata molto criticata in dottrina, poiché estende il campo di applicazione della proposta anche a sistemi che normalmente, oggi, non sono considerati come "intelligenti" e che spesso sono già in circolazione

[10] *Ibidem*, considerando AB.
[11] *Ibidem*, considerando AI.
[12] Il principale teorizzatore della possibile configurazione di una responsabilità penale diretta in capo ai sistemi di i.a. è il penalista israeliano Gabriel Hallevy, vd. Hallevy (2015); Hallevy (2010a); Hallevy (2010b); nello stesso senso, ma con accezioni spesso molto diverse tra loro, vd. Hu (2019); Mulligan (2018); Simmler, Markwalder (2019); LaGioia, Sartor (2020).
[13] Non è questa la sede per cercare di confutare, passaggio per passaggio, le argomentazioni proposte dai fautori della tesi della responsabilità penale diretta dei sistemi di i.a. Ci limitiamo qui a sottolineare che il principio di *personalità della responsabilità penale* (art. 27, co. 1, Cost.) pare un ostacolo insormontabile al riconoscimento di una responsabilità penale diretta del sistema intelligente, presupponendo una capacità di autodeterminazione dell'agente che, ad oggi, caratterizza esclusivamente gli esseri umani (seppure, anche in questo caso, soltanto come postulato epistemologico). Del pari, anche a voler riconoscere una "capacità criminale" in capo ai sistemi di i.a., non si vede quali sanzioni, applicate agli algoritmi, possano rispondere alle finalità classiche della pena (retribuzione; prevenzione generale e speciale). Per un'approfondita confutazione della tesi della responsabilità penale diretta delle macchine vd., per tutti, Cappellini (2018), p. 14 ss.; Piergallini (2020), p. 1766; Panattoni (2021), p. 345 ss.
[14] Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM/2021/206 final, 21 aprile 2021 (cd. *AI Act*)
[15] Gli Approcci indicati dall'allegato 1 sono: «a) Approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (*deep learning*); b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti; c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione».

da decenni[16].

Per il tema che qui ci proponiamo di indagare, emerge piuttosto la necessità di individuare una nozione "penalisticamente orientata" di intelligenza artificiale, che comprenda soltanto i sistemi che hanno caratteristiche *dirompenti* rispetto ai classici modelli di imputazione della responsabilità penale. Dovrebbero dunque essere esclusi dalle nostre prospettive di studio tutti quei sistemi che – essendo inquadrabili all'interno dei tradizionali schemi di *strumentalità* dell'oggetto rispetto all'agente umano – riproducono problematiche giuridiche note.

Il *cuore del problema* sembrerebbe consistere nell'*imprevedibilità* del comportamento di alcuni dispositivi intelligenti – caratteristica che, a sua volta, parrebbe derivare da tre proprietà che si riscontrano nei più sofisticati sistemi di i.a., l'*autonomia*, l'*interattività*, l'*opacità*:

(i) *autonomia* – è la caratteristica, evidenziata dalla gran parte della dottrina che si è occupata del tema[17], che rischia di scardinare i meccanismi classici di imputazione della responsabilità penale. Si tratta di un concetto che dev'essere inteso in senso restrittivo: non nell'accezione kantiana di *capacità morale di auto-governo della ragione*, ma, piuttosto, come *capacità di prendere decisioni in situazioni di incertezza* e di *compensare l'incompletezza delle informazioni ricevute in partenza attraverso l'apprendimento*;

(ii) *interattività* – gli algoritmi intelligenti spesso non agiscono come monadi, ma sono connessi tra loro e, talvolta, persino con l'ambiente fisico in cui si trovano (c.d. *internet of things*[18]). Da un lato, l'incontro tra due o più "autonomie" – nell'accezione anzidetta – può comportare *output* collettivi inaspettati (c.d. *collective machine behaviour*[19]), frutto di interazioni non sempre pienamente comprensibili dall'esterno; dall'altro, gli algoritmi connessi con sensori e infrastrutture fisiche complesse sono esposti ad una varietà infinita di *inputs*, risultando così non meno imprevedibili dell'ambiente con cui interagiscono[20];

(iii) *opacità* (c.d. *black box*) – gli algoritmi intelligenti non sono in grado di fornire una spiegazione teorica e causale dei risultati raggiunti, né i programmatori possono agevolmente intuirla. Per *black box* si intende l'imperscrutabilità dei meccanismi causali interni ai sistemi di i.a.: è possibile individuare *input* e *output*, ma non è invece possibile ricostruire *cosa accade* all'interno della scatola nera, ovverosia la catena causale che ha determinato il passaggio dagli *input* agli *output*[21]. Di *black box*, com'è noto, si parlava già con riferimento ai prodotti tradizionali[22]: in relazione ai più sofisticati sistemi di i.a., tuttavia, l'opacità sembrerebbe una caratteristica *intrinseca* e *ineliminabile*, derivante dalla discrepanza tra processo logico-computazionale probabilistico tipico dell'algoritmo e struttura causale e deduttiva propria del ragionamento umano.

I sistemi di i.a. che hanno le caratteristiche così descritte possono sostanzialmente essere ricondotti al *machine learning* – una tecnica, su cui torneremo a breve, che consente agli algoritmi di *apprendere* dall'esperienza e dall'ambiente circostante, modificando le proprie prestazioni nel corso del tempo[23]. Ci limitiamo qui a sottolineare che anche il Consiglio di Stato, in una pronuncia del 2021[24], ha adottato, seppur soltanto in un *obiter dictum*, una definizione restrittiva di intelligenza artificiale, limitata alle sole applicazioni di *machine learning*: nelle parole dei giudici amministrativi, l'i.a. è «un sistema che non si limita solo ad applicare le regole software e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico».

[16] Osborne (2021); Clarke (2021). Alcune fonti, in ogni caso, riportano che Consiglio e Commissione Europea si stiano accordando per restringere la definizione e limitare il campo di applicazione del Regolamento ai soli sistemi dotati di *machine learning*, vd. Kayser-Bril (2021).

[17] Vd., per tutti, Picotti (2022), p. 1032; Amidei (2019), p. 1717.

[18] Non esiste una definizione univoca di *internet of things*. L'ENISA (*European Union Agency for Cybersecurity*) lo definisce come «*a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making*»; lo European Research Cluster on the Internet of Things (IERC) lo definisce invece come «*a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network*».

[19] Rahwan e al. (2019), p. 482.

[20] Karnow (2016), p. 59; In generale, sull'interattività dei sistemi di i.a. vd. Beckers, Teubner (2022), p. 111 ss.

[21] Bathaee (2018), p. 905; Castelvecchi (2016).

[22] Vd. per tutti Stella (2003), p. 224-235; Piergallini (2004), p. 50 ss.

[23] Russell, Norvig (2020), p. 651.

[24] Cons. Stato, sez III, sent. 25 novembre 2021, n. 7891; in argomento vd. Paolucci (2022); Filicetti (2023).

2. I sistemi di *machine learning*: una tecnologia *unpredictable by design*.

Senza entrare in aspetti tecnici troppo specifici – che di certo non abbiamo le competenze per fornire e che sono già stati accuratamente delineati nelle sessioni precedenti –, ci limiteremo qui ad evidenziare brevemente alcune delle caratteristiche dei sistemi di *machine learning* che ne rendono problematico l'inquadramento all'interno delle categorie del diritto penale.

A differenza dei modelli simbolico-deduttivi di i.a. sviluppati a partire dalla metà del Novecento – che applicavano al caso concreto le regole astratte fornite in sede di programmazione[25] –, i sistemi di *machine learning* utilizzano un metodo induttivo (c.d. *bottom-up*) e probabilistico: osservano i dati forniti in sede di addestramento, riconoscono i *pattern* statistici sottostanti e ne traggono delle generalizzazioni[26].

Tale approccio parte dalla constatazione che molte delle attività che l'essere umano svolge non sono formalizzabili attraverso l'esplicitazione di regole definite, ma sono frutto di esperienza ed imitazione. Si pensi, ad esempio, al riconoscimento facciale: un'attività che svolgiamo senza difficoltà, in maniera intuitiva, ma per la quale sarebbe arduo stilare un elenco di regole precise che possano essere applicate, in via deduttiva, da una macchina. Se invece forniamo ad un algoritmo di *machine learning* una serie di immagini, indicando appositamente, attraverso un'etichetta (*label*), quali ritraggono Tizio e quali ritraggono Caio, il sistema ragionerà per analogia e, quando posto di fronte ad immagini non etichettate, sarà in grado di generalizzare quanto appreso in fase di addestramento, distinguendo il volto di Tizio da quello di Caio (c.d. apprendimento supervisionato o *supervised learning*)[27].

Un simile risultato sarebbe difficilmente raggiungibile attraverso l'approccio simbolico e "causale", che richiederebbe la definizione di un procedimento logico astratto, da applicare nel caso concreto. D'altra parte, lo stesso algoritmo non è in grado di formulare una *regola di classificazione* – che consenta *in tutti i casi*, in maniera infallibile, di etichettare le immagini – ma ragiona *per analogia*: il sistema non sa spiegare quali sono stati i criteri che, in un *database* contenente milioni di immagini, gli hanno consentito di individuare il viso di una determinata persona.

Così, se, da un lato, il *machine learning* consente agli algoritmi di individuare *pattern* ricorrenti che potrebbero non essere percepibili dall'uomo, dall'altro, il ragionamento analogico tipico dei sistemi di auto-apprendimento sconta una carenza assoluta di comprensione "semantica", che talvolta può determinare la commissione di errori che, ad uno sguardo umano, possono apparire come grossolani e macroscopici[28]. Può capitare, allora, che un sistema di riconoscimento di immagini basato sul *machine learning* scambi una tartaruga per un fucile[29]. Ancora, alcuni ricercatori hanno dimostrato che possono bastare degli adesivi o dei graffiti su un segnale stradale per causare un errore di riconoscimento da parte di un sistema di guida autonoma[30]. Piccolissime variazioni nell'*input* – insignificanti agli occhi di un osservatore umano – possono determinare una percezione erronea da parte del sistema di i.a., proprio per il fatto che le tecniche di *machine learning* sono in grado di individuare associazioni statistiche nei dati, ma non sono invece capaci di tracciare modelli astratti di spiegazione causale di tali ricorrenze[31].

Per concludere questa introduzione di carattere fenomenologico, un aspetto che è fondamentale rimarcare è che il funzionamento delle tecniche più sofisticate di *machine learning* è ancora ignoto, nonostante se ne sfruttino ampiamente le potenzialità applicative: insomma, non si sa bene *perché*, ma le previsioni effettuate dagli algoritmi di i.a. sono, nella maggioranza dei casi, corrette, e spesso più accurate di quelle umane. Ci si affida ad esse come ad un *oracolo*

[25] I modelli simbolico-deduttivi di i.a. potevano applicare regole di tipo consequenziale (*if-this-then-that rules*), semplificando e velocizzando le attività umane, ma non erano in grado di gestire situazioni di incertezza. Questi modelli – sebbene utilizzati fino a non molto tempo fa – costituiscono quella che potremmo chiamare l'*archeologia* dell'intelligenza artificiale e sono oggi comunemente chiamati, con un misto di derisione e nostalgia, "*Good Old-Fashioned AI*" (GOFAI), vd. Wallach, Allen (2009), p. 183; Lemley, Casey (2019), p. 1322-1323.
[26] Vd. per tutti Russell, Norvig (2020), p. 651; Domingos (2012), p. 79.
[27] Italiano (2022), p. 50-51.
[28] In argomento vd. Selbst (2020), p. 1318 ss. Sull'incapacità di comprensione simbolica dei sistemi di *machine learning* vd. per tutti Magro (2020), p. 12.
[29] Athalye e al. (2018).
[30] Eykholt e al. (2018).
[31] Selbst, Barocas (2018), p. 1097; Coeckelbergh (2020), p. 2060; Lipton (2018), p. 8-9.

o ad uno "stregone", tanto che i riferimenti alla *magia* e al *genio* sono frequenti da parte degli stessi ricercatori che sviluppano i sistemi di i.a.[32]

Con la diffusione dei sistemi di i.a., si assiste dunque ad una nuova fase del rapporto tormentato tra tecnologia e *agency* umana. In questo caso, infatti, l'imprevedibilità non è un *bug* nel sistema, ma piuttosto un risultato voluto e ricercato dagli stessi programmatori, poiché consente di raggiungere i risultati più efficienti: in questo senso, si dice che i sistemi di i.a. sono *unpredictable by design*[33].

3. La responsabilità civile del produttore di sistemi di i.a. (cenni).

Date queste brevi premesse fenomenologiche, ci concentreremo ora sugli aspetti più strettamente attinenti all'attribuzione della responsabilità per eventi lesivi derivanti dai sistemi di i.a.

Innanzitutto, può essere utile sottolineare che, ad oggi, il dibattito in sede normativa e accademica si è perlopiù focalizzato sui meccanismi ascrittivi della responsabilità *civile* del produttore[34]. La responsabilità aquiliana si candida infatti ad essere lo strumento cardine per la tutela delle persone danneggiate dai sistemi di i.a.: da un lato, grazie al ricorso al modello di imputazione oggettiva previsto dalla direttiva sul danno da prodotto; dall'altro, attraverso la predisposizione di meccanismi di agevolazione probatoria per il ricorrente.

Il testo fondamentale è ovviamente la direttiva sulla responsabilità per danno da prodotto (dir. 85/374/CEE[35]), che prevede la responsabilità oggettiva del produttore per i danni cagionati dal prodotto difettoso. La Commissione Europea, nel settembre 2022, ha presentato una proposta di direttiva volta ad aggiornare e a rendere applicabile tale testo normativo ai nuovi prodotti intelligenti e volta altresì ad introdurre delle inversioni dell'onere della prova a favore del danneggiato (in particolare, delle presunzioni di difettosità del prodotto e di causalità tra difetto e danno)[36]. Complessivamente, questi accorgimenti dovrebbero agevolare il ristoro della persona che ha subito danni provocati da sistemi di i.a. Cercando di riassumere al massimo, la strategia che sta cercando di implementare la Commissione europea parrebbe quella di *accollare economicamente al produttore il rischio dell'imprevedibilità del sistema di i.a.*, garantendo così, al consumatore, un rimedio risarcitorio efficace e facilmente esperibile[37].

4. La responsabilità penale del produttore di sistemi di i.a.

Se la responsabilità aquiliana si conferma uno strumento duttile, capace di adattarsi ai nuovi fenomeni tecnologici, di certo lo stesso non può dirsi dell'ordinamento penale. Le garanzie che circondano il sistema costituzionale del diritto penale (prime tra tutte: legalità, offensività, colpevolezza, presunzione di innocenza) lo rendono infatti un diritto *rigido*, inidoneo a contenere quei fenomeni sistemici, globalizzati ed incerti che caratterizzano la post modernità.

[32] Così, ad esempio, afferma Pedro Domingos, uno dei più noti ricercatori in materia di *machine learning*: «*developing successful machine learning applications requires a substantial amount of 'black art' that is difficult to find in textbooks*», vd. Domingos (2012), p. 78; vd. anche Giacconi (2023), in cui si riportano le considerazioni di Jamie Paik, direttrice del *Reconfigurable Robotics Lab* (RRL) di Losanna: «ogni volta che accendiamo un robot, gli diamo vita e fa quello che ci aspettavamo, è un momento magico, di gioia, euforia. È come se dicessimo sempre una piccola preghiera: *fa' che funzioni questa volta, fa' che funzioni questa volta…*».

[33] Calo (2015), p. 542; Millar, Kerr (2016), p. 107; vd. anche le riflessioni pioneristiche svolte, quando ancora non erano state sviluppate le tecniche di *machine learning*, da Karnow (1996), p. 192.

[34] Nella letteratura italiana si vd., per tutti, il volume curato da A Pajno e al., *Intelligenza artificiale e diritto: una rivoluzione?*, vol. 1 e 2, Il Mulino, 2022, in particolare i contributi di Ruffolo, Amidei (2022); Ruffolo (2022); Amidei (2022); vd. anche Alpa (2021); Fusaro (2020); Palmerini (2020); in ambito europeo vd. Beckers, Teubner (2022) e i contributi contenuti in Ebers, Navas (2020) e in Lohsse e al. (2019).

[35] Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi.

[36] Commissione europea, *Proposta di Direttiva del Parlamento Europeo e del Consiglio sulla responsabilità per danno da prodotti difettosi*, COM (2022) 495 final, 28 settembre 2022.

[37] La Commissione europea ha altresì presentato una Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale), COM (2022) 496 final, 28 settembre 2022, che mira ad introdurre, per i danni cagionati da sistemi di i.a. ai quali non sia applicabile la Direttiva sulla responsabilità da prodotto, una *presunzione del nesso di causalità in caso di colpa* (art. 4) e la possibilità, per l'autorità giudiziaria, di *ordinare la divulgazione degli elementi di prova*, qualora emergano indici di fondatezza della domanda risarcitoria (art. 3).

In particolare, il reato "da intelligenza artificiale" costituisce solo l'ultima tappa di quella tendenziale crisi del delitto d'evento che caratterizza, ormai da decenni, il diritto penale di fronte alla c.d. "società del rischio"[38]: è il noto "shock da modernità" di cui parlava Federico Stella[39].

La problematica riconducibilità del fatto algoritmico alla "persona" del produttore si innesta infatti in un contesto, già esistente, di grave messa in discussione (fino, talvolta, alla forzatura) delle categorie dogmatiche tradizionali, incapaci di contenere – se non attraverso notevoli flessibilizzazioni – la complessità dei fenomeni moderni. Nello specifico, il danno da dispositivo intelligente ripropone, accentuandoli, alcuni dei profili più problematici già sorti in relazione alla responsabilità penale per danno da prodotto: l'indebita sovrapposizione tra struttura commissiva e omissiva del reato; l'ostica identificazione dei soggetti personalmente responsabili all'interno delle organizzazioni complesse; l'individuazione del nesso di causalità in relazione a prodotti caratterizzati da opacità; l'accertamento della colpa in situazioni di incertezza scientifica.

Se le prime tra le questioni citate riproducono sostanzialmente, aggiornandoli, gli interrogativi già emersi in passato, l'imprevedibilità dei sistemi di i.a. porta invece ad un ulteriore livello di complessità l'accertamento del nesso eziologico tra condotta umana ed evento lesivo, nonché la valutazione della colpa in capo all'agente – con particolare riferimento al requisito della *prevedibilità* dell'evento lesivo. È su questi aspetti ci concentreremo ora.

5. L'accertamento del nesso di causalità: incompatibilità tra ragionamento causale e approccio probabilistico del *decision making* algoritmico?

L'ostacolo maggiore all'accertamento del nesso di causalità, ad oggi, è costituito dall'assenza di leggi scientifiche consolidate che siano in grado di descrivere il dispiegarsi della catena causale nel funzionamento degli algoritmi di *machine learning*. Come è stato già accennato parlando della *black box*, in relazione agli algoritmi intelligenti è astrattamente possibile individuare *input* e *output*, ma non è invece agevole ricostruire la catena causale che lega un determinato *input* ad un determinato *output*, a causa del modello di ragionamento *probabilistico* che caratterizza il funzionamento dei sistemi di *machine learning*.

Secondo alcuni studiosi, a tale *gap* conoscitivo potrebbe sopperire l'installazione di *event data recorders* (c.d. EDR, comunemente conosciuti come "scatole nere" o "*logs*"), funzionali ad illuminare, *ex post*, la dinamica dell'evento lesivo[40]. Tali strumenti, tuttavia, non sembrano pienamente in grado di rimediare al *deficit* di *comprensibilità* delle decisioni algoritmiche. Per quanto riguarda gli autoveicoli, ad esempio, l'*event data recorder* può, a seconda delle versioni, registrare la velocità di crociera, l'accelerazione, gli eventuali *input* da parte del conducente (es. la pressione sul pedale del freno), l'attivazione di spie o segnali da parte del veicolo[41]. La scatola nera, tuttavia, *non può dire nulla sulle cause dell'incidente*: si limita a fornire *dati grezzi* da interpretare in sede processuale – attraverso l'ausilio di periti e consulenti tecnici – ma non è di per sé risolutivo ai fini della ricostruzione del nesso causale. Insomma, le questioni restano aperte: perché il veicolo a guida autonoma non ha rallentato di fronte al semaforo rosso? Perché non ha applicato lo spazio di frenata previsto? Il prodotto algoritmico era difettoso? E, se sì, quale componente difettosa del prodotto ha cagionato l'evento lesivo?

Può tra l'altro ipotizzarsi che, in futuro, diventerà tecnicamente possibile ricostruire *ex post* la catena causale che ha condotto alla verificazione di singoli eventi lesivi algoritmici – magari

[38] Vd. Piergallini (2005), p. 1684; Stella (2003); Gargani (2011), p. 397 ss.; Silva Sánchez (2004; ed. spagn. 1999); Herzog (2004), p. 357; Centonze (2004). Il concetto di "società del rischio", come noto, si deve a Beck (2000; ed. ted. 1986), che ha notevolmente influenzato le citate riflessioni penalistiche, ponendo l'accento su come le tecniche di produzione moderna creino sistematicamente rischi che la società, nel suo complesso, non è in grado di controllare ed assorbire.

[39] Stella (2003), *passim*; vd. sul punto Basile (2019), p. 4.

[40] Così Piergallini (2020), p. 1760; Spindler (2019), p. 139; Wagner (2019), p. 612. L'*event data recorder* è stato reso obbligatorio, a partire dal 6 luglio 2022, per tutte le automobili di nuova immatricolazione, ai sensi del Regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio del 27 novembre 2019 relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi. Una misura simile potrebbe essere introdotta, per i sistemi di i.a. ad alto rischio, dal già citato *AI Act*, che all'art. 12 prevede l'installazione obbligatoria, sui suddetti sistemi, di strumenti di registrazione automatica degli incidenti.

[41] T. Lehouillier e al. (2013).

proprio attraverso lo sviluppo di sistemi di i.a. di *reverse engineering* (c.d. *Explainable Artificial Intelligence*)[42]. Anche in questo caso, tuttavia, dalla costante verifica empirica sarà difficile individuare una legge scientifica che consenta di spiegare – in maniera *non solo retroattiva*, ma *anche predittiva* – il rapporto eziologico tra l'*input* x e l'*output* y, proprio a causa della discrasia tra modello stocastico tipico del *machine learning* e paradigma deterministico. Se, insomma, con l'avanzamento delle conoscenze scientifiche sarà probabilmente possibile identificare, nel caso concreto, *la specifica causa dell'evento lesivo algoritmico*, più complessa sarà l'individuazione di una *legge di carattere generale* che sia in grado di spiegare il rapporto di causa-effetto tra una classe di *input* e una classe di *output*.

Questo, ovviamente, pone problemi di compatibilità con il paradigma nomologico-deduttivo dell'accertamento causale, che richiede che sia sempre individuabile una legge scientifica di copertura. La stessa sentenza Franzese[43], pur avendo segnato un primo passo nella direzione della valorizzazione del metodo induttivo, richiede pur sempre, come noto, la sussistenza di una legge scientifica di copertura, benché quest'ultima possa avere anche probabilità statistica *bassa*, qualora dal compendio probatorio emerga una spiegazione causale convincente e «la sicura non incidenza nel caso di specie di altri fattori interagenti in via alternativa» (c.d. *alta probabilità logica*).

6. L'accertamento della colpa del produttore.

La crisi del modello nomologico-deduttivo, determinata da una tendenziale inesplicabilità dei rapporti causa-effetto che governano l'agire algoritmico, sembrerebbe ripercuotersi, a cascata, sull'intera struttura del reato e, nello specifico, sull'accertamento dell'elemento soggettivo in capo al produttore[44]. In particolare, prendendo atto che l'attività illecita di quest'ultimo sarà, nella maggior parte dei casi, *involontaria*, in questa sede ci concentreremo sulla possibilità di muovergli un rimprovero colposo – nonostante non sia escluso che la condotta del produttore possa essere caratterizzata da *dolo*, e, in particolare, da dolo *eventuale*.

In assenza di conoscenze approfondite circa il concreto funzionamento degli algoritmi di *machine learning*, gli eventi lesivi scaturenti dai sistemi di i.a. possono considerarsi *prevedibili* per quanto concerne l'*an*, ma *imprevedibili* con riferimento al *quantum* e al *quomodo*.

L'*imprevedibilità genericamente prevedibile*[45] dei sistemi di i.a. parrebbe così mettere in discussione la stessa possibilità di muovere un rimprovero colposo al produttore, se si considera che, secondo il criterio di copertura del rischio tipico, affinché l'evento lesivo sia rimproverabile all'agente esso deve costituire realizzazione specifica del rischio che la norma cautelare mirava a prevenire. D'altra parte, in giurisprudenza, si è ormai affermato il principio in base al quale il giudizio di prevedibilità non concerne l'evento *hic et nunc* realizzatosi, quanto, piuttosto, la generica classe di eventi in cui si colloca quello oggetto del processo[46].

L'alternativa, dunque, pare netta: qualora prevalga quest'ultimo orientamento, la colpa potrebbe essere considerata sempre sussistente, dal momento che il produttore di un sistema di i.a. potrà sempre prevedere una determinata classe di eventi lesivi algoritmici; al contrario, qualora prevalga una concezione restrittiva, difficilmente potrebbe ritenersi esistente una colpa in capo al produttore, stante il carattere di intrinseca imprevedibilità dell'evento lesivo concretamente realizzatosi.

In ogni caso, un argine all'espansione del giudizio circa la prevedibilità e l'evitabilità dell'evento lesivo potrà essere costituito dal riconoscimento di un'area di rischio consentito, che possiamo definire come quell'area di impermeabilità al giudizio sulla colpa generica dell'agente, delimitata dall'esistenza di regole cautelari positive (vd. v*infra*, § 6.2.). Si pone dunque il problema di verificare: (i) se esistano cautele scritte in materia di sviluppo e commercializzazione di sistemi di i.a. (vd. *infra*, § 6.1.); (ii) quali sono i criteri che consentono l'individuazio-

[42] La letteratura in materia è orma vastissima; si vd. per tutti Guidotti e al. (2018); Selbst, Barocas (2018), p. 1110 ss; Wischmeyer (2020), p. 75 ss.; per una ricostruzione sistematica dei principali lavori in materia di *Explainable Artificial Intelligence* vd. F. Sovrano e al. (2022), p. 126 ss.
[43] Cass., sez. un., 11 luglio 2022, n. 30328, Franzese.
[44] Sul problema della causalità come "origine" di tutte le altre difficoltà applicative del diritto penale nella materia del danno da prodotto vd. Piergallini (2005).
[45] Piergallini (2020), p. 1762; vd. anche Magro (2019), p. 1208-1209; Beck (2016), p. 139.
[46] Per una ricostruzione di tale orientamento giurisprudenziale si vd., per tutti, Civello (2022), p. 1017; Piergallini (2005), p. 1692.

ne di un'area di rischio consentito (vd. *infra*, § 6.2.).

6.1. *Le regole cautelari scritte.*

In assenza di generalizzazioni scientifiche sui decorsi eziologici del *decision making* algoritmico, potrebbe apparire ontologicamente impossibile la redazione di *standard* tecnici funzionali al contenimento di eventi lesivi[47]. Pur non conoscendo le precise modalità con le quali i sistemi di i.a. decidono, sappiamo tuttavia che gli errori dei sistemi di *machine learning* possono avere variamente a che fare: (i) con un errore nel codice algoritmico; (ii) con l'alimentazione dell'algoritmo con dati erronei o incompleti; (iii) con un addestramento dell'algoritmo carente o inadeguato[48]. In relazione a questi aspetti, è dunque auspicabile l'elaborazione di cautele volte a minimizzare il rischio di eventi algoritmici lesivi (c.d. *cautele improprie*)[49].

Attualmente, tuttavia, le norme cautelari scritte aventi ad oggetto lo sviluppo e la messa in commercio di sistemi di i.a. sono pochissime. Qualora venisse approvata, la già citata proposta di regolamento europeo sull'intelligenza artificiale (c.d. *AI Act*) rappresenterebbe il principale riferimento in materia. In particolare, la bozza di Regolamento europeo prevede una serie di requisiti per la commercializzazione di sistemi di i.a., specie per quelli c.d. "ad alto rischio"[50], che saranno poi specificati e concretizzati attraverso l'emanazione di norme armonizzate da parte degli enti di normalizzazione a ciò preposti (CEN, Comitato europeo di normalizzazione, e CENELEC, Comitato europeo di normalizzazione elettrotecnica)[51].

Tra i vari requisiti per lo sviluppo e la messa in commercio di dispositivi "ad alto rischio", ci limitiamo a ricordarne alcuni: l'adozione di un "sistema di gestione dei rischi" (art. 9); l'utilizzo di *dataset* "di qualità" (art. 10); la predisposizione di idonea documentazione tecnica (art. 11); l'installazione di *event data recorder* sui dispositivi (art. 12); la previsione di meccanismi che garantiscano il controllo di una persona fisica sul funzionamento del sistema (art. 14, c.d. principio dell'*human-in-the-loop*).

L'emanazione di *standard* tecnici specifici per la messa in commercio di dispositivi intelligenti è auspicata dalla gran parte dei commentatori, come misura di attenuazione dell'incertezza regolativa in materia e, di conseguenza, del *deficit* di precisione e determinatezza della fattispecie colposa[52]. In realtà, un guadagno in termini di determinatezza sarebbe conseguibile soltanto qualora la norma positivizzata fornisse *standard* di comportamento rigidi ed esaustivi, dal momento che le cautele elastiche si fondano sul medesimo meccanismo ricostruttivo uti-

[47] Lo notava, in relazione ai prodotti tradizionali, Piergallini (2004), p. 243.

[48] Va tuttavia nuovamente sottolineato che eventi lesivi potranno derivare anche da sistemi di *machine learning* pienamente conformi alle cautele esistenti, dal momento che i meccanismi probabilistici che ne costituiscono la base di funzionamento sono, per loro natura, *fallibili*. Sono proprio questi eventi lesivi che dovrebbero rientrare nell'area del rischio consentito.

[49] Come noto, per norme cautelari improprie si intendono quelle regole che prevedono l'adozione di misure idonee a ridurre il rischio, al contrario di quelle *proprie*, che invece tendono alla sua completa neutralizzazione. La definizione è stata proposta da Veneziani (2003) ed è ormai comunemente accettata in dottrina, vd. per tutti Piergallini (2017), p. 229; Zirulia (2018), p. 364; Brusco (2012), p. 391.

[50] I sistemi di i.a. ad alto rischio sono individuati dall'art. 6 della proposta attraverso una duplice tecnica normativa: attraverso menzione espressa e attraverso rinvio al campo di applicazione di normative europee settoriali. Quanto alla prima categoria, l'art. 6, § 2 rinvia ai settori elencati all'allegato III, che comprendono, da un lato, sistemi che possono mettere in pericolo l'incolumità pubblica o la sicurezza fisica delle persone (es. n. 2 "*Gestione e funzionamento delle infrastrutture critiche*", si pensi alle componenti di sicurezza nella fornitura di acqua o di gas) e, dall'altro, sistemi che, se usati in maniera scorretta, possono causare gravi violazioni dei diritti fondamentali (es. n. 1 "*Identificazione e categorizzazione biometrica delle persone fisiche*", si pensi ai sistemi di riconoscimento facciale). Quanto alla seconda categoria, ai sensi dell'art. 6, § 1, sono altresì ad alto rischio i sistemi che soddisfano entrambe le seguenti condizioni: 1) sono prodotti – o sono destinati ad essere utilizzati come componenti di sicurezza di un prodotto – disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato II (si tratta, ad esempio, della Direttiva c.d. macchine CE/2006/42, del Regolamento c.d. dispositivi medici UE/2017/745, della Direttiva c.d. giocattoli CE/2009/48, della Direttiva c.d. imbarcazioni di diporto CE/1994/25); 2) sono prodotti soggetti a una valutazione di conformità da parte di terzi, ai fini dell'immissione sul mercato o della messa in servizio, ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II. L'*AI Act* prevede una compiuta disciplina in materia di *product safety* soltanto in relazione ai suddetti sistemi "ad alto rischio" (vd. titolo III, artt. 6 ss.).

[51] La Commissione Europea, il 5 dicembre 2022, ha pubblicato la bozza di "richiesta di standardizzazione" nei confronti di CEN e CENELEC. Una volta adottata la proposta, gli *standard* dovrebbero essere pubblicati entro il 31 gennaio 2025 (dunque prima dell'entrata in vigore dell'*AI Act*, che sarà applicabile dopo 24 mesi dall'approvazione, ai sensi dell'art. 85). Per un approfondimento sul funzionamento del processo europeo di standardizzazione – che si propone di favorire una maggiore armonizzazione tra le normative interne e, di conseguenza, di agevolare la circolazione dei beni – si rinvia a Commissione europea, *La guida blu all'attuazione della normativa UE sui prodotti 2022*, 29 giugno 2022, 2022/C 247/01.

[52] In generale, sul ruolo delle norme cautelari codificate nell'attenuazione del *deficit* di determinatezza della fattispecie colposa vd. per tutti Marinucci, Dolcini (2001), p. 41 ss.

lizzato per la colpa generica, ossia il riferimento all'agente modello[53].

La bozza di regolamento europeo sull'intelligenza artificiale, in questo senso, non pare fornire soluzioni del tutto soddisfacenti, dal momento che la vaghezza con la quale descrive i requisiti minimi per l'accesso dei sistemi di i.a. sul mercato europeo sembra prefigurare l'introduzione di norme cautelari *elastiche*. Si pensi, ad esempio, all'art. 9, § 4, lett. a), dell'*AI Act*, che stabilisce che il sistema di gestione dei rischi debba garantire l'eliminazione o la riduzione dei rischi "*per quanto possibile*": è ovvio che tale riferimento non può che aprire la strada ad una comparazione con il parametro dell'*homo eiusdem condicionis et professionis*.

Un ruolo fondamentale nella codificazione delle norme cautelari sarà probabilmente svolto, inoltre, dagli *standard* emanati dalla *International Organization for Standardization* (c.d. ISO) e dalla *International Electrotechnical Commission* (c.d. IEC). In particolare, ISO e IEC hanno istituito un *focus group* congiunto (ISO/IEC JTC 1/SC 42), finalizzato alla pubblicazione di *standard* per lo sviluppo e la produzione di sistemi di intelligenza artificiale[54]: tra 2020 e 2022, tra gli altri, sono stati pubblicati *standard* in materia di discriminazione algoritmica[55], *risk governance*[56], affidabilità[57], valutazione qualitativa dei sistemi di reti neurali artificiali[58], etc. Fondamentale sarà tuttavia la pubblicazione di *standard* che disciplinino settorialmente gli specifici campi in cui può essere utilizzata l'intelligenza artificiale.

Già *de jure condito*, d'altra parte, sono valide le norme cautelari già esistenti previste dalle direttive della c.d. *legislazione europea verticale*, a seconda del settore nel quale lo specifico dispositivo di intelligenza artificiale rientra: si pensi, ad esempio, alla c.d. Direttiva macchine (Dir. 2006/42/CE)[59], al Regolamento sui dispositivi medici (UE/2017/745)[60], alla Direttiva c.d. giocattoli (CE/2009/48)[61], etc. In chiave complementare e sussidiaria rispetto alle suddette cautele positive si pongono poi i modelli di *autonormazione* e *autocontrollo* eventualmente implementati dal produttore, che possono essere considerati dal giudice nella valutazione circa la sicurezza del prodotto (vd. art. 105, co. 3, d.lgs. 6 settembre 2005, n. 206, cod. cons., che fa riferimento, tra i parametri di valutazione della sicurezza del prodotto, anche ai «codici di buona condotta in materia di sicurezza vigenti nel settore interessato»).

6.2. *Il rapporto tra regole cautelari scritte e regole cautelari non scritte: quale spazio per il rischio consentito?*

Poniamo ora il caso che il dispositivo intelligente abbia cagionato un evento lesivo *nonostante l'osservanza*, da parte del produttore, delle norme cautelari codificate. Il rispetto delle cautele positive stabilite dagli *standard* tecnici non potrà infatti evitare il rischio che dal concreto operare dei sistemi di i.a. derivino eventi lesivi per la vita, la salute o l'integrità fisica: nel momento in cui, infatti, si attribuisce una capacità di autonomo *decision making* ad un algoritmo – ancorché parziale e sotto supervisione di un essere umano – non si potrà escludere che da questo si verifichino decorsi eziologici dannosi. Di qui la questione: il rispetto degli *standard* tecnici di settore – quando saranno introdotti – sarà sufficiente ad escludere la colpa in capo al produttore, o il giudice dovrà invece valutare se la condotta di questi sia conforme a quella dell'*homo eiusdem condicionis et professionis*?

È un problema ben noto, che ancora non ha trovato una soddisfacente e condivisa solu-

[53] Castronuovo (2005), p. 328; Palazzo (2011), p. 189.
[54] Informazioni sui lavori del *focus group* – comprensive dell'elenco completo degli *standard* in materia di i.a. pubblicati fino ad oggi – sono consultabili a questo link.
[55] International Organization For Standardization – International Electrotechnical Commission, *ISO/IEC TR 24027:2021 – Bias in AI systems and AI aided decision making*.
[56] International Organization For Standardization – International Electrotechnical Commission, *ISO/IEC TR 24368:2022 – Information technology — Artificial intelligence — Overview of ethical and societal concerns*.
[57] International Organization For Standardization – International Electrotechnical Commission, *ISO/IEC TR 24028:2020 – Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence*.
[58] International Organization For Standardization – International Electrotechnical Commission, *ISO/IEC TR 24029-1:2021 – Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview*.
[59] Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine. La direttiva è attualmente oggetto di una proposta di riforma presentata dalla Commissione Europea (Proposta di Regolamento del Parlamento europeo e del Consiglio sui prodotti macchina; COM (2021) 202 final, 21 aprile 2021).
[60] Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici.
[61] Direttiva 2009/48/CE del Parlamento europeo e del Consiglio del 18 giugno 2009 sulla sicurezza dei giocattoli.

zione sul piano dogmatico. Tradizionalmente, come noto, si ritiene che il rispetto delle norme cautelari positive non esoneri l'agente dal tenere un comportamento diligente, da identificarsi sulla base del criterio del c.d. agente modello[62]. Nel caso delle attività produttive, tuttavia, il problema si complica, poiché le norme cautelari, oltre che una funzione di *prevenzione* rispetto al verificarsi dell'evento lesivo, hanno altresì una funzione di *garanzia* e di *orientamento* nei confronti dell'agente, in settori particolarmente rischiosi e ad alta complessità tecnico-normativa.

Si apre così la questione circa la sussistenza di un'area di c.d. "rischio consentito" (*erlaubtes risiko*), da tempo dibattuta in dottrina[63] e oggetto di rinnovata attenzione, recentemente, proprio in relazione agli eventi lesivi derivanti da sistemi di i.a.[64].

Non è questa la sede per soffermarci sulle varie ricostruzioni ermeneutiche del "rischio consentito" che, nel corso del tempo, sono state date. Possiamo qui limitarci a citarne una particolarmente autorevole, proposta da Gabrio Forti, secondo la quale la nozione di rischio consentito indicherebbe un'area di «condotte pericolose, ammesse dall'ordinamento nonostante che l'adozione di cautele idonee a contrastare i possibili svolgimenti lesivi sia destinata a residuare un certo grado di pericolosità»[65]. In quest'accezione, il rischio consentito viene anche qualificato come "rischio residuale *(Restrisiko)*"[66], intendendosi, con tale designazione icastica, quel *pericolo marginale* che le misure preventive non sono in grado di disinnescare (o che, sulla base di un rapporto costi-benefici, le autorità che "producono" la normativa cautelare *decidono* di non disinnescare) e che, di conseguenza, ricade sulla società. In quest'accezione, la nozione di "rischio consentito" delinea quelle ipotesi in cui il rispetto delle norme cautelari *codificate* impedisce che possa essere mosso all'imputato un rimprovero per non aver osservato norme di diligenza, prudenza, perizia *non codificate*.

Come noto, l'istituto del rischio consentito è strutturalmente legato all'idea che la norma cautelare è *inidonea a prevenire tutti i rischi che è finalizzata a prevenire*. Si tratta di un'inidoneità *prevedibile* e *programmata*: il legislatore – e gli altri soggetti che, a vario titolo, sono deputati alla definizione delle regole cautelari – nel momento in cui delineano il bilanciamento tra interessi divergenti *sanno* che la cautela è talvolta destinata a fallire, poiché non sarà in grado di avere efficacia impeditiva nei confronti di *tutti* gli eventi lesivi[67]. Così, per riportare il discorso sui binari dell'intelligenza artificiale, il legislatore europeo, con l'*AI Act*, introduce una serie di norme cautelari volte a *minimizzare* il rischio di eventi lesivi algoritmici, non a *neutralizzarlo*: accetta, dunque, sebbene implicitamente, che dallo sviluppo e dalla commercializzazione di sistemi di i.a. derivi una *certa quota* di eventi offensivi.

L'unico margine di operatività di una valutazione della colpa generica dell'agente dovrebbe configurarsi nel caso in cui la regola cautelari manifesti *segnali univoci* di fallimento "non preventivato"[68]. In questi casi – quando la norma cautelare scritta, dunque, si riveli inidonea al raggiungimento degli obiettivi che ne costituiscono il fondamento –, la diligenza impone di adottare cautele ulteriori; il che, nella prospettiva del produttore di un sistema di i.a., potrebbe significare: il fornire ulteriori informazioni al consumatore, l'aggiornamento del *software*, o, nei casi più gravi, il ritiro o il richiamo del prodotto.

Il problema che si è sempre posto nell'applicazione di questi principi, tuttavia, è quello di riconoscere univocamente i suddetti *segnali* di fallimento "non preventivato" delle regole cautelari scritte. Nel settore dell'intelligenza artificiale, un aiuto in questo senso potrebbe derivare dalla possibilità, per i produttori, di monitorare costantemente le *performance* degli algoritmi, attraverso i già citati meccanismi di *explainability* – possibilità che potrebbe determinare un incremento nella *calcolabilità* degli errori e, di conseguenza, degli eventi lesivi che possono derivarne.

[62] Vd. per tutti Marinucci (1965), p. 236; Mantovani (1988), p. 309.
[63] La letteratura sul tema è ormai di ampiezza considerevole; si vd. Forti (1990), p. 250 ss.; Forti (2006), p. 155 ss.; Piergallini (2004), *passim;* Piergallini (2005), p. 1670 ss.; Militello (1988), p. 55 ss. (che preferisce, tuttavia, l'espressione "rischio adeguato"); Giunta (2006), p. 227 ss.; Consulich (2022a), p. 1102 ss.; Zirulia (2018), p. 335 ss.; Castronuovo (2011), *passim*; Castronuovo (2012), *passim*; Donini (2004), p. 119 ss.; Massaro (2011), *passim*; Pulitanò (2008), p. 647; Ruga Riva (2006), p. 1743 ss.
[64] Vd., con vari accenti, Gless, Silverman, Weigend (2016), pp. 430-431; Piergallini (2020), p. 1750; Salvadori (2021), p. 116 ss.; Manes (2020), p. 5; Cappellini (2018), p. 19; Fiorella (2022), p. 656 ss.; Piva (2022), p. 681 ss.
[65] Forti (1990), p. 457.
[66] Forti (1990), p. 457.
[67] Consulich (2022a), p. 1116.
[68] Parlano di eventuale "fallimento" delle norme cautelari, tra gli altri, Forti (1990), p. 671 ss.; Veneziani (2003), p. 61 ss.; Zirulia (2018), p. 380.

Poniamo il caso, ad esempio, che il legislatore stabilisca un apparato di norme cautelari rigide per lo sviluppo e la produzione di *software* di guida autonoma (es. modelli di raccolta e gestione dati, addestramento, sperimentazione, etc.), esplicitando che la fissazione di tali norme è funzionale a mantenere il tasso di incidenti al di sotto della soglia dell'x% rispetto all'utilizzazione del veicolo. Nel caso in cui, nonostante il rispetto delle norme cautelari rigide, il produttore verifichi che il tasso di sinistri derivanti dall'utilizzo del *software* sia superiore rispetto alla soglia del rischio lecito, questi dovrà adottare cautele ulteriori per minimizzare i rischi e, eventualmente, richiamare o ritirare il prodotto. Non è necessario, a tal fine, che la suddetta verifica abbia i crismi di un rigoroso accertamento del nesso di causalità condotto con gli *standard* penalistici – accertamento che, come abbiamo rilevato, sconta problematiche che potrebbero risultare insormontabili. La verifica dovrebbe essere tuttalpiù in grado di *isolare* gli errori algoritmici, senza che sia invece necessario, in ipotesi, individuare il preciso *input* che ha determinato il verificarsi dell'errore algoritmico e, dunque, dell'evento lesivo.

Il superamento del tasso stabilito in via legislativa non determinerebbe l'automatica imputazione degli eventi lesivi "ulteriori" al produttore, ma dovrebbe essere considerato come segnale di *incipiente fallimento delle norme cautelari scritte*: dovrebbe, dunque, indurre il produttore ad adottare cautele più pregnanti rispetto a quelle previste dalla normativa esistente.

Un approccio simile è stato proposto da una parte della dottrina civilistica, con riferimento al tema contiguo dell'accertamento di un difetto di *design*[69]. In particolare, tale orientamento ipotizza di valutare la difettosità del prodotto intelligente attraverso la comparazione tra la prestazione complessiva del sistema di i.a. che ha causato il danno e la *performance* di un modello di algoritmo mediamente sicuro. A tal fine, si prospetta l'opportunità di individuare una soglia di riferimento – relativa al rapporto percentuale tra eventi lesivi verificatisi e utilizzo complessivo del *software* – al di sopra della quale l'algoritmo dovrebbe essere considerato difettoso.

Simili soluzioni – sia nel settore civile, sia in quello penale – avrebbero il vantaggio di spostare il *focus* della valutazione sulla sicurezza del prodotto intelligente, dalla prestazione singola alla sua *performance* complessiva: una traslazione valutativa che appare indispensabile se si vuole godere dei benefici derivanti dallo sviluppo dei sistemi di i.a., senza che singoli eventi lesivi possano mettere in discussione la sicurezza del prodotto.

In conclusione, non possono, in ogni caso, essere trascurati i limiti di una siffatta prospettazione. Potrebbe emergere, innanzitutto, un limite tecnico, relativo alla disponibilità, per il produttore, di affidabili e tempestivi meccanismi di controllo sulle *performance* algoritmiche: tale problema, tuttavia, potrebbe essere risolto in un futuro non troppo lontano, dati i continui progressi scientifici in materia di *Explainable AI*. Più pregnante è invece la questione di natura politica: quale regolatore, infatti, espliciterebbe mai in maniera così diretta il bilanciamento tra esercizio di un'attività pericolosa e beni giuridici di estremo rilievo (quali, in ipotesi, vita ed integrità fisica)? Il rischio, d'altra parte, è che anche qualora si pervenisse all'individuazione di una soglia quantitativa, questa sia ispirata a logiche *iper-cautelative*, che determinerebbero di fatto, per il produttore, la necessità di adottare sempre cautele *ulteriori* rispetto a quelle positive.

7. Una tutela anticipata in relazione ai sistemi di i.a. pericolosi: prospettive *de jure condito* e *de jure condendo*.

Nonostante lo sforzo di ricostruzione ermeneutica sin qui svolto, il cammino per il riconoscimento di una responsabilità penale in capo al produttore di sistemi di i.a. appare in tutta la sua tortuosità. In particolare, l'imprevedibilità e l'opacità del *decision making* algoritmico *allontanano* l'evento lesivo dalla condotta umana, incidendo così sulla possibilità di muovere un rimprovero colposo al produttore e, prima ancora, di individuare con certezza il nesso di causalità tra condotta umana ed evento lesivo. Già da tempo, d'altra parte, autorevole dottrina segnala come il diritto penale, di fronte alle sfide della società del rischio tecnologico, si trovi di fronte ad una vera e propria "crisi da incontenibilità"[70], determinata dalla difficoltà di ritenere nel "tipo" fenomeni complessi, globalizzati, imperscrutabili.

[69] Borghetti (2019), p. 63 ss.
[70] Paliero (1994), p. 1238.

Di qui la convinzione che – a meno di non voler rinunciare ai principi cardine del diritto penale – una responsabilità del produttore per gli eventi lesivi algoritmici costituirà una rarità. In questo contesto, una tutela penalistica – la sola, ci pare, in grado di esprimere il disvalore insito nella creazione o nel mantenimento di rischi illeciti a beni giuridici di primaria importanza, quali la vita e l'integrità fisica – potrebbe appuntarsi in forma anticipata, attraverso il ricorso a reati colposi di mera condotta.

Già *de jure condito* si potrebbe fare riferimento alle fattispecie contravvenzionali previste dall'art. 112 cod. cons., commi 1, 2, 3, che puniscono la commercializzazione di prodotti *pericolosi*, e che trovano applicazione in via sussidiaria, «*se il fatto non costituisce più grave reato*»: l'efficacia deterrente di tali norme, tuttavia, rischia di essere risibile, stante l'esiguità delle pene ivi previste (la pena per la fattispecie più grave, quella di cui al primo comma, prevede l'arresto da sei mesi ad un anno e l'ammenda da 10.000 a 50.000 euro). Non è detto, d'altra parte, che il sistema di i.a. rientri sempre nella nozione di "prodotto" fornita dall'art. 3, co. 1, lett. e), cod. cons., in base alla quale per "prodotto" si intende «qualsiasi prodotto destinato al consumatore, anche nel quadro di una prestazione di servizi, o suscettibile, in condizioni ragionevolmente prevedibili, di essere utilizzato dal consumatore, anche se non a lui destinato, fornito o reso disponibile a titolo oneroso o gratuito nell'ambito di un'attività commerciale […]». Tralasciando l'evidente problema di circolarità della norma (*un prodotto è… un prodotto!*), la riconducibilità dei sistemi di i.a. alla suddetta definizione sembrerebbe possibile soltanto nei casi in cui l'algoritmo di intelligenza artificiale sia incorporato in un bene *destinato al consumatore* o *suscettibile di essere da lui utilizzato* (es. sistema di guida autonoma installato su un veicolo)[71]. Non sembrerebbe, invece, esservi alcuno spazio per un'estensione dell'ambito applicativo della norma ai c.d. *prodotti digitali*, ovverosia ai *software* che non sono incorporati in un *hardware*.

Uno spunto per l'introduzione di una tutela penale anticipata potrebbe venire, piuttosto, dalla già citata Proposta di Regolamento europeo, che – nel prevedere una serie di requisiti per lo sviluppo e la messa in commercio di sistemi di i.a. – obbliga gli Stati membri ad introdurre sanzioni «effettive, proporzionate e dissuasive» per il caso di mancato rispetto della disciplina ivi stabilita (vd. art. 71, § 1, *AI Act*). Una parte della dottrina, a tal proposito, ha proposto l'introduzione di reati colposi di mera condotta, volti a criminalizzare: (*i*) l'omessa predisposizione, da parte del produttore, di determinati presidi di sicurezza nei sistemi di i.a.; (*ii*) la disattivazione, la mancata attivazione o il mancato aggiornamento, da parte dell'utilizzatore, dei presidi di sicurezza di cui invece il sistema di i.a. fosse stato originariamente dotato[72].

In quest'ottica, uno spazio potrebbe essere riservato, sempre *de jure condendo*, alla valorizzazione del modello ingiunzionale [73], favorendo così un coordinamento tra sanzione penale e capillare controllo amministrativo[74]. L'ingiunzione, da parte delle autorità competenti, di assumere misure di sicurezza (es. adozione di ulteriori cautele, sottoposizione dei dispositivi intelligenti a *training* o sperimentazione aggiuntiva, fino all'ordine di disattivazione) potrebbe infatti essere presidiata da sanzioni penali, così da fronteggiare – in un'ottica di governo condiviso del rischio – l'eventuale inosservanza, da parte dell'impresa, di prestazioni di *facere* individualizzate e infungibili[75]. Non si può non rilevare, tuttavia, come misure di questo tipo – già presenti nella disciplina generale sulla sicurezza dei prodotti (vd. art. 112, co. 1 e 3, cod. cons.) – siano, ad oggi, rimaste soltanto sulla carta.

Infine, in una logica di "democratizzazione" dei processi di valutazione e prevenzione del rischio[76] – e prendendo atto delle conoscenze specifiche esistenti all'interno delle imprese –, si potrebbero prevedere, a carico delle società produttrici, degli *obblighi di diffusione delle informazioni* sui rischi derivanti dallo sviluppo e dalla messa in commercio dei sistemi di i.a.[77].

[71] Consulich (2022b), p. 1039.
[72] Consulich (2022b), p. 1038-1039; LaGioia, Sartor (2020), p. 459.
[73] Piergallini (2020), p. 1773.
[74] In generale, sulla tecnica ingiunzionale vd. Marinucci (2005), p. 56 ss.; Alessandri (2000), p. 50 ss.
[75] È questo uno dei più apprezzabili vantaggi del modello ingiunzionale; vd. a tal proposito Alessandri (2000), p. 51-52.
[76] Forti (2006), p. 217.
[77] È la tesi di Forti (2006), *passim*; per un "aggiornamento" della tesi al contesto produttivo dell'intelligenza artificiale vd. Piergallini (2020), p. 1773.

8. Conclusioni.

L'ampio e stimolante dibattito emerso durante questo Corso testimonia come l'intelligenza artificiale ponga davanti ai penalisti – e, in generale, a tutti i giuristi – problemi inediti e urgenti. D'altra parte, se è vero che ci troviamo di fronte ad un fenomeno dalle caratteristiche nuove e dirompenti, lo studio dell'impatto dell'intelligenza artificiale sulla responsabilità penale sembrerebbe costituire un avamposto privilegiato per osservare alcune tendenze più generali del diritto penale, relative, in particolare, all'accertamento del nesso di causalità e della colpa in contesti di incertezza scientifica.

La riscontrata difficoltà nell'individuazione delle responsabilità *personali* nell'ambito della produzione dei sistemi di i.a. sembrerebbe inoltre aprire ad una rinnovata riflessione sul ruolo della responsabilità amministrativa degli enti nella prevenzione delle attività criminali[78]. In particolare, nel settore della produzione dei sistemi di i.a. emerge plasticamente la disarmonia tra carattere intrinsecamente *plurisoggettivo* degli illeciti e conformazione *personalistica* della responsabilità penale: una disarmonia che si riscontra in relazione a tutti i fenomeni tipici della criminalità d'impresa e che sconta il rischio che la ricerca del soggetto rimproverabile all'interno delle società si trasformi in una caccia al capro espiatorio[79]. *De jure condendo*, proprio il settore della produzione di sistemi di i.a. – per le peculiarità che abbiamo tentato di descrivere – potrebbe rappresentare un utile banco di prova per sperimentare modelli volti a realizzare una maggiore *autonomia* della responsabilità dell'ente rispetto a quella della persona fisica[80].

Per concludere, resta sullo sfondo l'interrogativo su quale ruolo il diritto penale potrà concretamente svolgere, sul lungo periodo, in una società retta da meccanismi artificiali, il cui funzionamento non è del tutto conoscibile nemmeno ai loro creatori. La sfida sarà quella di salvaguardare l'insostituibile *utilità sociale* del diritto penale, senza rinunciare alle garanzie e ai principi che ne costituiscono il fondamento democratico (colpevolezza e legalità, *in primis*).

Bibliografia

Alessandri, Alberto (2000): *Parte generale*, in Pedrazzi, Cesare e al. (a cura di), *Manuale di diritto penale dell'impresa*, Monduzzi, II ed.

Alpa, Guido (2021): *Quale modello normativo europeo per l'intelligenza artificiale?*, in *Contr. impr.*, n. 4, p. 1003 ss.

Amidei, Andrea (2019): *Intelligenza Artificiale e* product liability*: sviluppi del diritto dell'Unione Europea*, in *Giur. it.*, luglio 2019, p. 1715 ss.

Amidei, Andrea (2022): *Le responsabilità del produttore di intelligenza artificiale «difettosa» tra misure di attenuazione* by design *e obblighi di trasparenza*, in Pajno, Alessandro, e al. (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. 1, il Mulino.

Athalye, Anish, e al. (2018): *Synthesizing Robust Adversarial Examples*, in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*.

Basile, Fabio (2019): *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Dir. pen. uomo*, 2019.

Bathaee, Yavar (2018): *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, in 31 *Harvard Journal of Law & Technology*, n. 2, p. 889 ss.

[78] Panattoni (2021), p. 362 ss.
[79] Su tale rischio vd. Marinucci (2005), p. 57. Per una recente analisi, da una prospettiva sociologica, del meccanismo del capro espiatorio organizzativo vd. Catino (2022).
[80] Sull'emancipazione, *de jure condendo*, della responsabilità *ex* d.lgs. 231/2001 dalla dipendenza dal reato della persona fisica vd. Gargani (2022), p. 48 ss., e, in tema di reati ambientali, Maldonato (2021), p. 504 ss.; per una valorizzazione, *de jure condito*, dell'art. 8 del d.lgs 231/2001, vd., sempre in materia di criminalità ambientale, Consulich (2018b), p. 22 ss.; in materia di imputazione di eventi lesivi algoritmici, Consulich (2018a), p. 224 ss.

Beck, Susanne (2016): *Intelligent agents and criminal law – Negligence, diffusion of liability and electronic personhood*, in 86 *Robotics and Autonomous Systems*, p. 138 ss.

Beck, Ulrich (2000): *La società del rischio. Verso una seconda modernità*, Carocci, 2000 (ed. ted. 1986).

Beckers, Anna, Teubner, Gunther (2022): *Three Liability Regimes for Artificial Intelligence*, Bloomsbury.

Borghetti, Jean-Sébastien (2019) *How can Artificial Intelligence be Defective?*, in Lohsse, Sebastian e al. (eds): *Liability for Artificial Intelligence and the Internet of Things*, Nomos, Baden-Baden.

Brusco, Carlo (2012): *Rischio e pericolo, rischio consentito e principio di precauzione*, *La c.d. "flessibilizzazione delle categorie del reato"*, in *Criminalia*, 2012, p. 383 ss.

Calo, Ryan (2015): *Robotics and the Lessons of Cyberlaw*, in 103 *Calif. L. Rev.*, 2015, p. 513 ss.

Cappellini, Alberto (2018): Machina delinquere non potest? *Brevi appunti su intelligenza artificiale e responsabilità penale*, in *Criminalia*, pubblicato successivamente in *disCrimen*, 2019

Cappellini, Alberto (2023): *Reati colposi e tecnologie dell'intelligenza artificiale*, in Balbi, Giuliano e al. (a cura di), *Diritto penale e intelligenza artificiale. "Nuovi Scenari"*, Giappichelli

Cassens Weiss, Debra (2023): *ChatGPT falsely accuses law prof of sexual harassment; is libel suit possible?*, in *ABA Journal*, 6 aprile 2023;

Castelvecchi, Davide (2016): *Can We Open the Black Box of AI?*, in *Nature*, 5 ottobre 2016.

Castronuovo, Donato (2005): *Responsabilità da prodotto e struttura del fatto colposo*, in *Riv. it. dir. proc. pen.*, p. 301 ss.;

Castronuovo, Donato (2011): *Principio di precauzione e beni legati alla sicurezza*, in *Dir. pen. cont.*, 21 luglio 2011.

Castronuovo, Donato (2012): *Principio di precauzione e diritto penale. Paradigmi dell'incertezza nella struttura del reato*, Aracne.

Catino, Maurizio (2022): *Trovare il colpevole. La costruzione del capro espiatorio nelle organizzazioni*, il Mulino.

Centonze, Francesco (2004): *La normalità dei disastri tecnologici: il problema del congedo dal diritto penale*, Giuffrè, 2004.

Civello, Gabriele (2022): (voce) *Prevedibilità e reato colposo*, in Donini, Massimo (diretto da), *Reato colposo*, *Enc. dir. – I Tematici*, Giuffrè.

Clarke, Laurie (2021): *The EU's leaked AI regulation is ambitious but disappointingly vague*, in *Tech Monitor*, 15 aprile 2021.

Coeckelbergh, Mark (2020): *Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability*, in 26 *Science and Engineering Ethics*, p. 2051 ss.

Consulich, Federico (2018a): *Il nastro di Möbius. intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca borsa*, vol. 71, n. 2, p. 195 ss.

Consulich, Federico (2018b): *Il giudice e il mosaico. La tutela dell'ambiente, tra diritto dell'Unione e pena nazionale*, in *Leg. pen.*, 27 luglio 2018,

Consulich, Federico (2022a): (voce) *Rischio consentito*, in Donini, Massimo (diretto da), *Reato colposo*, *Enc. dir. – I Tematici*.

Consulich, Federico (2022b), Flash offenders. *Le prospettive di* accountability *penale nel contrasto alle intelligenze artificiali devianti*, in *Riv. it. dir. proc. pen.*, fasc. 3, p. 1015 ss.

Domingos, Pedro (2012): *A Few Useful Things to Know about Machine Learning*, in *Communications of the ACM*, vol. 55, n. 10, nov. 2012.

Donini, Massimo (2004): *Il volto attuale dell'illecito penale*, Giuffrè.

Ebers, Martin, Navas, Susana (2020, eds.): *Algorithms and Law*, Cambridge University Press.

Eykholt, Kevin, e al. (2018): *Robust Physical-World Attacks on Deep Learning Visual Classification*, in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*.

Filicetti, Carmine (2023): *Sulla definizione di algoritmo (nota a Consiglio di Stato, Sezione Terza, 25 novembre 2021, n. 7891)*, in *Giust. ins.*, 8 febbraio 2023.

Fiorella, Antonio (1988): *Responsabilità penale* (voce), in *Enc. Dir.*, vol XXXIX, p. 1289 ss.

Fiorella, Antonio (2022): *Responsabilità penale dei* Tutor *e dominabilità dell'Intelligenza Artificiale*, *Rischio permesso e limiti di autonomia dell'Intelligenza Artificiale*, in Giordano, Rosaria, e al. (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Giuffrè.

Forti, Gabrio (1990), *Colpa ed evento nel diritto penale*, Giuffrè.

Forti, Gabrio (2006), *"Accesso" alle informazioni sul rischio e responsabilità: una lettura del principio di precauzione*, in *Criminalia*, 2006, p. 155 ss.

Fusaro, Arianna (2020): *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso*, in *Nuova giur. civ. comm.*, n. 6, p. 1346.

Gargani, Alberto (2011): *La "flessibilizzazione" giurisprudenziale delle categorie classiche del reato di fronte alle esigenze di controllo penale delle nuove fenomenologie di rischio*, in *Leg. pen.*, n. 2, p. 397 ss.

Gargani, Alberto (2022): *Profili della responsabilità collettiva da reato colposo*, in *Riv. trim. dir. pen. econ.*, fasc. 1-2, p. 48 ss.

Giacconi, Riccardo (2023): *Una sorta di magia. Intelligenze artificiali, origami, marionette, serpenti: scoprire l'incanto nei laboratori di robotica*, in *Il Tascabile*, 2 marzo 2023.

Giunta, Fausto (2006): *Il diritto penale e le suggestioni del principio di precauzione*, in *Criminalia*, p. 227 ss.;

Gless, Sabine, Silverman, Emily, Weigend, Thomas (2016): *If Robots Cause Harm, Who Is to Blame: Self-Driving Cars and Criminal Liability*, in *New Criminal Law Review*, p. 412 ss.

Guidotti, Riccardo e al. (2018), *A Survey of Methods for Explaining Black Box Models*, in 51 *ACM Computing Surveys*, p. 1 ss.

Hallevy, Gabriel (2010a): *"I, Robot – I, Criminal"—When Science Fiction Becomes Reality: Legal Liability of AI Robots committing Criminal Offenses*, in 22 *Syracuse Sci. & Tech. L. Rep. 1*, p. 1 ss.

Hallevy, Gabriel (2010b): *The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control*, in 4 *Akron Intellectual Property Journal*, p. 171 ss.

Hallevy, Gabriel (2015): *Liability for Crimes Involving Artificial Intelligence Systems*, Springer.

Herzog, Felix (2004): *Società del rischio, diritto penale del rischio, regolazione del rischio*, in Stortoni, Luigi, Foffani, Luigi (a cura di), *Critica e giustificazione del diritto penale nel cambio di secolo. L'analisi critica della Scuola di Francoforte*, Giuffrè, 2004, p. 357 ss.;

Hu, Ying (2019): *Robot Criminals*, in 52 *U. Mich. J. L. Reform*, p. 487 ss.

ID R&D (2022): ID R&D, *Human or Machine: AI Proves Best at Spotting Biometric Attacks*, 2022.

Italiano, Giuseppe F. (2022), *Intelligenza artificiale: dalla ricerca scientifica alle sue applicazioni. Una introduzione di contesto*, in Pajno, Alessandro, e al. (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. 1, il Mulino, 2022.

Karnow, Curtis E.A. (1996): *Liability for Distributed Artificial Intelligence*, in 11 *Berkeley Technol. Law J.*, p. 147 ss.

Karnow, Curtis E.A. (2016): *The application of traditional tort law*, in Calo, Ryan e al. (eds.), *Robot Law*, Edward Elgar Publishing, p. 51 ss.

Kayser-Bril, Nicolas (2021): *European Council and Commission in agreement to narrow the scope of the AI Act*, in *Algorithm Watch*, 24 novembre 2021.

Khatsenkova, Sophia, Huet, Nathalie (2023): *Mayor mulls defamation lawsuit after ChatGPT falsely claims he was jailed for bribery*, in *Euronews.next*, 8 aprile 2023.

LaGioia, Francesca, Sartor, Giovanni (2020): *AI Systems Under Criminal Law: A Legal Analysis and a Regulatory Perspective*, in *Philosophy & Technology*, 33, p. 433 ss.

Lehouillier, Trevor e al. (2013), *The Use of Event Data Recorders in the Analysis of Unintended Acceleration Incidents*, testo della relazione tenuta alla *23e Conférence canadienne multidisciplinaire sur la sécurité routière Montréal, Québec, 26-29 mai 2013*.

Lemley, Mark A., Casey, Bryan (2019): *Remedies for Robots*, in 86 *University of Chicago Law Review*, p. 1311.

Lipton, Zachary C. (2018): *The Mythos of Model Interpretability*, in 16 *Queue*, May-June 2018.

Lohsse, Sebastian e al. (2019, eds): *Liability for Artificial Intelligence and the Internet of Things*, Nomos, Baden-Baden.

Magro, Maria Beatrice (2019): Robot, cyborg *e intelligenze artificiali*, in Cadoppi, Alberto e al. (a cura di), *Cybercrime*, Utet.

Magro, Maria Beatrice (2020): *Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica*, in *Leg. pen.*, 10 maggio 2020.

Maldonato, Lucia (2021): *Il crimine ambientale come crimine delle corporations: cooperazione pubblico-privato e responsabilità indipendente dell'ente*, in *Riv. trim. dir. pen. econ.*, fasc. 3-4, p. 504 ss.

Manes, Vittorio (2020): *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in Ruffolo, Ugo (a cura di), *Intelligenza artificiale – Il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020, pubblicato anche in *disCrimen*, 15 maggio 2020.

Mantovani, Ferrando (1988): (voce) *Colpa*, in *Dig. pen.*, II, Utet.

Marinucci, Giorgio (1965): *La colpa per inosservanza di leggi*, Giuffrè.

Marinucci, Giorgio (2005): *Innovazioni tecnologiche e scoperte scientifiche: costi e tempi di adeguamento delle regole di diligenza*, in *Riv. it. dir. proc. pen.*, fasc. 1, p. 29 ss.

Marinucci, Giorgio, Dolcini, Emilio (2001): *Corso di diritto penale*, Giuffrè, III ed.

Massaro, Antonella (2011): *Principio di precauzione e diritto penale:* nihil novi sub sole?, in *Dir. pen. cont.*, 2011.

Matthias, Andreas (2004): *The responsibility gap: Ascribing responsibility for the actions of learning automata*, in *Ethics and Information Technology*, vol. 6, p. 175 ss.

McKinsey & Company (2015): *Ten ways autonomous driving could redefine the automotive world*, 1 giugno 2015.

Militello, Vincenzo (1988): *Rischio e responsabilità penale*, Giuffrè.

Millar, Jason, Kerr, Ian (2016): *Delegation, relinquishment, and responsibility: The prospect of expert robots*, in Calo, Ryan e al. (eds.), *Robot Law*, Edward Elgar Publishing, p. 102 ss.

Mulligan, Christina (2018): *Revenge Against Robots*, in 69 *South Carolina Law Review*, p. 579 ss.

Osborne, Cailean (2021): *The European Commission's Artificial Intelligence Act highlights the need for an effective AI assurance ecosystem*, in *Centre for Data Ethics and Innovation Blog*, 11 maggio 2021.

Palazzo, Francesco (2011): *Morti da amianto e colpa penale*, in *Dir. pen. proc.*, n. 2, p. 185 ss.

Paliero, Carlo Enrico (1994): *L'autunno del patriarca. Rinnovamento o trasmutazione del diritto penale dei codici*, in *Riv. it. dir. proc. pen.*, p. 1220 ss.

Palmerini, Erica (2020): *Soggettività e agenti artificiali: una soluzione in cerca di un problema?*, in *Oss. dir. civ. comm.*, fasc. 2, p. 445 ss.

Paolucci, Federica (2022): *Algoritmi e intelligenza artificiale alla ricerca di una definizione: l'esegesi del Consiglio di Stato, alla luce dell'AI Act*, in *Quest. giust.*, 8 aprile 2022.

Panattoni, Beatrice (2021): *Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'autonomia artificiale*, in *Dir. inf.*, fasc. 1, p. 317 ss.

Picotti, Luca (2022): *I primi vent'anni della Convenzione di Budapest nell'ottica sostanzialista e la mancata ratifica ed esecuzione del Primo Protocollo addizionale contro il razzismo e la xenofobia*, in *Dir. pen. proc.*, n. 8, p. 1028 ss.

Piergallini, Carlo (2004): *Danno da prodotto e responsabilità penale. Profili dogmatici e politico-criminali*, Giuffrè, 2004.

Piergallini, Carlo (2005): *Il paradigma della colpa nell'età del rischio: prove di resistenza del tipo*, in *Riv. it. dir. proc. pen.*, p. 1684 ss.

Piergallini (2017): (voce) *Colpa (diritto penale)*, in *Enc. dir.*, Annali, X.

Piergallini, Carlo (2020): *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*, in *Riv. it. dir. proc. pen.*, n. 4, p. 1745 ss.

Piva, Daniele (2022): Machina discere, (deinde) delinquere et puniri potest, in Giordano, Rosaria, e al. (a cura di), *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Giuffrè.

Pulitanò, Domenico (2008): *Colpa ed evoluzione del sapere scientifico*, in *Dir. pen. proc.*, p. 647 ss.

Rahwan, Iyad, e al. (2019): *Machine Behaviour*, in *Nature*, n. 568, p. 477 ss.

Ruffolo, Ugo (2022): Artificial Intelligence *e responsabilità. «Persona elettronica» e teoria dell'illecito*, in Pajno, Alessandro, e al. (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. 1, il Mulino.

Ruffolo, Ugo, Amidei, Andrea (2022): *La regolazione* ex ante *dell'intelligenza artificiale tra gestione del rischio* by design*, strumenti di certificazione preventive e «autodisciplina» di settore*, in Pajno, Alessandro, e al. (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. 1, il Mulino.

Ruga Riva, Carlo (2006): *Principio di precauzione e diritto penale. Genesi e contenuto della colpa in contesti di incertezza scientifica*, in Dolcini, Emilio, Paliero, Carlo Enrico (a cura di) *Studi in onore di Giorgio Marinucci*, II, Giuffrè, 2006, p. 1743 ss.

Russell, Stuart J., Norvig, Peter (2020): *Artificial Intelligence: A Modern Approach*, Pearson College Div., 4th ed., 2020.

Salvadori, Ivan (2021): *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. proc. pen.*, n. 1, p. 83 ss.;

Scopino, Gregory (2020): *Algo Bots and the Law: Technology, Automation, and the Regulation of Futures and Other Derivatives*, Cambridge University Press.

Selbst, Andrew D. (2020): *Negligence and AI's Human Users*, in 100 *Boston University Law Review*, p. 1315 ss.

Selbst, Andrew D., Barocas, Solon (2018): *The Intuitive Appeal of Explainable Machines*, in 87 *Fordham Law Review*, p. 1085 ss.

Silva Sánchez, Jesús María (2004): *L'espansione del diritto penale. Aspetti della politica criminale nelle società postindustriali*, Giuffrè, 2004 (ed. spagn. 1999);

Simmler, Monika, Markwalder, Nora (2019): *Guilty Robots? – Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence*, in *Crim. Law Forum*, n. 30, p. 1 ss.

Sovrano, Francesco e al. (2022), *Metrics, Explainability and the European AI Act Proposal*, in *J*, n. 5, p. 126 ss.

Sparrow, Robert (2007): *Killer robots*, in *J. Appl. Philos.*, vol. 24, p. 62 ss.

Spindler, Gerald (2019): *User liability and strict liability in the Internet of Things and for Robots*, in Lohsse, Sebastian e al. (eds.), *Liability for Artificial Intelligence and the Internet of Things*, Nomos, Baden-Baden.

Stella, Federico (2003): *Giustizia e modernità. La protezione dell'innocente e la tutela delle vittime*, Giuffrè, III ed.

Veneziani, Paolo (2003): *Regole cautelari "proprie" ed "improprie" nella prospettiva delle fattispecie colpose causalmente orientate*, Cedam.

Wagner, Gerhard (2019): *Robot, Inc.: Personhood for Autonomous Systems?*, in 88 *Fordham Law Review*, 2019, p. 591 ss.

Wallach, Wendell, Allen, Colin (2009): *Moral Machines: Teaching Robots Right from Wrong*, Oxford University Press

Wischmeyer, Thomas (2020): *Artificial Intelligence and Transparency: Opening the Black Box*, in Wischmeyer, Thomas, Rademacher, Timo (eds.), *Regulating Artificial Intelligence*, Cham, 2020.

Zirulia, Stefano (2018): *Esposizione a sostanze tossiche e responsabilità penale*, Giuffrè.

AI and Criminal Liability. Algorithmic Error and Human Negligence in the Context of the European Regulation

IA e responsabilità penale. Errore dell'algoritmo e colpa della persona fisica nel contesto della regolamentazione europea

IA y Responsabilidad Penal. Error de algoritmo y culpa de la persona natural en el contexto de la regulación europea

Marta Giuca
Ph.D. in Criminal Law, University of Catania
marta.giuca@unict.it

Artificial Intelligence, EU Law | Intelligenza artificiale, Diritto UE | Inteligencia artificial, Derecho UE

Abstracts

Drawing on European interventions in the field of Artificial Intelligence (in particular the Proposal for a Regulation of April 2021 (AI Act)), the article reflects on the apportionment of responsibilities between the manufacturer and the user of AI systems when a negligence offence occurs due to an error of the algorithm, defined here as "artificial negligence". It is argued that the manufacturer's liability could be assessed for non-compliance with rules established by written norms (case of "specific negligence") or through the reasonable man standard (case of "generic negligence"). For this purpose, a notion of "artificial diligence" is given since it is argued that the reasonable manufacturer parameter will be modelled on the product that complies with the characteristics specified by law and is safe at the same time. Then, discussing the hypothesis of artificial negligence, a distinction between cases of errors that are ex ante foreseeable and unforeseeable is offered in order to address the manufacturer's liability and to define his duty of care. As far as the user is concerned, the duty of information, vigilance and to intervene are investigated, to conclude that compliance with the duty of "human oversight" in the assessment of negligence should be ascertained *in concreto*, in order to evaluate whether to exclude culpability or even the objective dimension of negligence, according to the reasonable man standard.

Traendo spunto dagli interventi europei in tema di Intelligenza Artificiale (in particolare la Proposta di Regolamento dell'aprile 2021, (AI Act)), il contributo offre una riflessione sulla riparto delle responsabilità tra il produttore e l'utente di sistemi di IA, allorché sia commesso un reato colposo di evento a causa di un errore dell'algoritmo, ipotesi qui definita come "negligenza artificiale". Si sostiene che la responsabilità del produttore può essere fondata sull'inosservanza di regole scritte (ipotesi di colpa specifica) o stabilita attraverso il parametro del produttore modello (ipotesi di colpa generica). A tal fine, viene fornita una nozione di "diligenza artificiale", in quanto si sostiene che il parametro del produttore modello sarà calibrato sulle caratteristiche del prodotto che rispetta i requisiti prescritti dalla legge ed è allo stesso tempo sicuro. In seguito, discutendo l'ipotesi di negligenza artificiale, si propone una distinzione tra casi di errori ex ante prevedibili e imprevedibili, al fine di affrontare la responsabilità del produttore e definire il contenuto del suo dovere di diligenza. Quanto alla posizione dell'utente, si indagano i doveri di informazione, vigilanza e intervento, per concludere che l'adempimento del dovere di "sorveglianza umana" nella valutazione della responsabilità colposa deve essere accertato in concreto, al fine di valutare l'opportunità di escludere la colpevolezza o anche la dimensione oggettiva della colpa, secondo lo standard dell'agente modello..

Basándose en las intervenciones europeas en el ámbito de la Inteligencia Artificial (en particular, la Propuesta de Reglamento de abril de 2021 (AI Act)), el artículo reflexiona sobre la división de la responsabilidad entre el productor y el usuario de sistemas de IA cuando se produce un delito imprudente debido a un error del algoritmo, aquí definido como "negligencia artificial". Se argumenta que la responsabilidad del productor podría fundarse en el incumplimiento de las normas establecidas por estándares específicos de conducta ("negligencia específica") o mediante el estándar de la persona razonable ("negligencia general"). Para ello, se aporta una noción de "diligencia artificial", en la que se sostiene que el estándar del productor razonable tendrá como modelo el producto que cumple las características especificadas por la ley y que, al mismo tiempo, es seguro. A continuación, discutiendo la hipótesis de la negligencia artificial, se propone una distinción entre los casos de error que eran previsibles desde una perspectiva *ex ante*, y aquellos que eran imprevisibles, con el fin de abordar la responsabilidad del productor y definir su deber de diligencia. Por parte del usuario, se investigan los deberes de información, vigilancia e intervención, para concluir que el cumplimiento del deber de "vigilancia humana" en la apreciación de la negligencia debe constatarse *in concreto*.

Sommario

1. Introduction.

That of AI is a topic that draws attention on the relationship between law and technology. The legal issues that emerge are many, from the problem of regulating the production of AI systems, which is called into a confrontation with the right of free economic initiative, to that of transparency, which clashes with intellectual property rights protected by secrecy, stretching onto the issue of liability. What can be seen, in the face of these technological innovations, is a 'thirst for law', now that man has created a new world, he cannot escape what is implied by the creative act of a new reality: ordering it and giving it laws[1].

In the European context, the reaction to the new technological phenomenon of AI was quite immediate[2]. The institutions quickly realised the importance of dealing with a sector that offers new opportunities but also brings with it new risks[3].

Certainly, the EU already has a solid regulatory framework that lends itself to regulating certain aspects of new technologies[4]. Despite such legislative apparatus, the damage caused by AI systems has been considered a field that needs regulatory intervention, which would take into account the characteristics of the new technological products. Indeed, AI applications present themselves as *complex, opaque, open, autonomous, unpredictable systems, in a dependent relationship with data and vulnerable*[5]. It follows that these peculiarities open up new scenarios in terms of liability for damage caused by AI systems, before which the European legislator certainly did not remain silent[6]. As it was observed, the European approach to AI is a "regulatory" one, whose purpose is to establish norms for new technological phenomena, with the ambition to render the European one a model to be imitated by other geopolitical regions[7].

In general, the idea that emerges from the European Institutions' interventions on the topic of AI is that of regulation both upstream, aimed at guiding production, and downstream, aimed at protecting those who suffer damage. Such an approach is fully in line with the dual role of liability, which must certainly guarantee fair compensation to those who suffer damage, but at the same time must constitute an incentive to avoid causing damage or harm *ab origine*[8].

It has rightly been observed that the issue of liability in the field of AI is perhaps the most

[1] Cotta (1968), p. 82.

[2] Already in 2017 the European Parliament adopted the Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), *www.europarl.europa.eu*.

[3] *Report from the Expert Group on Liability and New Technologies - New Technologies Formation*, *Liability for AI and other emerging technologies,* (European Commission 2019), p. 32. For a Critical discussion of such a Report, see Bertolini, Episcopo (2021), 644-659.

[4] C*ommunication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions "Building Trust in Human-Centric Artificial Intelligence"* COM(2019) 168 final, 8.04.2019, par. 2, p. 2. In particular, data protection, by design, is guaranteed by the General Data Protection Regulation (GDPR); as for non-personal data, their free movement and processing in Europe is guaranteed by the Regulation on the free movement of Data (Regulation (UE) 2018/1807, 14 November 2018, on the free movement within the EU for non-personal data) and finally, the Regulation on cybersecurity (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013) helps to create a climate of confidence in the operations carried out online.

[5] *Report from the Expert Group on Liability and New Technologies*, p. 32 et seq., but also COM (2020) 64 final del 19.02.2020, which refers to the document of the High-Level Expert Group.

[6] The Resolution of the European Parliament of 2017 was then followed by some Communication from the European Commission (see, for example, *Artificial Intelligence for Europe,* COM (2018) 237 final, 25 April 2018; *Coordinated Plan on AI,* COM (2018) 795 final, 7 December 2018; COM(2019) 168 final, 8 April 2019), the White Paper of the European Commission "*An European approach to excellence and trust"* of 19 February 2020, the *European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence* (2020/2014(INL)), the *European Commission Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, of April 202, COM/2021/206 final, and the *Commission Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence*, of September 2022. For an in-depth analysis of the AI Act Proposal, see Camardi (ed.) (2022).

[7] Is it the so-called "Brussels effect", *see* Bradford (2020).

[8] See par. A., *Motion for a European Parliament Resolution with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)).*

delicate from a legal point of view since it also involves profiles linked to economic growth and the development of research[9]. And indeed, the AI sector is a tester for the coexistence of law and technology, a coexistence in which limits must be drawn not only on technology by law, but also on law by technology. A balance must therefore be found between regulation and industrialization. New rules must not constitute an obstacle in developing and using new technologies but should rather serve as a means of orienting the production towards the pursuit of improving people's living conditions, providing that, in some cases, AI systems can even reduce the exposure to the danger of interests protected by law[10].

Therefore, the unprecedented scenario of AI systems opens the field to new areas of regulation, but not necessarily to an entirely new regulation. New laws do not always appear indispensable in the face of a new phenomenon. This is the direction taken by the debate in the European institutions on liability for AI systems, which always comes down to recognising the relevance of the regulations already in place, especially those concerning defective products, which need to be complemented by new regulations based on the new characteristics of AI products[11].

In line with such an approach, this article explores the field of criminal liability for the production and the use of AI systems, applying the traditional categories of criminal law, leaving apart, at least in such a context, the idea of criminal liability of the AI system, in order to reflect on possible subjects of intervention for national legislators.

2. The field of investigation: criminal negligence.

In dealing with the categories of "the criminal law of the result" in the face of the new risks created by the production and use of intelligent systems, the investigation plan chosen here is that of negligent offence, which is the privileged field of application of studies on the criminal law of risk[12].

The renewed vitality of the negligent offence model has definitively asserted itself with the transition to the risk society and has found further confirmation in this current historical era which is characterized by what doctrine often refers to as the fourth revolution[13], a time in which man is no longer the only "informational organism", but is assisted in his activities by intelligent artificial agents to perform certain tasks and duties.

In this context, the positions that come to the fore are those of the manufacturer and the user and the subject of product damage knows a new extension that pushes scholars to go beyond the traditional 'human perspective' of approaching the subject and to "measure themselves against the performance of the *new entry AI*"[14]. If the actions in which an AI system is involved become criminally relevant, they will be so mainly in the guise of the negligent offence, commissive and omissive, on which this investigation will focus. Whereas, it is likely that the issues raised by an intentional act on the part of the agent, be it the producer or the user of the intelligent system, will not differ from those that have traditionally been addressed in the study of intentional offences[15] at least in case of a perfect correspondence between the

[9] Bifulco (2018), p. 389.
[10] Ruffolo, Al Mureden (2019), 7, p. 1704 et seq. The Authors refer to driverless cars, which would guarantee higher security standards, significantly reduce road traffic accidents, and would ensure other virtuous effects, such as greater access to traffic also for disabled people.
[11] An example of such an approach is the product liability regime, since, as stated by the Commission, "The Product Liability Directive covers producer's no-fault liability for defective products, leading to compensation for certain types of damages, mainly suffered by individuals", whereas the recent proposal for a Directive "covers national liability claims mainly based on the fault of any person with a view of compensating any type of damage and any type of victim", so that the two legislative interventions "complement one another to form an overall effective civil liability system" (See the AI Liability Directive, p. 3).
[12] But it is well known that reflections on permissible or appropriate risk also apply to intentional offences, on the point. See Militello (1988), p. 55, p. 205 et seq.; Donini (2010), p. 646 et seq. On the topic of AI and criminal negligence offences, see for example Beck (2016), 138-143; *Id.* (2017), 227-252.
[13] Floridi (2017a), p. 99 et seq. The philosopher identifies the first revolution in the discovery of heliocentrism by Nicholas Copernicus, with the publication of his treatise *Sulle rivoluzioni dei corpi celesti* in 1543, a moment from which man would cease to believe in his centrality, at least with reference to planet Earth. The second revolution is made to coincide with the publication of Charles Darwin's *The Origin of Species* in 1859, which pushes man to renounce his centrality in the animal world, having to confront the idea that every living species derives from common ancestors through a process of natural selection. The third revolution came with the psychoanalytic work of Freud, who disproved the idea of the mind thought of as a box that can be known simply by looking inside, showing that many of our actions are the result of the unconscious. The fourth revolution questions man as the only being unsurpassed in intelligence.
[14] Piergallini (2020), p. 1745-1774, particularly p. 1749.
[15] On the topic of intentional offence, see Gless, Silverman, Weigend (2016), p. 425, who conclude that the case does not raise particular

conduct conceived by the author and that occurred *in concreto*[16].

The case of negligent offence is different. Here, questions arise concerning the identification of objective rules of diligence on a praxeological basis or on a legal basis, with particular reference to the role of the criteria of foreseeability and avoidance of the result, and the content of the duty of care with specific regards to the position of the producer and the user. The apportionment of liability between these two figures also appears problematic, especially in the presence of the self-learning mechanisms of AI systems.

In the background remains the broader problem of balancing the performance of a dangerous but socially useful activity, such as the production of intelligent systems, and the protection of the interests threatened by it, which prompts us to question the extent of the area of "acceptable risk" (*Erlaubtes Risiko*)[17].

In production activities, the "acceptable risk" involves two kinds of responsibility: "for the type of production" and "for the mode of production"[18]. With specific regard to the producer's criminal liability for product damage, scholars have observed that this is a "*transversal" liability*, embracing both the type and the mode of production[19].

3. The position of the manufacturer.

In the context of this study, the duty of care will be addressed to the manufacturer and the user and may be a written rule, thus setting the groundwork for the assertion of "specific negligence", for which it is unnecessary to establish the violation of the duty of care according to the reasonable person parameter[20].

The tendency to establish written rules of conduct is more and more pronounced in the technological age, while unwritten rules are characteristic of "more technologically tranquil and restful eras"[21]. This trend is not exempt from the context of the production of AI technologies, which already has European regulations that set the criteria for the production chain.

The proposal of the AI Act of April 2021[22] establishes rules regulating the production of high-risk AI systems with a precautionary purpose, and thus intended for producers. They are contained in Chapters II and III of Title I. However, as this is only a proposal for a regulation, at present such rules are not yet in force.

Chapter II, in setting out the "requirements for high-risk AI systems", already identifies quite specific obligations addressed to the producer. For instance, it is stipulated that high-risk intelligent products must be equipped with risk management systems for the entire life cycle of the system (Art. 9), which allows not only to identify known and foreseeable risks but also to take appropriate measures to manage them (para. 2 (d)). The manufacturer is then obliged to eliminate or reduce risks by means of adequate design and development (para. 4(a)) and to put in place measures to mitigate and control risks that cannot be eliminated (para. 4(b)). Hence, according to the meaning of this provision, it would seem that the European legislator requires the manufacturer to introduce into the system forms of emergency control of control-

problems; the conclusion, among others, is also shared by Vagliasindi (2021), p. 375-76; Salvadori (2021), p. 100; Borsari (2019) p. 264; in this regard, according to Basile (2019), "We must, in short, prepare ourselves for an era in which the commission of crimes with the tool of AI could become very frequent and incisive, also because of the increased vulnerability of certain aspects of human life connected to uses of artificial intelligence" and therefore the A. asks "Is it necessary, then, to field new criminal offences (or to remodel existing ones) in order to make them applicable to the implementation of criminal conduct through the AI tool, thus offering protection to legal assets also from this new source of attacks?", pp. 26-27.

[16] On the contrary, a problematic scenario could be that of intentional criminal use of the AI system with an unexpected development of the factual dynamic.

[17] Fundamental works on the topic include Preuss (1974); Roeder, (1962); Hilgendorf (1993); Prittwitz (1993). In the Italian doctrine, Militello, (1988); Forti (1990), pp. 250 et seq.; Gallo (1960) p. 638; Marinucci (1965), p. 210 et seq.; Donini (1989), p. 588; Consulich (2021), p. 1102 et seq.

[18] Bricola (1978), pp. 75 et seq..

[19] Piergallini (2004), p. 46.

[20] The specific negligence is so-called since the judgment on foreseeability and avoidance is established by a written rule laid down by the legislator, the authority, or even a private person (e.g. the owner of a firm), and this makes it unnecessary to establish the violation of the duty of care according to the reasonable person parameter. See *ex multis,* Bartoli (2021) pp. 519 et seq.; Canestrari (2013), p. 144; Mantovani (1988), p. 306.

[21] Mantovani (1988), p. 306.

[22] The Commission's proposal of the EU AI Act will become law once both the Council and the European Parliament agree on a common version of the text. At the time of writing this contribution, the European Parliament's Internal Market Committee and the Civil Liberties Committee adopted a draft negotiating mandate on the AI Act proposal (*www.europarl.europa.eu*).

lable risks and forms of mitigation of uncontrollable risks. In this way, indications are given on the characteristics of the product that will then be launched on the market, which must always be accompanied by a sort of "first aid kit" provided by the manufacturer to the user, useful in the event of risks arising during the use of the intelligent product[23].

Production criteria are also introduced concerning training data sets, which must meet certain quality standards (Art. 10). In addition, detailed technical documentation is required (Art. 11), and the design shall be sufficiently transparent to enable users to interpret the system's output and use it appropriately (Art. 13). High-risk systems must also be robust, *i.e.* resistant to attacks by third parties aimed at modifying their use or performance by exploiting system vulnerabilities (Art. 15(4)).

Rules on production are also contained in Chapter III. One example is the provision of a conformity assessment procedure for systems before they are placed on the market (Art. 19).

From the Proposal for a regulation emerge many rules of diligence that could be classified as second-rate, *i.e.* aimed at preventing risks and not specific events (most of the rules set out above, in my opinion, can be brought into this category, starting from Article 9 on the risk management system, then moving on to the one on data set requirements in Article 10, and concluding with those in Article 13 on transparency and interpretability of output and Article 15 on the robustness of systems), as well as rules with a monitoring purpose and rules with an administrative attitude and a precautionary purpose only in a mediated way (this is the case of the certification and conformity assessment regime).

According to the doctrine[24], such characteristics of the duty of care make necessary the ascertainment of the generic negligence in the light of the reasonable man standard. This represents a guarantee for the defendant: his negligence must be ascertained *in concreto*, according to the parameter of *homo eiusdem professionis et condicionis,* since it is not sufficient to state that he behaved contrary to a written diligence rule with generic or technical-administrative content, and which is not intended to prevent a specific result[25].

In the case of criminal product liability, the reasonable manufacturer parameter will be modelled on the product that complies with the characteristics specified by law and is safe at the same time. Then to ascertain negligence we will ask whether the product meets the standards of the defect-free product.

Having thus drawn our line of enquiry into product liability, we need to dwell on the characteristics that the intelligent product must have to be defect-free.

3.1. *Artificial diligence.*

Since intelligent systems are characterised by their ability to make decisions, we could consider that technological devices function according to a certain "behaviour", which is a response-output to a particular input[26]. This "behaviour" of the system is not left to chance, but is guided by the "information" fed into it during the design and training phase. It may be that such information coincides with social norms, *i.e.* rules of actions used to constrain the AI system's behaviour[27], in a way that guarantees the successful coexistence of multiple programs[28], so that AI systems are defined as Normative Multi-Agent Systems (NMAS)[29]. Indeed, according to normative computing theories, the system's (agent) behaviour is guided by norms, which are encoded by the designer, in an off-line design approach, or inferred from

[23] There will be negligence on the part of the developer or programmer for not providing manual intervention on the system in emergency conditions, see Salvadori (2020), p. 103.
[24] Di Giovine (2003), pp. 391 ff.
[25] However, such a conclusion is not always shared by Italian case law. It is then considered that the failure to comply with a duty of care imposed by law, regulation, order, or discipline is sufficient to prove negligence, provided that the event that occurred is attributable to the type of event that the duty of care is intended to prevent (see, *ex multis,* Cas. Pen. sez. IV, 01/12/1989, n.1501; Cass. pen. sez. IV, 08/11/2022, (ud. 08/11/2022, dep. 01/02/2023), n.4155; Cass. Pen. sez. IV, 17/05/2022, (ud. 17/05/2022, dep. 23/05/2022), n.20035).
[26] Lagioia, Sartor (2020), p. 434, arguing that "under an appropriate level of abstraction", AI systems have cognitive attitudes (intentions, beliefs, awareness) which are relevant for the realisation of *mens rea* and might be taken into consideration to appropriately react to their harmful behaviour.
[27] Hollander, Wu, (2011) , par. 1.3 and 2.18.
[28] Shoham, Tennenholtz (1992), p. 276.
[29] Andrighetto, Governatori, Noriega, der Torre (2013).

the environment through machine learning techniques, in the bottom-up approach[30].

In the case of 'agent' products, *i.e.* those that move in a real or virtual environment[31] and make decisions, as intelligent systems do, we could then say that the free-defect good is that artefact that "acts with diligence"[32]. It is clear that this diligence cannot be equated with the human one, because the machine, though intelligent, is different from humans[33]. This is an "artificial" diligence, in the sense that it derives from the knowledge that the AI system has acquired during the production phases, or from the information learned during its training or/and use. In order to establish the diligence behaviour requested from the machine, the parameter will not be that of the reasonable man, but that of the reasonable algorithm, with a consequent transition from the *homo eiusdem professionis et condicionis* to the *machina eiusdem fabricationis et condicionis.*

As a result, social norms aimed at governing an agent's behaviour may consist in rules of conduct that, just as they direct the behaviour of human agents, are intended to orient the behaviour of the artificial agent called upon to perform a function typically intended for humans. One need only think of the conduct of driving on the road or that of medical diagnosis. The driver, before driving, is required to know the rules of the highway code. Similarly, the doctor, before making a diagnosis, is required to know the rules that allow a correct diagnosis to be made and to behave in essence in the manner prescribed by the *leges artis*.

When these tasks are delegated to an AI system, such a claim to knowledge of the rules of the road and the *leges artis* is no longer addressed to the human agent, but to the artificial one[34]. It follows that, in this context, the duty of care expressed by a rule of conduct becomes a cognitive element that must be incorporated into the intelligent system through training, and that contributes to forming its knowledge[35], in line with the theory of normative multi-agent systems (NMAS).

Thus, cognitive competencies of AI systems are preconditions for criminal liability[36], as will be discussed in the following paragraphs.

3.2. *Ontological and nomological basis of artificial foreseeability.*

Some scholars argue that AI systems can achieve "situation awareness", which consists of three steps: the perception of the elements of the environment where the systems act, the comprehension of the current situation through the integration of all the disjointed information collected during the perception step, the projection of future action in the environment[37].

The process that leads to situation awareness characterises the first moment of the artificial systems' "behaviour", which ends with a decision corresponding to the output. Therefore, a distinction between an "internal behaviour", identified in the achievement of the situation

[30] Savarimuthu, Cranefield (2009), p. 6. The A. describe also a third approach defined as norm-entrepreneur. On the topic of translating law into the algorithm and the two approaches (top-down and bottom-up) ungern-sternberg (2018), p. 262.

[31] As Lagioia, Sartor (2020), p. 441, correctly underline, both AI systems with or without a physical presence (think of robots, for the former, and software agents and bots for the latter), can fulfill the conducts requirement of an *actus reus*.

[32] The idea of a standard of care referring directly to the artificial system is taken into consideration in the area of civil liability, where it is customary to refer to the so-called 'reasonable algorithm' with regard to ML algorithms, which autonomously make decisions. It is understood that the 'reasonable algorithm' standard will find a safe place of application when algorithms are recognised as having legal personality, thus being equated with humans (*see* Abbot (2020), p. 69) it is held that it may be relevant even where the algorithm is not considered an independent center of imputation, since such an assessment serves to direct the judgment on the producer's conduct towards a form of liability requiring a different burden of proof from that required in product liability; rather, the producer's diligence should be assessed in light of the reasonable algorithm standard, Chagal-Feferkorn, (2018), pp. 111-148. However, the foreign doctrine does not agree on the subject. Some opinions emphasise that it is not necessary to examine algorithmic reasonableness (diligence), given that algorithms are not comparable to human agents, but are still tools that can be used by humans, Colonna (2012); Balkin (2017), underlines that *"there is no little person inside the program"* and that algorithms take the decisions for which they have been programmed so that there is no point in examining algorithmic reasonableness independently of that of the programmers.

[33] La Vattiata (2023), p. 492.

[34] Ungern-Sternberg (2018), p. 252 with regards to the case of autonomous cars.

[35] As it emerges from the *Commission Implementing Regulation (EU) 2022/1426, of 5 August 2022, laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles cit.,* providing that automated driving systems (ADS) shall comply with traffic rules. Such knowledge of traffic rules changes according to the level of autonomy, as explained by Heikoop, Hagenzieker, Mecacci, Calvert, Santoni De Sio, Arem (2019). On the topic, see also Ungern-Sternberg (2018), p. 262.

[36] Lagioia, Sartor (2020), p. 435.

[37] *Ibidem,* p. 441.

awareness, and an "external behaviour", corresponding to the output reflected to the external environment (which in NMAS should rely on a given norm of conduct) can be made.

At this point, we could define as *diligent* the so-called *norm-abiding behaviour*[38], *i.e.* the behaviour of the system that recognises a given situation through the correct interpretation of the input data (internal behaviour) and that produces an output that conforms to that required by a norm (external behaviour). On the contrary, the behaviour of the system that errs in the interpretation of the input data, therefore it does not correctly recognise the situation in which it is called to intervene and produces an output that differs from the one that would be required by the observance of the norm, or the system that, although correctly interpreting the input data, produces an output that is inconsistent with the interpretation of the input due to a defect of internal functioning, will be *negligent*.

If the error of the system produces or contributes to the production of a risk that results in an offence to one or more legally protected interests, this negligence will be causal with respect to the production of an injury or endangerment of interests. This opens up the scenario of the producer's criminal liability for having produced and placed on the market a defective and unsafe good.

Let us consider the case of the system that errs in the interpretation of the input data, thus not correctly recognising the situation in which it is called upon to intervene, and produces an output that differs from what would normally be required. The question we must ask ourselves is first of all what factors enable the system to recognise a given piece of information and avoid producing an output that is harmful to a certain legal interest.

According to criminal scholars, *recognisability* and *avoidance* are the parameters of the probabilistic judgement of the negligent fact used for the *ex ante* verification of the adequacy between the conduct carried out and the result[39]. We can then draw on the doctrine's reflections concerning the parameter of recognisability to develop them on the terrain of the responsibility of the producer of the intelligent system.

The starting point is that under the theory of the "double measure of negligence"[40], the *Erkennensollen* relevant to the objective measure of negligence is composed of a *nomological* basis and an *ontological* one, constructed in relation to a reasonable person[41]. In particular, causal laws make up the nomological component, while the ontological one encompasses all the factual elements capable of connecting nomological knowledge to the concrete situation, in the sense that the presence of certain initial conditions enables the agent to read the concrete situation in the light of causal laws.

This scheme could be re-proposed for the intelligent agent who is required to recognise the factual situation in order to avoid reaching a decision that endangers legal interests.

We will say, then, that in a NMAS the nomological basis of recognisability consists in the duty to possess norms or models of knowledge representation that allow causal correlations between input and output to be identified, while the ontological basis is substantiated in the duty to understand the elements of the factual situation in which the system operates through the techniques of knowledge acquisition and the sensors, in case of an artificial physical system, or the instruments for tracking activities, in case of software, that make the external environment perceptible.

The nomological component of artificial recognisability requires us to dwell further on the characteristics of artificial learning. When designing AI systems, the idea of building thinking machines, mechanical brains that emulate human cognitive capacities, has been abandoned[42]. Nowadays, in fact, science is not yet able to explain how exchanges between neurons translate into 'consciousness', and consequently technology is not capable of building a system with its own thinking and creativity[43].

[38] Conte, Castelfranchi (1993), p. 40.
[39] Exner (1910), p. 137 ff.; In the Italian doctrine, see, *ex multis,* Forti (1990); Castronuovo (2009). Scholars highlight the difference between the concept of recognisability (*Erkennbarkeit*) and foreseeability (*Voraussehbarkeit*), *see,* for example, Schroeder (2003), §16, par. 128, (68)-(69); Gallo (1960), p. 638.
[40] This theory highlights the distinction between the objective element and the subjective element of negligence, the first concerning the breach of the duty of care according to the standard of the reasonable agent, the latter dealing with the personal capabilities of the agent and the specific circumstances of the case. See, for example, in the traditional German doctrine, Hippel (1908), p. 568 et seq.; Engisch (1995), p. 349 et seq.; Jescheck, Weigend (1996), p. 561 et seq.; among the Italian Authors, see De Francesco (1977-78), pp. 275 et seq.
[41] Forti (1990), p. 211 et seq., 233.
[42] For a clear explanation of the technique of machine learning, see Searle (1990), p. 26-32.
[43] Amato (2020), p. 86.

The machine's lack of reasoning capacity means that it is not able to understand the meaning of a piece of data, rather it merely establishes a correlation[44], associating the data with a certain result that may consist of a behaviour to be adopted. For example, the algorithm learns to recognise the 'stop' signal through the data fed into the system and the instructions given by the trainer; however, this will not be sufficient to command the autonomous car to drive: the algorithm will also need to be instructed to stop as soon as it recognises the signal in question[45]. A correlation is then established between the input (the 'stop' signal) and the output (the vehicle's stopping behaviour), and to achieve such a result the algorithm must be 'fed' not only with data but also with norms describing behavioural response practices to the input classification. Stopping in front of a stop signal will thus be achieved without the system understanding the reasons for such a behavioural command. Therefore, the system is unable to develop argumentative reasoning as a human brain does. Machines are not required critical thinking, they are required to work properly[46].

I do not think that this can be totally contradicted by the ability of AI systems to acquire 'situation awareness'. After all, the notion of 'situation awareness' does not include, nor is identifiable with that of 'situation comprehension'. Being aware of something means "knowing that something exists, or having knowledge or experience of a particular thing", while comprehension implies "understanding something completely", "knowing the meaning of something"[47], something that machines are not yet capable of doing. This is in line with the idea that AI is not "about coupling artificial agency and intelligent behaviour into new artefacts", but the opposite: "AI is about decoupling successful problem solving from any need to be intelligent", because "[i]t is only the outcome that matters, not whether the agent or its behaviour is intelligent. Thus, AI is not about reproducing human intelligence, it is about doing without it"[48]. AI systems have an "unconscious knowledge" that could be better defined as mere "information"[49].

All this leads us to conclude that 'artificial diligence' does not imply that the algorithm understands the meaning of the instructions given during the learning phase[50]. The direct consequence of this is that the 'thinking mind' during the operation of an AI system always remains the human one, more precisely, that of the trainer in the training phase, while in the moment of deployment, it is that of the user.

3.3. *Artificial Negligence.*

These premises on the structure of human and artificial recognisability of a factual situation are useful for the study of pathologies in the functioning of the AI system that can give rise to liability for what scholars call "AI-Crime" (AIC)[51]. We can therefore identify two main reasons that hinder perfect learning on the part of the AI system: I) faults in the moment of knowledge representation (nomological basis of machine learning) and II) faults in the moment of knowledge acquisition (ontological basis of machine learning), and then there are III) hybrid situations, involving both (I) one and the other (II) basis of machine learning.

I) Since the representation capacity is strictly dependent on the system's programming and the settings chosen during its design, including the set of norms encoded by the designer of a normative "top-down" MAS, the defects found in the knowledge representation phase can be blamed on the producer[52]. According to the classification proposed above, these defects can be

[44] *See* Searle (1980) and Id., (1990); Gigerenzer (2022), p. 122 et seq., and p. 143 et seq.
[45] *See* Gigerenzer (2022), p. 96, and p. 102.
[46] Amato (2020), p. 90.
[47] Definitions from *dictionary.cambridge.org.*
[48] Floridi (2017b), p. 126.
[49] Faggin (2022), p. 54.
[50] See, for this purpose, the interesting example of the school bus proposed by Gigerenzer (2022), p. 100 et seq., and the reflections on the concept of consciousness proposed by Faggin (2022), pp. 128 et seq.
[51] King, Aggarwal, Taddeo, Floridi (2021), pp.195-227
[52] Consider the cases of overfitting and underfitting. If in the training phase, the system learns to recognise the input data, providing an output that corresponds perfectly to expectations, the result will not be satisfactory, because the model is not able to generalise well and will produce errors if fed with data other than those entered in the training phase. In the case of underfitting, the model will present inaccuracies already in the training phase, because it is unable to recognise the input data, and it will continue to err even when it is faced with data other than those used at the time of learning.

classified as construction or manufacturing defects, depending on the fact that they affect the entire production series or only some elements of it.

II) The case of defects at the time of knowledge acquisition is different. An erroneous acquisition of external data may depend, for example, on a sensor malfunction caused by a production defect (being then construction or manufacturing defects[53]), imputable to the manufacturer, or by poor maintenance attributable to the user.

III) Then there are hybrid situations or ones that are more difficult to classify, in which the damaging event is the result of a mixture of limitations (and not defects) of the system found in the ontological and nomological phase. This is the case if we imagine that an incomplete (and not erroneous) acquisition of knowledge can be determined by the peculiarities of the concrete case, where circumstances arise that make the factual situation completely unique and unpredictable and such as to be characterised by an *eccentric risk*. Just think of the case of the sudden crossing of a pedestrian on a street at night that could not be perceived in time by the sensor[54]. Or the case in which a certain piece of data is perceived by the sensors, therefore acquired, but the system is then unable to process it because the unique character of the situation made it unforeseeable by the producer, who therefore did not 'train' the system to recognise such a situation[55].

To avoid flaws of this kind in the knowledge representation and acquisition phase, the producer should be required during the designing or training stage to describe all possible situations of risk exposure of legal interest, a goal that is difficult to achieve[56] because it is impossible to predict the factual details of every single situation in which the system will operate[57]. It is impossible to predict the future.

This, moreover, is in line with the idea that the 'warning signals' that make a certain danger recognisable "must be seen, not foreseen; they are a matter of detection, not of foresight" and that recognisability is of a reconnaissance nature and not of an investigative one, in that the agent is not required to explore all factors that make the offence abstractly possible[58].

Such statements seem to be confirmed by the recent *Commission Implementing Regulation (EU) 2022/1426, of 5 August 2022, laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles*. Annex II provides the *Performance requirements in different traffic scenarios*, distinguishing among nominal, critical and failure scenarios. In the case of critical traffic scenarios, it is stated that the automated driving system shall be able to perform the dynamic driving task for *all reasonably foreseeable critical traffic scenarios* in the operational design domain[59]. It follows that the manufacturer's duty of care does not comprehend traffic scenarios which are not reasonably foreseeable, therefore *ex ante* unpredictable[60].

The inexistence of such a demand on the producer becomes apparent if we move from the field of AI applied to cars to that of AI applied to medical science. Think of the case of *new medical knowledge*, in which a new virus manifests itself after a robot has been placed on the market to diagnose infectious diseases. The virus will not be recognised by the system because it is not included among the possible infections and will therefore not be diagnosed. For such

[53] The distinction is elaborated by Piergallini, (2004), p. 46 et seq.
[54] Similarly Ungern-Sternberg (2018), p. 258
[55] As observed by the Panasonic Professor of robotics at MIT, Rodney Brooks, "A lot of technologists think if you do a demo, then that's it. But scaling is what kills you". "You run into all sorts of things that didn't happen at a smaller scale" (commenting on the news of Cruise's robot cars blockade in the streets of San Francisco, reported by Marshall in Wired, Jul. 8, 2022, *www.wired.com/story/cruises-robot-car-outages*). On the issues of criminal liability and self-driving cars, see, *ex multis*, Lohmann (2016); Crane, Logue, Pilz (2017), in the Italian doctrine, Picotti (2021), 813-837; Cappellini (2019), 325-353.
[56] Faggin (2022), p. 72, refers to the case of autonomous driving, arguing that many problems can never be completely solved.
[57] As noted by Selbst (2020), p. 1324, with regards to risks correlated to driverless cars: "Autonomous vehicles will face unexpected changes: detours from road construction, drivers who break traffic laws or stop very suddenly, or other drivers misapprehending what the automated vehicle itself will do and reacting badly. Each of these will be unique in some way—the timing, the type of stimulus—such that the machine cannot possibly be trained on all of them", p. 1324. See also Ruffolo (2020), p. 165.
[58] Giunta (2019), p. 16.
[59] Annex II, par. 2.1.
[60] See Annex III, Appendix I, para. 1 describing the "Generation and classification of scenarios", providing that: "From a qualitative perspective, scenarios can be classified into Nominal/Critical/Failure and correspond to normal or emergency operation. For each of these categories, a data-based approach and a knowledge-based approach can be used to generate corresponding traffic scenarios. A knowledge-based approach utilizes expert knowledge to identify hazardous events systematically and create scenarios. A data-based approach utilizes the available data to identify and classify occurring scenarios. Scenarios shall be derived from the ODD of the fully automated vehicle". These scenarios, once identified, must be assessed through simulation or physical testing (par. 5).

an algorithmic limitation, no blame can be laid at the door of the manufacturer, since the discovery of the virus is subsequent to the programming of the algorithm. On the other hand, a fault may be found if, following the discovery of the virus, the manufacturer does not provide a software update that covers the new pathology[61].

We have thus drawn an initial distinction between situations in which it is possible to provide an *ex ante* description in terms of danger, and situations in which such an *ex ante* description of danger is nearly impossible (case of the *eccentric risk* and *new medical knowledge*), since they are related to concrete dynamics that are difficult to foresee, therefore not imagined in the algorithm's training phase and proposed as examples of the training set.

It should also be considered at this point that the unpredictability of the output result may be, not much due to the inability to condense all the concrete variables in algorithmic programming, but rather to the evolution of the algorithm as a result of self-learning during the utilisation phase[62] (*self-learning* case). Such circumstances are usually defined as "emergent behaviour"[63], since the artificial agent acts beyond the original expectation. That is, while the tests at the design stage reveal a relatively simple behaviour, during its deployment the AI system acts in a more sophisticated way, and might even misalign his conduct with the original design, with possible criminal implications[64].

The emergent behaviour could also result from the interaction among AI systems through cloud computing, a technology that brings together AI systems operating in different environments and leads to an exponential increase in initial knowledge[65].

In all these cases, the knowledge implementation may lead to decision outcomes that differ from those assessed during the manufacturer's validation tests, which are therefore unpredictable[66], with the result that the decision of the ML algorithm is not always attributable to the programming that preceded its release[67].

It can then be observed that "artificial negligence" does not always automatically lead to producer liability[68]. Rather, three typical situations could be identified: a) cases in which the system had to act diligently and did so; b) cases of artificial negligence in which the system did not act as expected; c) cases in which the system did not act as expected but could not have done otherwise, which we could call "temperate artificial negligence" or unattainable diligence. These options are reproduced in the summary table below.

Case a)	Diligent producer	Diligent Algorithm
Case b)	Negligent Producer	Negligent Algorithm
Case c)	Diligent Producer (Acceptable risk)	Negligent Algorithm (Unattainable diligence)

The cases of algorithmic error include the last two type-situations, but the outcomes in terms of liability will be different. If artificial negligence gives rise to producer liability (hypothesis *sub b)*), the same cannot be said for hypotheses of the third type, *i.e.* for cases in which the producer, on the basis of the technical-scientific knowledge available, is unable to design and train the algorithm to cope with the concrete situation in the best way possible so as to avoid a certain risk (cases of *eccentric risk, new medical knowledge* and *self-learning*). This is a margin of risk that the law tolerates when it authorises an activity of production of goods in which the zero margin of error does not exist[69], because the error is inherent in deci-

[61] Chagal-Feferkorn (2018), p. 136.
[62] Hubbard (2014), p. 1851.
[63] *Ibidem;* King, Aggarwal, Taddeo, Floridi, (2021), p. 6.
[64] King, Aggarwal, Taddeo, Floridi, (2021), p. 6.
[65] Borsari (2019), p. 265.; Severino (2020), p. 533; Hubbard (2014), p. 1851, notes that this leads to considerable probations difficulties at trial.
[66] Chagal-Feferkorn (2018), p. 133, emphasises how complexity increases if one considers that many machine learning algorithms improve their knowledge through interactions with the network, as they are online-based (also p. 135 on this point). Furthermore, the author notes that the programmer could certainly set limits to the self-learning capacity, and insert a data selection mechanism, as well as subject any changes to the algorithm's decision-making process to its pre-approval. Nonetheless, this last characteristic could represent an impediment to the algorithm's functionality and usefulness: think of the repercussions such a system would have on self-driving cars, which would cease to function and be usable if they had to wait for the programmer's approval every time they were confronted with new situations (*ibidem,* p. 134).
[67] Cappellini (2022), p. 9.
[68] Borsari (2019), p. 265.
[69] As noted by Selbst (2020), p. 1331: "Because AI will not prevent all accidents, the promise of AI is to reduce—not eradicate—errors. Thus,

sion-making systems that proceed by correlations and generalisations from a set of input data to produce an output[70]. We are therefore faced with the area of *permissible or acceptable risk*[71], in which the producer-agent is not liable for negligence with regard to the damage that could be *in abstracto* foreseeable, but occurred despite the faithful observance of technical rules[72], and which strikes a balance between the opposing needs to protect the threatened legal interests and to carry out useful but inherently dangerous activities, identified by grading the intensity of protection of the exposed protected legal interests according to their value[73].

To hold the manufacturer liable in such cases, it would mean, for the legal system, to contradict itself, on the one hand, authorising the production of high-risk AI systems and, on the other hand, imputing to the manufacturer any foreseeable harmful consequences (if one considers that AI systems based on ML techniques are not by their very nature zero-risk systems) and avoidable only by refraining from the risky activity.

Of course, the conclusion is different in the case of a legislative intervention aimed at criminalizing endangerment, therefore punishing conduct which is not linked to a result, with the consequence of anticipating criminal usage[74]. In any case, it should not be forgotten that the exclusion of the manufacturer's criminal liability is not an obstacle to the application of other sanctions that do not have a criminal nature, but that can be effective in guaranteeing the protection of the victim.

I have therefore emphasised here how, from the point of view of traditional categories of negligent crime, the impossibility of avoiding the occurrence of the negligent act is already relevant in the context of the objective duty of care if the conduct required from the producer in order to avoid the situation of damage or danger falls outside the compendium of duties outlined in the light of the *Maßfigur* instead of the concrete agent. Moreover, the response that we have imagined on the part of the legal system in these cases would be the same as that which occurs when other professional figures, such as doctors, are involved. Just as the duty to save a terminally ill person is not imposed on the doctor by law because there is no treatment that can avoid the inauspicious outcome, neither can the duty be imposed on the manufacturer to produce a system that does not realise risks for which no technology exists that can avoid them.

What is already unattainable on the level of the manufacturer's duty of care, *e.g.* the prediction of the individual and peculiar concrete case when training the system, may however leave room for a claim of a duty of care from the human agent. That is why we must now analyse the position of the user and the content of the duty of care addressed to him/her so that the table we have drawn above can be enriched with a further column, the one describing the position of the user.

4. The position of the user.

The analysis of duties of care and their respective holders in the context of intelligent product damage must at this point turn to the figure of the user.

One of the first observations focuses on the fact that the offence invoking the remedy offered by criminal law will reasonably take place during the user's use of the AI system. It is then precisely from the context of the use of the intelligent product that the investigation of the user's position must begin with observing how the use of the product implies the establishment of a "relationship" between the user and the AI system. Together with what has already been defined as "artificial diligence", special concern must also be given to the human diligence of the user, which has different contents.

when AI is used, there will still be some errors that result in harm". See also Gless *et al.* (2016), p. 426.

[70] Such a feature is taken into consideration in the European Commission's AI Act proposal when stating that a risk management system shall be established, implemented, documented, and maintained in relation to high-risk AI systems (art. 9 (1)). It is then requested the adoption of suitable risk management measures (2 (d)) which "shall be such that any residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is judged acceptable, provided that the high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse" (4).

[71] Severino (2020), p. 536

[72] Mantovani (1988), p. 311, on the acceptable risk.

[73] Forti (1990), p. 459 et seq.

[74] Consulich (2022), p. 1051.

4.1. *Duty of information.*

The user's duty of care consists first and foremost of information obligations.

Negligence due to 'failure to inform' naturally presupposes the existence of an apparatus of rules capable of guiding the agent's behaviour in the face of a dangerous situation. Well then, in the context of the activities of production and use of goods, this apparatus of rules may include the conditions of use of the product, even an intelligent one. What follows is quite obviously a reflection on the role that negligence for violation of duties of information has in the panorama of intelligent systems.

As the European approach to AI teaches us, for regulatory purposes it is always good to distinguish between high-risk and low-risk systems, and it is within the first case that scope can be found for user negligence due to failure to inform. The user must be responsible and must realise the complexity of the system in order not to leave its use to improvisation. An indication in this sense comes once again from the proposal of the AI Act of April 2021, which states in Article 29 para. 1 that "users of high-risk AI systems shall use such systems in accordance with the instructions for use accompanying the systems". Indeed, high-risk systems must always be accompanied by instructions for use containing "concise, complete" and "clear" information that is "accessible and comprehensible to users" (Art. 13), in the absence of which negligence on the part of the manufacturer will certainly be found because the product has an information defect[75].

But on closer inspection, in addition to this specific provision concerning the user's obligation of information provided for by the draft regulation for high-risk systems, this obligation to inform can be traced more generically to the duties of social solidarity, given that the user who decides to use a high-risk system creates an area of potentially harmful effects not only for himself but also for third parties who might suffer harm[76].

The user's duty to inform is not new in the product liability scenario; the user is put in a position to comply with it as soon as he is provided with an instruction manual by the manufacturer, which should indicate the potential risks that may arise when using the good. If, therefore, this duty of information exists for all products, it is, however, true that in the case of high-risk intelligent systems, unlike for other products, the duty of information is certainly more stringent because of their greater potential for harm[77]. Moreover, it must be considered that this duty of information can also be reminded to the user by means of software update messages sent through the system by the manufacturer. The user's duty to inform is therefore also characterised by a *duty to update* him/herself, which is added to the initial duty to know the conditions of use of the product, given the capacity of these intelligent systems to "evolve". This is a condition that especially involves machine learning systems, which are subject to change as a result of self-learning.

4.2. *Duty of vigilance and duty to intervene.*

In his or her relationship with the AI system, the user acts as a "human controller", whose supervision of the system's operation is twofold. On the one hand, as a safeguard mechanism, aimed at preventing damage resulting from the system's malfunctioning and on the other hand, as a liability catalyst, *i.e.*, as the subject to whom any avoidable damage is to be attributed[78].

To this twofold function of human control correspond two duties of care: the *duty of vigi-*

[75] In this sense, *see Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022, cit.,* Annex II, para. 11 "Operating manual". On the topic of information defect, see Piergallini, (2004), p. 47-48.

[76] The duty of solidarity may have a constitutional base, as it is in the Italian legal system, where the duty of social solidarity is stated in Article 2 of the Constitution.

[77] In favour of specific training for the use of self-driving cars Barré (2022); differently Leiman (2021), p. 262, concerning the case in which the duty to inform results in "extra training" for the user of the intelligent product as compared to the user of a product without such features. In particular, the consideration is developed concerning drivers of self-driving cars, to argue that requiring them to undergo additional training beyond that required to obtain a driving license would be unreasonable since such a requirement is not imposed by law; moreover, it could lead to the consequence that a higher standard of diligence would be required of those who decide to drive cars with automated systems, which are known to be safer, and not of those who drive traditional vehicles that expose members of the public to greater risk.

[78] Piergallini (2020), p. 1757-58.

lance and the *duty of intervention*. The latter both represent fundamental requisites of the user's virtuous example and act as a mechanism for safeguarding legal interests. Should any violation be ascertained, it would result in the catalysing of liability on the person of the user[79].

Beginning with the examination of the *duty of vigilance*, it should be noted that human control seems to be unavoidable at present and the European vision of AI is also oriented in this direction. Such an approach can only be endorsed[80], also in light of the fact that "weak AI systems" have limited computational cognition, i.e. they move well within a given perimeter of knowledge but do not go beyond the thematic field of knowledge set up in the production phase[81].

Today, there are highly intelligent forms on delimited topics, nonetheless, an Artificial General Intelligence (AGI) -also called strong artificial intelligence- which is an intelligence of the same level as the human one, has not yet been created[82].

The result we draw from this in terms of the user's duties is that the duty of vigilance is made current at the time of the system's start-up and remains throughout its use.

The duty of vigilance is however susceptible to change in character, and to become a *duty to intervene*.

4.2.1. *Situations actualizing the duty to intervene.*

In order to identify the circumstances in which the user's duty of vigilance turns into a duty to intervene, we can refer to some examples to make our reflection easier.

Let us first think of a robot-doctor used to recognise only a limited number of pathologies. The diagnosis referring to one of those pathologies will certainly be more precise and will probably also arrive more quickly than a human doctor can. Nevertheless, the system will only be "intelligent" within that field (*e.g.* in the diagnosis of tumour pathologies of the eye), but once we have ruled out the occurrence of one of those pathologies, we cannot consider the patient to be healthy (the machine will not be able to recognise an infection symptomatic of a neurological pathology because that type of disease does not belong to its "knowledge").

Let us now imagine another scenario, in which diligent conduct is performed in fulfilment of a rule describing a duty of care with a very generical content. This rule could be of social source, then being the basis of generic negligence, or a written rule which makes reference to the duty of care of common experience, now for the determination of diligent conduct, now for the identification of the factual conditions for the rule's applicability[83].

Let us take as example the rule "drive carefully" taken from Article 140 of the Italian Road Traffic Act, according to which "road users must behave in such a way that they do not constitute any danger or hindrance to traffic and in such a way that road safety is in any case safeguarded"[84]. In this case, we have a written rule, nevertheless, its content is determined by reference to the social duty of care[85].

[79] Selbst (2020), p. 1345: "The human-in-the-loop aspect of the technologies that still rely on negligence law ensure that this type of wildly unexpected AI injury cannot happen, or in fact, the human would be reasonably blamed for it". The A. discusses the interesting example proposed by Lemley, Casey (2019), p. 1311 et seq. The case is that of a drone trained to reach the centre of a circle. The drone, after the first few attempts during which it received positive reinforcement for its success in the assigned task, began to behave differently: when it got close to the edge of the circle, it would suddenly move away from it. The trainers then switched him off and placed him back in the centre of the circle to start the experiment again. After various investigations, the programmers discovered that the drone had realised that if it moved away from the edge, it would somehow find itself 'teleported' to the centre of the circle, thus achieving its goal. Selbst (2020), p. 1345, then observes that if the operation of the drone had been supervised by a human being, as soon as it started to move away from the circle, the human being could have taken control of it again and prevented it from moving away from the centre.

[80] But it is worth noting the observations that the American doctrine makes on this point when it emphasises how in certain situations the need for human intervention could create additional risks over and above those that would result from a fully automated operating process that does not require human oversight at all. The example is related to the presence of the vehicle's automatic steering system, whereby it is observed that once the driver perceives the concrete possibility of an imminent collision, he might decide to take back control of the steering but intervene, due to the panic situation, in a way that aggravates the situation. It is concluded, then, that *"At some point, then, removing the human entirely from active driving may be safer than managing the "mushy middle" of shared human-machine operation"*. Smith (2017), p. 49.

[81] And this is also true in the case of self-learning machines: the algorithm will increase its knowledge but always in order to accomplish the task it has been given. If this consists of the recognition of tumour diseases of the eye, the expansion of knowledge cannot occur towards neuronal diseases for which the machine was not designed to recognise.

[82] See Searle (1990), pp. 26-32; Selbst (2020), p. 1344; Calo (2017), p. 432.

[83] See Giunta (1999), p. 92, indications on art. 140 of the Italian road traffic Act.

[84] The same principle is stated in art. R. 412-6 of the French Traffic Road Act, see www.legifrance.fr

[85] Giunta (1999), p. 92.

It is precisely its essence as a social rule, and not a legal one, that makes the rule "drive carefully" comprehensible to a human agent, who is capable of declining and framing it in its realistic scenario because he is endowed with critical capacity. Such a rule will be, for example, declined in the following *dictum*: "in the presence of a green traffic light, make sure in any case that there are no cars coming from the side before continuing to drive", or again: "in the presence of road signs whose recognisability has been hindered by stickers or graffiti, slow down to make sure you have understood their content". The reasoning capacity of the human mind makes it possible to deduct from a generic or elastic rule (drive carefully) a peculiar rule to a given context (check that there are no cars in the intersection even when you have the right of way; slow down when road signs are covered with stickers or graffiti in order to check their content).

Let us now turn to the perspective of the artificial agent. A rule such as "drive carefully" would be a "silent" rule, from which the normative "top-down" MAS alone is unable to extrapolate generalisations to be translated into rules suited to the concrete context presented. This means that the system is unable to read the factual situation of potential danger in the light of the general rule "drive carefully", and that all the possible situation of danger should be pre-codified by the manufacturer[86].

It could be argued that a NMAS based on a bottom-up technology would be able to act in compliance with the general norm "drive carefully" thanks to the observation of the environment, and learning from the experience[87]. However, two observations are urged in dealing with normative "bottom-up" MAS. The first is that learning from experience does not necessarily imply the comprehension of the rule "drive carefully", since there will always be new empiric conditions in which that rule will still be "silent" for the AI system, which must be first experienced by it in order to be detected as dangerous situations[88]. The second implication is that the legal system cannot be open to the idea of authorising AI agents that, when acting in real environments, could cause harm to legal goods in order to learn from the experience. Such a case must be part of the unpermitted risk and no more doubts should arise.

In conclusion, it seems that the algorithm cognition will remain limited in the presence of norms with general content, as is the case of the norm "drive carefully".

Also, the first example, that of the robot-doctor, reveals limited artificial knowledge. Hence, we can conclude that *limited algorithmic cognition* emerges either when the algorithm is confronted with a concrete phenomenology that is outside its field of knowledge (this is the case of eye disease and the newly discovered virus), or when a general rule of diligence intervenes to avoid exposing the legal interest to danger and the consequent offence (these are the cases in which generic negligence would normally come into play, or specific negligence in which the diligent behaviour is described by a generical rule, see Art. 140 of the Road Traffic Act), which while understandable for a human driver, will be much more difficult to "understand" for an artificial driver.

Such phenomena of *limited algorithmic cognition* fall within those type-situations that, in dealing with the manufacturer's position, we have classified as hypotheses in which the system has not produced the expected result, but could not have done otherwise (case *sub c)*). This is a situation type in which, according to the proposed reasoning, it does not seem possible to contest the manufacturer's liability, since his action would be within the area of the acceptable risk (but see the clarifications developed *supra*). We may now add that, within this area of acceptable risk, the user's liability may be found, provided that the circumstances of the concrete case are such as to transform the user's duty of vigilance over the AI system into a duty to intervene which, if disregarded, lays the foundations for his negligence. Under what conditions does the user's duty of vigilance exist is the question we shall now address.

Let us begin by examining situations that are outside the knowledge of the algorithmic, taking the example of medical conditions not recognised by the robotic doctor. In this situation, the duty to intervene is actualized by the limited computational knowledge of the algo-

[86] The example proposed here referred to the give way rule in case of green light could be considered just a textbook case since it is reasonable to argue that the producer will encode into the system the rule "check that there are no cars in the intersection even when you have the right of way"; notwithstanding, a similar conclusion is more difficult for all the other dangerous situations arising from the act of driving.

[87] In such a case, after having realised that the give-way rule is not always respected by the other agents (more likely human agents rather than artificial ones), the driverless car will comply with the right of way rule only when assured that no cars are coming from the side before continuing to drive

[88] This concept is explained by Faggin (2022), pp. 140-41, when he compares the learning activities of the child and that of the algorithm, concluding that human knowledge is characterised by the intuitive aspect of understanding.

rithm, which is designed to respond to specific tasks (recognition of eye tumours)[89].

The user's duty to intervene is then a direct consequence of the limited field of knowledge of the algorithm, which operates, and even better than man, only within a restricted cognitive environment[90]. These "intelligent" machines are designed to react to situations foreseen by those who create them, but not to those that are beyond the programmer's cognition[91].

Let us now move on to the other situation-type of limited algorithmic knowledge, the one in which the elastic rule of diligence presents content that is not comprehensible, *i.e.* characterised by reference to a rule from a social source that the system is unable to assimilate. Once again, we note that these limits characterise the AI alone and not just the human agent, who is a conscious part of that society which elaborates unwritten social rules through generalisations and which constitute the source of generic negligence and supplement the generical rules from which specific negligence is derived. Think, for example, of the rule "verify that there are no other cars at the crossroad even when you have priority" which, although not codified, can in any case be presumed by the driver from the more general rule "drive carefully". Therefore, the law's expectation of the user's duty of diligence does not stop at compliance with the rules on road circulation regulated by traffic lights or road signs to give way but also extends to compliance with the more general principle "drive carefully" of traffic regulations, which, in the specific case, requires verifying that there are ideal conditions for continuing to travel despite having road priority.

Peculiar is the hypothesis of traffic signs covered with stickers or graffiti. A group of researchers demonstrated that such disturbing elements are able to mislead the algorithm, which interprets a "stop" sign covered with stickers as a speed limit sign of 45 km/h[92]. Here too, then, the "drive carefully" rule fails for the algorithm, which does not perceive the sticker, errs in its interpretation of the road sign and fails to realise its content in the concrete situation.

There are other circumstances which implement the user's duty to intervene. That is the case for context in which it would be more appropriate for the protection of legal goods not to comply with the duty of care[93]. This happens especially when the duty of care is not generic, rather it has a rigid structure, and the damage cannot be neutralised except when the duty of care is violated. The function of prevention is then reversed. The rigid structure of the duty of care is transformed from safe protection into an occasion for offending the legal good[94]. In these situations, it could be problematic for AI systems to recognise that the concrete situation requires non-compliance with the duty of care[95].

Such a case is taken into consideration in the recommendations of the European Commission Expert Group established to advise on specific ethical issues raised by driverless mobility for road transport[96]. Recommendation 4 (Consider revision of traffic rules to promote safety of CAVs and investigate exceptions to comply with existing traffic rules by CAVs [*i.e.* Connected and Automated Vehicles]) provides that "Traffic rules are a means to road safety, not an end in themselves. Accordingly, the pursuit of greater road safety may sometimes require non-compliance with traffic rules", therefore "Policymakers and researchers should

[89] Another example from which the difference between human intelligence and artificial "intelligence" emerges, reported by Chagal-Feferkorn (2018), p. 137-138, is that of a woman who goes to the emergency room accompanied by her husband for injuries she claims to have sustained when she crashed into the door. The doctor, while the woman describes the incident, notices an introverted attitude of the woman, who avoids meeting her husband's eyes; he also notes a lack of empathy in the man and this makes him suspect that it is a case of domestic violence for which the intervention of a social worker is necessary, as indicated by the protocols of the health authority.
If the same case were presented to a doctor-robot, endowed with innumerable computational capabilities, even with the ability to deduce psychological states from the tone of voice, he might not process the hypothesis of possible domestic violence, thus not activating the appropriate procedure for treating the case.

[90] See Floridi (2017a), p. 155. According to the A., the most efficient AI systems are those that operate within an environment that is conformed around their limits. The environment must be adapted to the robot to make sure it can operate in it successfully; he notes that "the real difficulty for the AI system is to deal with the unpredictability of the world out there [...]. This is known as the frame problem, which relates to how a context-situated agent can represent to itself a changing environment and interact with it over time in an efficient manner", to conclude that (p. 163) AI systems "are not getting smarter while making us dumber. Instead, it is the world that is becoming an infosphere increasingly suited to [their] limited capabilities".

[91] Piergallini (2020), p. 1759.

[92] Eykholt *et al.* (2018).

[93] Such a situation is frequent in automated vehicle contexts (not just cars, but also airplanes) as highlighted by Ruffolo (2020), pp. 161-162.

[94] Marinucci (1965), p. 248.

[95] As stressed by Ungern-Sternberg (2018), ("[autonomous cars] will unconditionally obey all legal norms duly reflected in the driving algorithms. Unlike human drivers (…) autonomous cars can be programmed not to violate traffic law"), p. 257.

[96] *Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659). Ethics of Connected and Automated Vehicles: recommendations on road safety, privacy, fairness, explainability, and responsibility. 2020. Publication Office of the European Union: Luxembourg*, p. 29.

use data provided by manufacturers and deployers to identify contexts in which it would be more appropriate to (a) change a traffic rule so that CAVs can act safely without engaging in non-compliance, (b) have the CAV handover control so that a human can make the decision to not comply with a traffic rule, or (c) allow the CAV to not comply with a traffic rule if it can explain why it made this decision and leave it to the justice system to decide whether this non-compliance was justified by the pursuit of greater safety".

Hence, there are three solutions devised for the exception to comply with traffic rules. Among them, the latter is presented with caution by the Expert Group, which indeed highlights in the same Recommendation 4 that "Researchers should study the extent to which it is reasonable to expect that an intelligent non-human system is able to engage in the complex process of evaluation of the interpretation of a legal, ethical or societal norm and its balancing with another norm, value or principle. Researchers should also test the *ex-post* explainability of these decisions".

The second solution devises the human-in-the-loop situation, in which the decision not to comply with the traffic rule is referred to the driver. The human agent therefore, might be able to realise that the concrete situation requires the breach of the duty of care and would be required to resume control of the system, adapting his/her behaviour to a more general rule of conduct thus allowing peculiarities of the concrete situation to prevail over the rigidly structured rule[97]. It means that the focus should be on the manufacturers[98] and, ultimately, on the users, whose involvement may be necessary due to uncertainty in the interpretation of the concrete situation.

The time has therefore come to add another column to the table presented above, in which the user's position is taken into account, indicating the content of his duty of care. It will be noted that the duties of information, vigilance and intervention are always present but what is being highlighted is that these duties are latent until factual circumstances capable of activating them arise. Whereas it is the use of the system that activates the duties of information and vigilance, it is the arising of peculiar situations, such as those we have attempted to identify in the previous examples, that activates the duty to intervene.

Case a)	Diligent producer	Diligent Algorithm	Diligent User (duty of information, vigilance and duty to intervene)
Case b)	Negligent Producer	Negligent Algorithm	User's duty of vigilance and of intervene
Case c)	Diligent Producer (acceptable risk)	Negligent Algorithm (unattainable diligence)	User's duty of vigilance and of intervene

[97] This aspect, analysed here in the context of criminal guilt and the duty of care, actually ties in with the problem of the ethicality of artificial intelligence systems which is much debated, and concerns dilemmas, i.e. critical situations in which, at a given point in time, the machine will inevitably cause harm to a group of individuals. *See* Anderson, Anderson (2011); Wallach, Allen (2009); Tafani (2020), pp. 83 et seq.. The issue is made very concrete through the well-known trolley problem, which if originally posed as a dilemma for the man driving the tram, with the advent of AI has been presented as a dilemma for the vehicle itself, called upon to make decisions in emergency situations. The example was first presented by the English philosopher Philippa Ruth Foot, in her essay on abortion entitled "The Problem of Abortion and the Doctrine of the Double Effect", published in the Oxford Review, V, 1967, pp. 5-15, and then taken up and re-proposed under the name of the 'trolley problem' by Thomson (1976). In essence, one imagines the driver of a tram out of control, who has the only possibility of diverting the tram onto a track other than the one it is running on, but here is the dilemma: five men are working on one track and only one man on the other, and whoever is on the track the tram will enter is doomed to be killed. The question then is: kill five men who are on the track that the tram is already on, or kill one man who is on the track to which the tram may be diverted?
Dilemmas and crash avoidance are taken into account in recommendation 6 of the Ethics of Connected and Automated Vehicles report.

[98] *See Discussion of Recommendation 6* of the Expert Group report, *cit.*, p. 33, providing that "Rather than defining the desired outcome of every possible dilemma, it considers that the behaviour of a CAV in a dilemma situation is by default acceptable if the CAV has, during the full sequence that led to the crash, complied with all the major ethical and legal principles stated in this report, with the principles of risk management arising from Recommendation 5 and if there were no reasonable and practicable preceding actions that would have prevented the emergence of the dilemma. This may be necessary to give manufacturers and deployers of CAVs the confidence to deploy their systems, with reduced speed and preventative manoeuvres always being the best solution to decrease safety risks".

4.3. *When will the user be liable? Insufficiency of the breach of the duty of care.*

At this point an objection might be formulated: whereas the area of manufacturer liability will be reduced through the theory of the acceptable risk, the same will not occur for the user, who bears the burden of a new science unable to produce perfect machines capable of avoiding all kinds of harms. Notwithstanding, it must be noticed that the user's liability could be excluded when in specific circumstances an abnormal or extraordinary situation occurs. These abnormal situations may meet the requirements of *unforeseeable circumstances* or *force majeure* that, in the Italian criminal system, exclude sanction according to art. 45 of the Italian crim. Code.

There may also be extraordinary circumstances that, while not presenting the characteristics of unforeseeable circumstances or *force majeure*, are such as to render the user's compliance with the duty of care unattainable[99]. In the latter case, culpability, thus the subjective dimension of negligence, will be excluded, even if a duty of care is breached.

Indeed, when ascertaining culpability, it is requested to take into account the cognitive and physical limitations of the user. It follows that "this transfer of responsibility should only occur if the human operator has sufficient time and information to make responsible control decisions and in no circumstance should the human operator be assigned a task for which humans are unsuited or for which they have not been sufficiently trained"[100].

On this aspect, it should be pointed out that some researches carried out in the field of human-computer interactions (HCI) [101], which take into account the psycho-physical limits of users, have shown that the driverless car greatly reduces the capabilities of the average user to retake the control of the vehicle[102] (an aspect that would therefore already be relevant in the objective dimension of guilt for the reasonable user's parameter). In particular, it is customary to refer to the so-called "handover problem" [103] in level 3 of assisted driving vehicles, in which the user is required to regain control of the car when the automatic system encounters criticalities in the course of its operation. Well, such research shows that, on average, the level of attention with which users monitor the guidance of the system is not constant due to their lack of direct involvement in the act of driving, and this negatively affects their level of alertness[104]. Therefore, it is paramount to reconsider the role of the user as a fall-back mechanism during automated driving[105].

We can ask ourselves whether such scientifically proven difficulties in the level of monitoring can be taken into account for the purposes of establishing negligent culpability. The answer seems to me to be affirmative, especially in the context of criminal liability[106]: if even cognitive-psychological research shows that the average human being is not capable of always having an "extraordinary" level of attention, this must be taken into account by the judge when assessing the circumstances of the concrete case in order to ascertain the subjective dimension of negligence. To achieve such a goal, a legislative intervention seems appropriate, in order to introduce a sort of "immunity clause" that codifies the general principle of unattainability.

Furthermore, if researches will demonstrate with certainty that in some fields is unattain-

[99] Giannini (2021), p. 24, with regards to the effects of automation on the attainability of compliance with the duty of care.
[100] *Discussion of Recommendation 4* of the Expert Group report, *cit.*, p. 30.
[101] Selbst (2020), p. 1346.
[102] Aria, Olstam, Schwietering (2016), p. 764.
[103] See American Association For Justice, *Driven To Safety: Robot Cars And The Future of Liability* (2017), p. 14, (*perma.cc*): *"Research shows that humans are not well adapted to re-engaging with complex tasks, like driving a vehicle in an emergency situation, once their attention has been allowed to wander. A 2015 study by the National Highway Traffic Safety Administration (NHTSA) found that it took test subjects an average of 17 seconds to respond to a request to regain control of their vehicle. That's enough time for a car traveling at 60 miles per hour to travel a quarter of a mile"*. Reference is made to the study *Human Factors Evaluation of Level 2 and Level 3 Automated Driving Concepts, National Highway Traffic Safety Administration (NHTSA)*, August 2015, *www.nhtsa.gov*.
[104] *See* the previous footnote. A list of concerns raised by AV is presented in the work of Aria, Olstam, Schwietering (2016), which includes the degrading driving skills of human drivers in the absence of practice and his/her tendency to become involved with secondary tasks. The idea of establishing the boundaries of the negligence of the user is also supported by Beck (2016), p. 141.
[105] Heikoop, *et al.* (2019), p. 7, par. 3.3; Cappellini (2022), p. 13.
[106] Panattoni (2021), in dealing with the topic of human control, defines the user's oversight as "an overly tight obligation". More generally on the efficacy and impacts of human oversight policies in automated decision-making systems, including the criminal justice one, see Green (2022) who proposes a shift from human oversight to institutional oversight. The A. affirms that "policymakers must stop relying on human oversight as a remedy for the potential harms of algorithms" (p. 2) and that "there must be evidence suggesting that people can oversee the algorithm" (p. 14).

able even for the reasonable agent to grant a prompt intervention on the system in order to retake control of it, it could be possible to argue that the duty of care (*i.e.* the objective dimension of negligence) will be influenced. It follows that the reasonable agent parameter should take into consideration the limited capabilities of the average user.

5. Conclusion.

This work has explored the capabilities of an intelligent system, ultimately concluding that the diligent behaviour of the artificial system can never be equated with human diligence.

As I have tried to demonstrate, "artificial diligence" is limited to the field of knowledge available to the system, which will not be endowed with a critical spirit, common sense, and the ability to make an overall assessment of the dangerous situation, which altogether allow the application of duties of care, especially the generic ones, in the concrete case. The artificial system will know how to calculate the best solution in order to conform its behaviour using its set of inbuilt knowledge. However, as soon as the dangerous situation goes beyond the perimeter of its artificial knowledge, the machine will have no predetermined answer and will have to proceed making generic assumptions based on precedent examples and stored data thus increasing the risk of error.

Of course, the limits of artificial diligence are relevant for the purposes of assessing the manufacturer and user's negligent conduct, who are addressees of duties of care inferable from European legislation.

With the purpose to delineate the apportionment of responsibilities between the producer and the user, I distinguished the situations of danger connected to the non-observance of duties of care in two categories: situations in which it is possible to provide *ex ante* a description in terms of danger, and situations in which such an *ex ante* description of danger is unattainable since they are correlated to concrete dynamics that are difficult to foresee and therefore not imagined in the algorithm's training phase and offered as examples during training. In other words, these are cases that cannot be encoded in the computational language to make them knowable in advance to the machine, because they cannot be predicted.

In the presence of such circumstances (enlisted in situation types *sub c)* as seen in the previous chart) the system will proceed with generalisations that may contain a margin of error that could not have been avoided by the manufacturer even if using different training, due to the unpredictability of the concrete dynamics.

It follows that the manufacturer cannot be considered negligent for a generalisation that is unsuitable for the concrete case if – and only if – an entirely unforeseeable risk is involved, originating from the combination of a series of factors occurring in the concrete case, which make the entire dynamic leading to the causation of the event absolutely peculiar and unique.

However, situations that cannot be codified in computer language *ex ante* by the manufacturer may, at least in some cases, be recognisable and avoidable by the user, who is called upon to monitor the correct operation of the system and intervene where necessary. At this point, the intervention of the human agent – whose semantic reading capacity enables him/her to understand the dangerous situation in its concreteness – will be necessary and he/she will adopt a conduct that is the most diligent not in abstract, but in concrete terms.

Nevertheless, it must be taken into account that it is not always attainable compliance to the duty of care from the user. In the presence of specific circumstances, his/her liability could be excluded for lack of culpability of the subjective dimension of negligence. In other cases, unforeseeable circumstances or *force majeure* can occur, which will make the fact criminally irrelevant. Moreover, even the objective dimension of negligence can be excluded when scientific evidences demonstrate how not even a reasonable man could have complied with the duty of care.

I have tried to show how a criminal liability can be founded with the traditional categories of criminal law, without considering the machine as the author of a crime. Nevertheless, the liability regime seems to attribute much more responsibility to the user, rather than to the manufacturer. Therefore, on one hand, a legislative intervention seems necessary in order to delimitate the user's liability only to cases in which an intervention is attainable. On the other hand, the law should enhance the role of the manufacturer whose responsibilities can be established according to other branches of the legal system different from the criminal one.

It follows that the response of the law in front of the new risks of AI shall be considered as a whole[107]. Probably in a context of such a high degree of uncertainty, the jurist, but also the community, will have to accept a marginal role for criminal law, so that technological progress will be a confirmation of the achievements of modern legal civilisation and not a context favourable to the application of security measures that entrust a pivotal role to the criminal sanction. Criminal law is and must remain the last remedy, the *ultima ratio*.

Bibliography

Abbot, Ryan (2020): *The Reasonable Robot. Artificial Intelligence and the Law*, (Cambridge, Cambridge University Press)

Allen, Colin, Wallach, Wendell, (2009): *Moral Machines: Teaching Robots Right from Wrong* (Oxford, Oxford University Press)

Amato, Salvatore (2020): *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie* (Torino, Giappichelli)

Anderson, Michael, Anderson, Susan L. (eds.) (2011): *Machine Ethics* (Cambridge, Cambridge University Press)

Andrighetto, Giulia, Governatori, Guido, Noriega, Pablo, Van der Torre, Leendert W.N. (2013) (eds.): *Normative Multi-Agent Systems* (Schloss Dagstuhl, Leibniz-Zentrum für Informatik, GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany)

Aria, Erfan, Olstam, Johan, Schwietering, Christoph (2016), "*Investigation of Automated Vehicle Effects on Driver's Behavior and Traffic Performance", Transportation Research Procedia*, Volume 15, pp. 761–770

Balkin, Jack M. (2017): "*The Three Laws of Robotics in the Age of Big Data", 78 Ohio St. L.J. (Sep. 10*)

Barré, Jessy (2022) : « *Quelle formation pour les conducteurs de véhicules autonomes ? », Recherche, Transport, Sécurité,* February

Bartoli, Roberto (2021): "*voce Fonti della colpa", Enc. dir., I Tematici, Il reato colposo,* Milano, Giuffrè, pp. 519 et seq.

Basile, Fabio (2019): *"Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine", in Dir. pen. e uomo,* 29 September 2019

Beck, Susanne (2016): "*Intelligent agents and criminal law – Negligence, diffusion of liability and electronic personhood",* in *Robotics and Autonomous Systems,* 2016, 138-143

Beck, Susanne (2017): *"Google Cars, Software Agents, Autonomous Weapons Systems – New Challanges for Criminal Law*", in Hilgendorf, E., Seidel, U. (eds.), *Robotics, Autonomics and the Law*, Nomos, Baden-Baden, 2017, 227-252

Bertolini, Andrea, Episcopo, Francesca (2021): "*The Expert Group's Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies: A critical assessment*", in *European Journal of Risk Regulation, 12*(3), 644-65, doi:10.1017/err.2021.30

Bifulco, Raffaele (2018): "*Intelligenza artificiale, internet e ordine spontaneo*", in Pizzetti, F.(ed.), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, pp. *383-400*

Borsari, Riccardo (2019): *"Intelligenza Artificiale e responsabilità penale: prime considerazioni"*, in *MediaLaws*, Novembre 20, 3

[107] Ruffolo (2020), p. 155 stresses how the law should not be such to undermine technological development, considering the benefits for society from AI systems (particularly, the A. refers to the estimated reduction of car accidents thanks to the introduction of automated vehicles).

Bradford, Anu (2020): *The Brussels Effect: How the European Union Rules the World*, (New York, Oxford University Press)

Bricola, Franco (1978): "*Responsabilità penale per il tipo e il modo di produzione*", in *La responsabilità dell'impresa per i danni all'ambiente e ai consumatori*, Milano, Giuffrè, pp. 75-90

Calo, Ryan (2017): "*Artificial Intelligence Policy: A Primer and Roadmap*", 51 *U.C. Davis l. Rev*. 399-435

Camardi, Carmela (ed.) (2022): *La via europea per l'intelligenza artificiale,* (Milano, Wolters Kluwer)

Canestrari, Stefano (2013): "*La colpa*", in *Trattato di diritto penale, Parte generale, vol. II, Il Reato*, a cura di Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, Papa, Michele, (Torino, UTET)

Cappellini, Alberto (2019): "*Profili penalistici delle self-driving cars*", in *Dir pen. cont.-Riv. trim.*, 2, 325-353

Cappellini, Alberto (2022): "*Reati colposi e tecnologie dell'intelligenza artificiale*", *Arch. Pen.,* 3, 2022, 1-19

Castronuovo, Donato (2009): *La colpa penale* (Milano, Giuffrè)

Chagal-Feferkorn, Karni (2018): "*The Reasonable Algorithm*", in *University of Illinois Journal of Law (UIJL), Technology & Policy, no. 1,* pp. 111-148

Colonna, Kyle (2012): "*Autonomous Cars and Tort Liability*", *4 Case W. Res. J. L. Tech & Internet,* 81-130

Consulich, Federico (2021): "*voce Rischio consentito*", *Enc. dir., I Tematici, Il reato colposo,* (Milano, Giuffrè)

Consulich, Federico (2022): "Flash offenders. *Le prospettive di* accountability *penale nel contrasto alle intelligenze artificiali devianti*", in *Riv. it. dir. proc. pen.,* 3, 1015-1055

Conte, Rosaria, Castelfranchi, Cristiano (1993): *"Norms as mental objects. From normative beliefs to normative goals"*, in Castelfranchi, C., Müller, JP. (eds) *From Reaction to Cognition. MAAMAW 1993, Lecture Notes in Computer Science, vol 957,* Berlin, Heidelberg, Springer, online version: *aaai.org*

Cotta, Sergio (1968): *La sfida tecnologica* (Il Mulino, Bologna)

Crane, Daniel A., Logue Kyle D., Pilz, Bryce (2017): "*A survey of the legal issues arising from the deployment of autonomous and connected vehicles*", in *Michigan Telecom. And Tech. L. Rew.,* p. 191 et seq.

De Francesco, Vittorio (1977-78): "*Sulla misura soggettiva della colpa*", in *Studi Urbinati,* 1977-78, pp. 275 et seq.

Di Giovine, Ombretta (2003): *Il contributo della vittima nel delitto colposo* (Torino, Giappichelli)

Donini, Massimo (1989): "*Lettura sistematica delle teorie dell'imputazione oggettiva dell'evento*, P.te I", in *Riv. it. dir. proc. pen.*, 588-638

Donini, Massimo (2010): "(voce) *Imputazione oggettiva dell'evento (diritto penale)", in Enciclopedia del diritto, Annali*, vol. III, Milano, Giuffrè, p. 646 et seq.

Engisch, Karl (1995): *Untersuchungen über Vorsatz und Fahrlässigkeit im Strafrecht*, (Aalen, Scientia (reprint 1930 ed.))

Exner, Franz (1910): *Das Wesen der Fahrlässigkeit: eine Strafrechtliche Untersuchung*, (Leipzig, F. Deuticke)

Eykholt, Kevin, *et al.* (2018): "*Robust Physical-World Attacks on Deep Learning Visual Classification*", *arXiv.it*

Faggin, Federico (2022): *Irriducibile. La coscienza, la vita, i computer e la nostra natura* (Milano, Mondadori)

Floridi, Luciano (2017a): *La quarta rivoluzione. Come l'infosfera sta trasformando il modo* (Milano Raffaello Cortina Editore)

Floridi, Luciano (2017b): "*Digital's Cleaving Power and Its Consequences", Philosophy & Technology*, May

Forti, Gabrio (1990): *Colpa ed evento nel diritto penale* (Milano, Giuffrè)

Gallo, Marcello (1960): "*voce Colpa penale (dir. vig.)", Enciclopedia del diritto*, vol. VII, 1960, Milano, Giuffrè

Giannini, Alice (2021): *"Intelligenza artificiale, human oversight e responsabilità penale: prove d'impatto a livello europeo", Criminalia*, 21.11.2021, discrimen.it

Gigerenzer, Gerd (2022): *Perché l'intelligenza umana batte ancora gli algoritmi* (Milano, Raffaello Cortina editore)

Giunta, Fausto (1999): *"La normatività della colpa penale. Lineamenti di una teorica",* in *Riv. it. dir. proc. pen.* p. 86-115

Giunta, Fausto (2019), "Culpa, culpae", in *disCrimen*, 4.06.2019

Gless, Sabine, Silverman, Emily, Weigend, Thomas (2016): *"If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability",* in *New Criminal Law Review*, 3, 19, 412-436

Green, Ben (2022): "*The flaws of policies requiring human oversight of government algorithms", Computer Law&Security rew.,* 45, 1-22

Heikoop, Daniel, Hagenzieker, Marjan, Mecacci, Giulio, Calvert, Simeon, Santoni De Sio, Filippo, van Arem, Bart (2019): *"Human behaviour with automated driving systems: A quantitative framework for meaningful human control",* in *Theoretical Issues in Ergonomics Science (TIES)*, March.

Hilgendorf, Eric (1993): *Strafrechtliche Produzentenhaftung in der "Risikogesellschaft"* (Berlin, Duncker und Humblot)

Hippel, Robert (1908): *„Vorsatz, Fahrlässigkeit, Irrtum"*, in Birkemeyer, Karl v. (ed.), *Vergleichende Darstellung des Deutschen und Ausländischen Strafrechts, Allgemeiner Teil*, III, Berlin, Liebmann, 374-599

Hollander, Christopher. D., Wu, Annie S. (2001): *"The Current State of Normative Agent-Based Systems", Journal of Artificial Societies and Social Simulation,* 14 (2), 6, 2011

Hubbard, F. Patrick (2014), " *"Sophisticated Robots": Balancing Liability, Regulation, and Innovation", 66 Fla. L. Rev.*, 1803 et seq.

Jescheck, Hans-Heinrich, Weigend, Thomas (1996): *Lehrbuch des Strafrechts. Allgemeiner Teil. 5 Auflage* (Berlin, Duncker-Humbolt)

King, Thomas, Aggarwal, Nikita, Taddeo, Mariarosaria, Floridi, Luciano (2021): *„Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions", The 2020 Yearbook of the Digital Ethics Lab*, October, pp.195-227, *researchgate.net*

La Vattiata, Federico, Carmelo (2023): *„AI Systems Involved in Harmful Events: Liable Persons or Mere Instruments? An Interdisciplinary and Comparative Analysis"*, in *BioLaw Journal – Rivista di BioDiritto, n. 1,* 485-499

Lagioia, Francesca, Sartor, Giovanni (2020): "*AI Systems Under Criminal Law: a Legal Analysis and a Regulatory Perspective", Philosophy & Technology*, 2020, 33, 433–465

Leiman, Tania (2021): *"Law and tech collide: foreseeability, reasonableness and advanced driver assistance systems", Policy and Society*, 40:2, 250-271

Lemley, Mark A., Casey, Bryan (2019): "*Remedies for Robots", University of Chicago Law Review*, Vol. 86: Iss. 5, Article 3, p. 1311 et seq.

Lohmann, Melinda Florina (2016): "*Liability Issues Concerning Self-Driving Vehicles",* in *European Journal of Risk Regulation,* 7, 335 et seq.

Mantovani, Ferrando (1988): *"voce Colpa, in Dig. Disc. Pen.",* vol. II, Padova, Cedam

Marinucci, Giorgio (1965): *La colpa per inosservanza di leggi* (Milano, Giuffrè)

Militello, Vincenzo (1988): *Rischio e responsabilità penale* (Milano, Giuffrè)

Panattoni, Beatrice (2021): "*AI and Criminal Law: The Myth of 'Control' in a Data-Driven Society*", in (eds.) Vermeulen, Peršak, Recchia, *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice*, Antwerpen, Maklu, *Rev. int. droit pén., vol.* 92, 125-142

Picotti, Lorenzo (2021): "*Profili di responsabilità penale per la circolazione di veicoli a guida autonoma",* in *Studi in onore di Antonio Fiorella*, Vol. I (Roma Tre Press, Roma), 813-837

Piergallini, Carlo (2004): *Danno da prodotto e responsabilità penale* (Milano, Giuffrè)

Piergallini, Carlo (2020): "*Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?",* in *Riv. it. dir. proc. pen.*, 4, p. 1745-1774

Preuss, Wilhelm (1974): *Untersuchungen zum erlaubter Risiko im Strafrecht* (Berlin, Duncker und Humblot)

Prittwitz, Cornelius (1993): *Strafrecht und Risiko. Untersuchungen zur Krise von Strafrecht und Kriminalpolitik in der Risikogesellschaft* (Frankfurt a.M., Vittorio Klostermann)

Rehberg, Jürg (1962): *Zur Lehre vom „erlaubten Risiko"* (Zürich, Schulthess)

Roeder, Hermann (1969): *Die Einhaltung des sozialadäquaten Risikos* (Berlin, Duncker und Humblot)

Ruffolo, Ugo (2020): "*Intelligenza artificiale ed* automotive: *la responsabilità da veicoli* self-driving *e* driverless", in Ruffolo, Ugo (eds.) "*Intelligenza artificiale. Il diritto, i diritti, l'etica*", Milano, Giuffrè, 153-178

Ruffolo, Ugo, Al Mureden, Enrico (2019): "*Intelligenza artificiale e diritto. Autonomous vehicles e responsabilità nel nostro sistema e in quello statunitense",* in *Giur. It.*, 2019, 7, p. 1704 et seq.

Ruth Foot, Philippa (1967): *"The Problem of Abortion and the Doctrine of the Double Effect"*, *Oxford Review*, V, pp. 5-15

Salvadori, Ivan (2021): "*Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*", in *Riv. it. dir. proc. pen. (RIDPP),* 1, 2021, 83- 118

Savarimuthu, Bastin Tony Roy, Cranefield, Stephen (2009): "*A categorization of simulation works on norms", Dagstuhl Seminar Proceedings 09121, Normative Multi-Agent Systems*, *drops.dagstuhl.de/opus/volltexte/2009/1905i.*

Schroeder, Friedrich-Christian (2003): *„§16 Irrtum über Tatumstände"*, in *Strafgesetzbuch. Leipziger Kommentar, Großkommentar, 11, neu bearbeitete Auflage*, hrsg. von Jähnke, Burkhard, Laufhütte, Heinrich Wilhelm, Odersky, Walter, (Berlin, De Gruyter Recht), Bd. 1, (10)-(104)

Searle, John R. (1980): "*Minds, brains, and programs*", in *Behavioral and Brain Sciences,* 3 (3), 417-457

Searle, John R. (1990): "*Is the Brain's Mind a Computer Program?*", in *Scientific American*, Jan., p. 26-32

Selbst, Andrew D. (2020): "*Negligence and AI's Human Users*", in *Boston University Law Review,* 100, 1315-1376

Severino, Paola (2020): *"Intelligenza artificiale e diritto penale"*, in Ruffolo, Ugo (eds.), *Intelligenza artificiale. Il diritto, i diritti, l'etica* (Milano, Giuffrè), 531-546

Shoham, Yoav, Tennenholtz, Moshe (1992), "*On the synthesis of useful social laws for artificial agent societies (preliminary report)", www.aaai.org*, 276-281

Tafani, Daniela (2020): "*Sulla moralità artificiale. Le decisioni delle macchine tra etica e diritto",* in *Riv. di filosofia*, 1, aprile, pp. 83 et seq.

Thomson, Judith J. (1976), "*Killing, letting die and the trolley problem*", in *The Monist*, LIX, pp. 204-217

Ungern-Sternberg, Antie (2018): "*Autonomous driving: regulatory challenges raised by artificial decision-making and tragic choices*", in Barfield, Woodrow, Pagallo, Ugo, (eds.), *Research handbook on the law of artificial intelligence,* Edward Elgar**,** pp. 253-277

Vagliasindi, Grazia Maria (2021) : « *Intelligence artificielle et droit pénal entre outils d'augmentation de l'efficacité préventive et punitive de l'État et risques et défis pour les droits humains et l'État de droit* », in Sedjari, A. (ed.), *Impact du numérique et de l'intelligence artificielle sur les transformations des gouvernances publiques*, 357-382

La responsabilità penale al tempo di ChatGPT*

Prospettive *de iure condendo* in tema di gestione del rischio da intelligenza artificiale generativa

La responsabilidad penal en la era de ChatGPT

Perspectivas de iure condendo *en la gestión del riesgo de inteligencia artificial generativa*

Criminal Liability in the Era of ChatGPT

De Iure Condendo *Perspectives on Managing Risk from Generative Artificial Intelligence*

Leonardo Romanò
Dottorando di ricerca in Diritto penale all'Università del Lussemburgo e all'Università degli Studi della Tuscia
leonardo.romano@uni.lu

Intelligenza artificiale, Dolo, Colpa, Responsabilità da reato degli enti

Inteligencia artificial, Dolo, Culpa, Responsabilidad penal personas jurídicas

Artificial Intelligence, Intention, Negligence, Corporate Criminal Liability

Abstracts

Gli esempi dei possibili utilizzi della nuova Intelligenza Artificiale "generativa" (come ChatGPT) si moltiplicano senza sosta, e con essi, le preoccupazioni per le ricadute offensive che, in prospettiva futura, potrebbero derivare dalla sua applicazione in settori socio-economici in cui sono in gioco beni giuridici fondamentali. Ad oggi, la regolamentazione di tale tecnologia è ancora poco sviluppata e, quindi, aggalla con forza il tema di come i rischi connessi a questa post-moderna forma di tecnologia vadano governati e con quali strumenti. Dopo una breve premessa tecnica sul suo funzionamento, il lavoro si propone di scrutare i rapporti tra questa tecnologia ed il panorama regolatorio emergente a livello europeo, ponendo l'accento sul tema del controllo umano e della responsabilità penale rispetto a eventuali eventi avversi prodotti da tali sistemi. Vengono, infine, avanzate alcune proposte volte a individuare l'ambito (pur limitato) di un possibile reale utilizzo del diritto penale per fronteggiare adeguatamente i rischi rilasciati da questa nuova tecnologia.

Los ejemplos de posibles usos de la nueva Inteligencia Artificial "generativa" (como ChatGPT) se multiplican sin cesar, y con ellos, las preocupaciones sobre las posibles repercusiones delictivas que podrían derivarse de su aplicación en sectores socioeconómicos que involucran bienes jurídicos fundamentales. Hasta la fecha, la regulación de esta tecnología aún está poco desarrollada, lo que enfatiza la importancia de cómo se deben gobernar los riesgos asociados a esta forma de tecnología posmoderna y con qué herramientas. Tras una breve introducción técnica sobre su funcionamiento, este trabajo tiene como objetivo examinar las relaciones entre esta tecnología y el panorama regulatorio emergente a nivel europeo, poniendo énfasis en el tema del control humano y la responsabilidad penal frente a posibles resultados lesivos generados por dichos sistemas. Por último, se presentan algunas propuestas para identificar el alcance (aunque limitado) de un posible uso real del derecho penal para abordar adecuadamente los riesgos derivados de esta nueva tecnología.

* Si ringrazia il professor Carlo Sotis per i preziosi commenti e spunti di riflessione offerti nella stesura di questo articolo.

The examples of possible uses of the new "generative" Artificial Intelligence (such as ChatGPT) continue to multiply relentlessly, along with concerns about the potential harmful consequences that may arise from its application in socio-economic sectors where fundamental legal interests are at stake. Currently, the regulation of this technology is still underdeveloped, thus highlighting the pressing need to address how the risks associated with this post-modern form of technology should be governed and with which tools. After a brief technical introduction on its functioning, this work aims to examine the relationship between this technology and the emerging regulatory landscape at the European level, focusing on the issues of human control and criminal liability concerning any adverse events caused by such systems. Finally, some proposals are put forward to identify the scope (albeit limited) of a possible actual use of criminal law to adequately address the risks arising from this new technology.

Sommario

1. Premessa: diritto penale, nuovi rischi e vecchie paure.

Un nuovo oracolo algoritmico[1] ha fatto il suo ingresso nelle nostre vite: ChatGPT[2]. La diffusione di sistemi di Intelligenza Artificiale c.d. generativa (c.d. *Generative AI*, di seguito IAG)[3] – di cui ChatGPT e simili[4] rappresentano gli esempi più sofisticati attualmente in circolazione – ha messo in moto un radicale cambio di paradigma rispetto al nostro modo di generare e acquisire conoscenza; e i *social media* e i giornali si sono popolati di esempi sorprendenti e spaventosi di cosa questa tecnologia sia in grado di fare.

L'apprendimento automatico (c.d. *machine learning*)[5], che un tempo era destinato a eseguire solo compiti specifici e circoscritti, è stato ora impiegato per progettare complessi modelli linguistici[6] in grado di produrre, a partire da una richiesta dell'utente (o *prompt*), qualsiasi tipo di contenuto come *output* (tra cui testo, immagini, audio o codice). Sicché, un aspetto chiave che accompagna lo sviluppo di questa tecnologia riguarda proprio la vastità del suo potenziale utilizzo.

Basti immaginare uno studente che chieda a ChatGPT: scrivi un saggio su Napoleone, includi una o due citazioni dotte e concludi con una frase ad effetto[7]; uno scienziato che chieda: sintetizza questa proteina in modo che possa utilizzarla per creare un nuovo farmaco[8]; uno scrittore che chieda: scrivi un sonetto nella lingua di Shakespeare[9]; e ancora, un giudice che chieda: scrivi la sentenza al posto mio[10]. Gli esempi dei possibili utilizzi di questa tecnologia si moltiplicano senza sosta, e con essi, le preoccupazioni per le potenziali ricadute offensive che, in prospettiva futura, questa intromissione del non umano potrà avere sull'umano. Oltre alle prevedibili questioni di stampo etico, aggallano con forza i rischi derivanti sia dall'utilizzo dell'IAG per prendere decisioni automatiche in settori che incidono sui diritti fondamentali della persona (come nel mondo del lavoro, dell'assistenza sanitaria, delle assicurazioni, della previdenza sociale e della giustizia), sia dall'uso scorretto nonché da malfunzionamenti di tale

[1] L'espressione è di Manes (2020), p. 6.

[2] ChatGPT si basa sull'architettura *Generative Pre-trained Transformer* (GPT). Il sistema è stato addestrato utilizzando una rete neurale progettata per l'elaborazione del linguaggio naturale su un set di dati di oltre 45 terabyte di testo proveniente da Internet (libri, articoli, siti web e altri contenuti testuali), che in totale comprendeva miliardi di parole di testo. Il modello di base, GPT-3, rilasciato nel novembre 2022, viene perfezionato costantemente e la nuova versione, GPT-4, è stata rilasciata nel marzo 2023. Mentre quest'ultimo rappresenta una versione premium a pagamento, il primo è generalmente accessibile attraverso un sito web facile da usare: cfr. chat.openai.com.

[3] Per riferirci, in generale, ai sistemi di IA useremo di seguito, indifferentemente, espressioni come "sistema IA, *software*, agente artificiale, macchina, algoritmo".

[4] Alla famiglia dell'IAG appartengono sistemi in grado di generare testi (come ChatGPT o Bard), immagini (DALL-E), video (Synthesia) e persino arte (Midjourney). Per le specifiche tecniche dei vari modelli, cfr. l'*overview* pubblicata su platform.openai.com.

[5] Per un'analisi approfondita della tecnologia di *machine learning*, cfr. Hao (2018).

[6] Un modello linguistico consiste essenzialmente nell'uso di varie tecniche statistiche basate sul lavoro di algoritmi addestrati per analizzare miliardi di miliardi di parole (questo è il "*learning*" del "*machine learning*") e calcolare quanto è probabile che, data una certa sequenza di parole, ne segua una anziché un'altra. Ad esempio, date le parole "ha messo online un chatbot basato sull'ultima", "versione" è un seguito più probabile di "decisione". Cfr. OpenAI (2019).

[7] Le preoccupazioni per l'impatto che un uso improprio di ChatGPT potrà avere sul sistema educativo hanno portato al divieto espresso del suo utilizzo nelle scuole pubbliche a New York. V. Rosenblatt (2023).

[8] Uno studio, pubblicato su *Nature Biotechnology*, ha dimostrato come ProGen, un modello linguistico simile a ChatGPT, sia stato utilizzato per lo sviluppo di nuove proteine che possono essere utilizzate per molteplici applicazioni, da quella della progettazione di nuovi farmaci alla plastica degradante. Madani *et al.* (2023).

[9] ChatGPT si è dimostrato in grado di produrre testi scientifici o letterari a prova di revisione umana. Cfr. Sample (2023).

[10] Un magistrato colombiano ha utilizzato la chatbot di OpenAI nella stesura di una decisione in Colombia. Benché il giudice abbia svolto l'attività di sua competenza autonomamente, la redazione del testo è stata supportata dalla chatbot per quanto concerne la sezione dedicata alle argomentazioni a supporto della decisione. Inoltre, la chatbot della startup americana DoNotPay è già pronto a fare il suo debutto nelle aule di tribunale statunitensi come avvocato-robot.

tecnologia[11].

A tal riguardo, lo *Europol Innovation Lab* ha pubblicato un report in cui preconizza l'emergere nel prossimo decennio di nuove forme di criminalità associate all'utilizzo improprio di ChatGPT[12]. In particolare, il report evidenzia il rischio che i più diversi reati previsti dall'ordinamento possono combinarsi con modalità commissive che passano attraverso l'azione materiale dell'agente artificiale[13]. Da un lato, la capacità di tale tecnologia di redigere testi altamente verosimili la rende uno strumento estremamente utile nell'ambito del *cybercrime*[14], segnatamente nella commissione di frodi online: ad esempio, per stessa "ammissione" di ChatGPT[15], esso "potrebbe essere utilizzato per creare notizie false, per impersonare individui online o per automatizzare attività illegali, come la creazione di truffe di *phishing*, *hacking*, *deepfake* o messaggi di *spam*". Dall'altro lato, "anche se utilizzato conformemente alle sue finalità, permane il rischio che il sistema possa agire in modo difforme rispetto alle istruzioni impartite dall'agente umano, concretizzando così un fatto non voluto o addirittura diverso da quello avuto di mira da quest'ultimo. Ciò potrebbe comportare il rischio che il risultato finale sia inappropriato o addirittura dannoso per l'utente o per l'azienda utilizzatrice": si pensi a un sistema di IAG che "diffami" una persona rielaborando i suoi dati sensibili in modo inesatto, ovvero istighi l'utente a realizzare atti illeciti e financo autolesivi[16]. Proprio questa propensione a trasformare in modo imprevedibile l'*input* umano in un *output* differente è destinata ad aumentare in misura proporzionale ai margini di autonomia del sistema: quanto maggiore la sua autonomia, tanto maggiore il rischio che il "prodotto soggettivizzato"[17] provochi eventi avversi senza l'intervento diretto dell'uomo, sollevando dunque questioni proprie del diritto penale.

Osservazioni, quelle sin qui condotte, che possono apparire ovvie e scontate, specie se si considera che il diritto penale ha già avuto modo di confrontarsi con la questione della possibile attribuzione di responsabilità penale per le sempre più numerose manifestazioni lesive associate alla diffusione di agenti artificiali[18]. Ancor prima che l'IAG facesse la sua entrata in scena, una copiosa letteratura penalistica, sia italiana[19] che internazionale[20], ha a più riprese evidenziato come l'opacità e l'imprevedibilità di certi strumenti basati su IA renda estremamente difficile imputare per colpa un reato algoritmico[21] all'agire di un singolo soggetto umano[22].

Tuttavia, se per un verso i rischi da ignoto tecnologico rilasciati da ChatGPT sono in larga parte una riedizione di problematiche già note nell'interazione uomo-macchina, per altro verso esiste un dato peculiare e sostanzialmente nuovo rispetto al passato: il grado di autonomia e la vastità del potenziale applicativo dell'IAG parrebbero escludere del tutto la stessa possibilità di un controllo e/o intervento umano preventivo. Se questa ipotesi si rivelasse corretta, venendo meno la possibilità di imputare un eventuale risultato lesivo a un utilizzatore che non partecipa più all'attività algoritmica, addirittura ormai privato della capacità di governarla, non rimarrebbe altro che un problematico "fatto proprio" della macchina, o al massimo un caso

[11] Le preoccupazioni per le conseguenze negative che lo sviluppo di tale tecnologia potrà avere su ambiti come il lavoro, l'istruzione e l'economia ha spinto un gruppo di accademici ed esperti di tecnologia e informatica a chiedere, tramite una petizione su Futureoflife.org, di sospendere per sei mesi l'addestramento delle IAG. V. Future of Life Institute (2023).
[12] V. Europol Innovation Lab (2023).
[13] *Ivi*, p. 7.
[14] *Ivi*, p. 8.
[15] Si consenta questo poco ortodosso riferimento ai risultati generati da un'esplicita "intervista" a ChatGPT con *prompt*: "Quali sono i rischi penali derivanti dall'utilizzo di ChatGPT?".
[16] Casi di questo tipo si sono già verificati in passato con riferimento a chatbot meno sofisticati di ChatGPT. Cfr. Lana (2021).
[17] Questa espressione è di Cappellini (2023), p. 24, il quale preconizza l'avvento di un'IA "che non si limita più a realizzare la volontà umana che le sta dietro, ma agisce nel mondo in modo che non è più governato dalla mano dell'uomo".
[18] La casistica è ampia e non se ne può dar conto in questa sede. Tra i casi più "classici" di danno prodotto da sistemi di IA basti qui menzionare quelli nel settore della guida autonoma, in quello finanziario o in quello medico-chirurgico. Per tutti, cfr. rispettivamente: Cappellini (2019); Consulich (2018); Lagioia F. e Contissa G. (2020). In una prospettiva più ampia sui reati algoritmici: King *et al.* (2020); Caldwell *et al.* (2020); Pagallo (2013); Beck (2017).
[19] Con particolare riguardo alla dottrina italiana, la riflessione sulle implicazioni della IA per il diritto penale è già molto stratificata. Per tutti: Tripodi (2023); Salvadori (2021); Giannini (2022); Magro (2019); Piergallini (2020); Piva (2022); Panattoni (2021); Troncone (2022); Consulich (2022); Minelli (2022); Manes (2020); Ruffolo (2021). Per una disamina dei rapporti tra IA e giustizia penale, si rimanda, *ex multis*, a Basile (2019); sia consentito, infine, un riferimento al nostro Romanò (2022).
[20] La letteratura straniera sul tema è troppo vasta per essere qui sistematicamente ricordata: si rinvia, per tutti, ai richiami contenuti nelle altre note, oltre che ai riferimenti bibliografici di cui già al nostro scritto da ultimo citato.
[21] L'espressione "reati algoritmici" o "*AI crimes*" è di R. Abbott e A. Sarch (2019), p. 323, in cui viene definita come "*cases in which an AI would be criminally liable if a natural person had performed a similar act*".
[22] Per tutti, v. Surden e Williams (2016), p. 157; Salvadori (2021), p. 102; Bathaee (2018); R. Abbott e A. Sarch (2019), p. 330 ss.

fortuito, privo di copertura sul piano della responsabilità penale 23.

Una cosa è certa: all'indomani dell'ennesimo traguardo tecnologico, il quesito che la scienza penale è chiamata a porsi è sempre il medesimo – come i rischi connessi a questa post-moderna forma di tecnologia vadano governati e con quali strumenti[24]. Come noto, elemento ricorrente nelle analisi che valorizzano la "società del rischio"[25] in prospettiva penalistica è la riflessione sulle torsioni indotte nel diritto penale dal fatto di essere divenuto il sistema preposto alla minimizzazione dei rischi tipici di tale contesto, in funzione di rassicurazione sociale ed esorcismo dell'insicurezza collettiva[26]. Allo stesso modo, tale riflessione, nel confronto con sofisticati sistemi IAG e correlati pericoli, tenderà verosimilmente a riproporsi, con il rischio di alimentare – quando non sia possibile neutralizzare i nuovi rischi con divieti *tout court* – scelte politiche precauzionistiche e ultraresponsabiliste volte ad istituire in capo a utilizzatori e programmatori irreali doveri di controllo ad ampio spettro sull'attività algoritmica[27]. E ciò con una duplice conseguenza: sul piano penalistico, facendo ricorso a inaccettabili stravolgimenti del paradigma colposo, come già accaduto nelle dinamiche imposte dalla moderna società del rischio[28]; e su un piano più generale, disincentivando l'innovazione, impedendo così alla società di trarre beneficio da questa tecnologia.

È quindi alla luce di queste premesse che va affrontato il discorso volto ad individuare quale può e dev'essere l'ambito di un possibile reale utilizzo del diritto penale per fronteggiare adeguatamente i rischi rilasciati da questa nuova tecnologia. Per farlo, l'indagine si dipanerà lungo tre direttrici. Inizialmente si svolgerà una breve premessa tecnica sul funzionamento ed i limiti dei sistemi di IAG, con particolare attenzione alle differenze con i "tradizionali" sistemi di IA. Poi ci si soffermerà sul problema della regolamentazione e della responsabilità. Con riguardo al primo profilo, il lavoro si propone di scrutare i rapporti tra questa tecnologia ed il panorama normativo emergente a livello europeo, ponendo l'accento sul tema del controllo umano e della delimitazione di aree di rischio consentito; mentre, con riferimento al secondo, verranno esaminate le asperità probatorie che affliggono, sul terreno penalistico, l'allocazione delle responsabilità per eventi avversi prodotti dall'IAG. Nella parte conclusiva, saranno delineate alcune proposte per una futura dottrina penale del controllo dei rischi da ignoto algoritmico.

2. Caratteri e limiti dei modelli generativi: dall'IA specializzata verso un'IA a finalità generale.

Per comprendere il funzionamento e le possibili implicazioni giuridiche di ChatGPT è utile cominciare con una breve premessa teorica sulla nozione di IA.

Intesa nella sua accezione più ampia, l'IA è qualcosa che "si riconosce quando la si vede", ma che non è chiaramente definita. Nel dibattito tecnico non esiste una definizione unanimemente condivisa di IA, poiché le caratteristiche di una data applicazione sono definite dalle funzioni che persegue e dall'ambiente in cui opera[29]. Nel dibattito pubblico, di contro, l'IA è tipicamente considerata come una disciplina che mira a sviluppare sistemi computazionali in grado di compiere operazioni che richiederebbero le capacità cognitive e decisionali degli esseri umani[30]. Lo spettro di tecnologie riferibili a una simile definizione è, però, ampio e

[23] Cappellini (2023), cit., 12. Più in generale, in punto di *responsibility gap*, U. Pagallo e S. Quattrocolo, (2018), p. 385.
[24] Piergallini (2020), cit., 1746.
[25] Resta fondamentale il rinvio a Beck (1986).
[26] La letteratura sul punto è vasta, per cui si rimanda, *ex multis*, a Stortoni (2004); Perini (2018); Stella (2003).
[27] Cappellini (2023), cit., 28.
[28] V. Stella (2003), p. 221 e ss.
[29] Sull'indeterminatezza della nozione di IA v. Ubertis (2020), p. 76; McCarthy (2007). Che l'IA non è un concetto univoco è evidenziato da S. Legg e M. Hutter (2007), che individua oltre settanta definizioni diverse.
[30] I numerosi riferimenti rinvenibili nella letteratura scientifica tendono a convergere verso questa definizione. Per tutti, Kaplan (2016), p. 1, "programmi informatici capaci di comportamenti che riterremmo intelligenti se messi in atto da esseri umani", nonché Sartor (1996), "modelli computazionali capaci di eseguire compiti che richiederebbero intelligenza da parte dell'uomo". Quella elaborata dalla Commissione europea all'art. 3(1) della proposta di Regolamento UE sull'IA rappresenta una specificazione della definizioni appena richiamate: "un sistema progettato per operare con elementi di autonomia e che, sulla base di dati e input forniti dalla macchina e/o dall'uomo, deduce come raggiungere un determinato insieme di obiettivi utilizzando approcci basati sull'apprendimento automatico e/o sulla logica e sulla conoscenza, e produce output generati dal sistema come contenuti, previsioni, raccomandazioni o decisioni". *Proposta di Regolamento del Parlamento e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 21 aprile 2021, COM (2021) 206 final.

diversificato – da un veicolo senza conducente a una chatbot, da un *software* di *trading* ad alta frequenza a un robot industriale – con limitati punti di contatto.

Ma su un punto si registra un certo consenso: anche se ci sono esempi di IA ovunque si guardi, l'IA onnisciente e super intelligente, che di solito vuole conquistare il mondo nei romanzi distopici, non è ancora stata inventata e probabilmente mancano ancora diversi anni al traguardo[31]. Le tecnologie di IA in cui viviamo immersi perseguono perlopiù una funzione o un compito specifico (IA specializzata, o "*task-specific AI*"), mentre solo una parte limitata della ricerca in materia mira a replicare capacità simili a quelle umane (IA a finalità generali, o "*general purpose AI*"). In altre parole, si tratta di sistemi pensati per fare una cosa specifica (previsioni o classificazioni, guidare, riconoscere i volti nelle foto, raccomandare quale libro vuoi leggere successivamente, determinare se sei un buon rischio di credito, rilevare il cancro della pelle) – con l'ovvia conseguenza che tali sistemi, pur essendo migliori degli esseri umani nel loro ambito di addestramento, sono completamente inutili nel fare qualunque altra cosa diversa dal compito specializzato per cui sono stati progettati.

È alla luce di queste premesse che si coglie la portata del passaggio epocale in atto con la comparsa della IAG. Sistemi come ChatGPT e simili rappresentano i primi barlumi all'orizzonte dell'IA a finalità generale – quel momento a lungo profetizzato in cui le menti meccaniche supereranno i cervelli umani non solo quantitativamente in termini di velocità di elaborazione e dimensioni della memoria, ma anche qualitativamente in termini di intuizione intellettuale, creatività artistica e ogni altra facoltà distintamente umana[32]. Si tratta, in sostanza, di "modelli avanzati di apprendimento automatico che vengono addestrati per generare nuovi dati, come testo, immagini o audio"[33]; l'addestramento avviene "utilizzando varie tecniche per trovare schemi e relazioni nei dati in modo autonomo, senza che gli venga detto esplicitamente cosa cercare. Una volta appresi questi schemi, il modello è in grado di contestualizzare problemi anche molto complessi in maniera completamente autonoma, generando nuovi esempi simili ai dati di addestramento e nuovi contenuti".

Allo stesso tempo, però, l'architettura stessa di questi sistemi rende la perfezione difficile da raggiungere: avere una IAG non è come avere il genio della lampada, ma come avere un esercito di schiavi tonti ma onniscienti e molto veloci[34]. Le attuali versioni di questi sistemi non hanno prettamente coscienza di ciò che dicono o fanno, ma si limitano a valutare quale parola usare dopo quella che hanno appena selezionato, imitando informazioni prodotte dall'uomo in modo puramente statistico, anziché imparare effettivamente come funziona il mondo[35]. Per farlo, però, non attingono a una grande raccolta di informazioni verificate e aggiornate – che sarebbe del resto molto difficile da organizzare e mantenere aggiornata – ma attingono a enormi quantità di dati di testo provenienti dalle fonti più disparate reperibili su Internet – quindi anche quelle sbagliate[36]. Pertanto, per quanto sia a dir poco incredibile ciò che questi modelli sono in grado di fare, è ancora imperfetto: e in molti casi, un risultato imperfetto non basta. Per imbrogliare nello svolgimento di una traccia d'esame, almeno per lo studente che non ambisca al voto più alto, fa poca differenza; ma quando si tratta di applicazioni in cui sono in gioco beni giuridici (individuali o collettivi) ben più rilevanti (come nel settore medico, finanziario o bancario) un singolo errore rischia di avere conseguenze gravi e difficili da prevedere.

Proprio questa tendenziale fallibilità della macchina fa dell'IAG un vero rompicapo per il legislatore o le autorità di regolazione che tentino di prevenire o ridurre i rischi connessi agli innumerevoli tipi e applicazioni di questa tecnologia[37]. L'esempio dell'Italia, con il recente provvedimento dell'autorità Garante per la Protezione dei Dati Personali, che ha portato

[31] Per alcune interessanti riflessioni su questo passaggio generazionale, cfr. V. Muller e N. Bostrom (2016).
[32] Quelle che seguono sono le risposte fornite da ChatGPT ai seguenti *prompt*: "Cosa sono i modelli di IA generativa?" "Puoi spiegare le basi tecniche dei modelli generativi in modo semplice, in modo che un lettore inesperto possa comprenderle?".
[33] Si noti che la definizione di IA a finalità generali recentemente introdotta nella proposta di Regolamento UE all'art. 3(1) lett. B non è affatto dissimile da quella fornita da ChatGPT: si tratta di un sistema "destinato a svolgere funzioni di applicazione generale, quali il riconoscimento di immagini e vocale, la generazione di audio e video, il rilevamento di modelli, la risposta a domande, la traduzione e altre".
[34] Questa simpatica "definizione" è di Latronico (2022).
[35] Si registra già un certo scetticismo circa le reali capacità di ChatGPT, le cui risposte non sarebbero altro che una parafrasi o una "sfocata immagine del web". Più in generale sul punto, cfr. Chomsky (2023); nonché Chiang (2023).
[36] Europol Innovation Lab (2023), cit., 4. Il tentativo di correggere i possibili *bias* e creare un sistema più affidabile ha d'altra parte sollevato complesse questioni etiche, laddove è emerso come OpenAI abbia sfruttato lavoratori kenioti per effettuare correzioni manuali dei risultati di ChatGPT: cfr. Perrigo (2023).
[37] V. Hacker *et al.* (2023).

all'auto-sospensione del servizio per gli utenti italiani, ne è la prova[38]. Tra le varie obiezioni formulate in punto di protezione dei dati personali[39], il Garante della Privacy rileva che "le informazioni fornite da ChatGPT non sempre corrispondono al dato reale, determinando quindi un trattamento di dati personali inesatto". In buona sostanza, il timore più che fondato del garante è che gli utenti possano essere oggetto di diffamazione da parte di sistemi su cui è difficile agire o rivalersi[40].

Oltre ai prevedibili interrogativi di stampo etico, vengono dunque in gioco il problema della regolamentazione e della responsabilità. Temi con i quali avremo modo di confrontarci nel prosieguo di queste riflessioni.

3. Primi tentativi di regolamentazione dell'IAG: l'approccio europeo.

3.1. *La proposta di Regolamento sull'IA e la logica della precauzione moderata.*

Prima di porci il problema dell'ascrizione di responsabilità per le potenziali conseguenze negative, è forse opportuno affrontare preliminarmente la questione relativa ai rapporti tra rischio e precauzione[41].

Di fronte a sistemi che si ritiene siano o possano essere, almeno potenzialmente, fonte di pericolo per l'uomo, la prima decisione è extra e pre-penale – quindi di natura genuinamente politica[42]. Essa consiste nella scelta sul grado di rischio che si è disposti a tollerare nell'utilizzo di una certa tecnologia. Per un verso, nei casi in cui, a prescindere dai suoi potenziali benefici, un'applicazione presenti rischi difficilmente governabili ed evitabili da parte dell'uomo, non resta altra scelta che proibire in toto l'utilizzo della stessa. Per altro verso, i problemi maggiori nascono, logicamente, dopo che l'ordinamento, nell'alternativa tra consentire una certa attività o proibirla in radice, ha già optato per la prima soluzione. In questa ipotesi, il legislatore deve stabilire come governare preventivamente i rischi inerenti a una tecnologia rispetto ad applicazioni che si assumono utili e lecite, ritagliando a tal fine aree di rischio "algoritmico" consentito[43] presidiate da un apparato di sanzioni adeguato e funzionale alla tutela degli interessi coinvolti[44].

Sotto questo profilo, pur nell'attuale assenza di regole cautelari positivizzate, non si può non tener conto del quadro normativo emergente a livello europeo. Frutto maturo di un dibattito etico e giuridico da tempo in corso in seno alle istituzioni europee, la nuova proposta per un Regolamento europeo sull'IA (c.d. *AI Act,* per brevità "la proposta di Regolamento")[45], pubblicata nell'aprile del 2021 dalla Commissione, sembra fornire un primo quadro orientativo di misure cautelari e obblighi specificamente concernenti la messa in commercio e l'uso di sistemi IA (artt. 8-15). La proposta delinea una regolazione dell'AI proporzionata alla probabilità, al tipo e all'intensità del rischio rilasciato dall'applicazione che si intenda regolare (c.d. approccio *risk-based*)[46]. La regolazione basata sul rischio comporta l'individuazione di differenti classi di rischio e, specularmente, l'identificazione di regimi regolatori differenti.

[38] Garante per la protezione dei dati personali (2023).
[39] Le altre obiezioni del Garante per la Privacy riguardano la mancanza di una informativa agli utenti i cui dati vengono raccolti da OpenAI, per cui entrando nel sito si dà in sostanza esplicito consenso al trattamento dei dati, nonché l'assenza di qualsivoglia filtro per la verifica dell'età dei minori.
[40] Sebbene riteniamo che la posizione del Garante sia in linea di massima corretta, preme qui notare come il provvedimento si sia dimostrato ben poco efficace a fronte alla possibilità di aggirare facilmente il blocco avvalendosi di servizi VPN. Com'è agevole intuire, la portata sovranazionale (anzi, globale) del fenomeno esige l'attuazione di politiche sovranazionali, condannando all'inefficacia qualsiasi approccio normativo che si fondi e confronti unicamente con il contesto dell'ordinamento nazionale.
[41] Per una disamina dei complessi rapporti tra logica precauzionale, gestione del rischio e ricadute penalistiche, si rimanda a Ruga Riva (2006); Piergallini (2011); Castronuovo (2012).
[42] Stortoni (2004), cit., 83.
[43] Per un'approfondita disamina sul concetto di rischio consentito nel diritto penale moderno, con dovizia di riferimenti, si rimanda a Perini (2010), *passim*.
[44] Così Piva (2022), pp. 683 ss.
[45] V. *sub* nota 30.
[46] Per un commento all'approccio della proposta di regolamento, cfr. Contissa *et al.* (2021).

Così, per le AI considerate ad alto rischio (art. 6) sono previsti obblighi specifici, mentre vi sono sistemi vietati del tutto, perché, secondo la valutazione del legislatore europeo, pongono un rischio inaccettabile (art. 5)[47].

In particolare, per le IA ad alto rischio, la proposta sembra ritagliare aree di rischio consentito secondo una logica di precauzione moderata, stabilendo i limiti entro i quali è accettabile che un sistema di IA compia errori o causi danni; e lo fa statuendo espressamente che le figure soggettive tipizzate (ossia, il produttore, programmatore e l'utilizzatore della macchina, persona fisica o giuridica) siano gravate tanto da obblighi di condotta tipici articolati e complessi[48] quanto da disposizioni di principio – tra le quali primeggia quello di *accountability* e *human oversight* – che investono tutta la loro attività[49]. In questo senso, la proposta non prevede soltanto prescrizioni dirette e precise alla cui mancata applicazione segue l'irrogazione di una sanzione (si pensi alle misure minime di sicurezza) ma si fonda altresì su un obiettivo da realizzare (l'affidabilità, o *trustworthiness* della macchina) secondo modalità che lo stesso operatore deve, di volta in volta, determinare in ragione del livello di rischio. Si passa, dunque, da un approccio normativo che dettava indicazioni assai precise ad uno che impone a tali soggetti di modulare la concreta attuazione dei principi sanciti, in astratto, dalla normativa in materia.

In questa prospettiva, è immediatamente evidente la centralità attribuita al principio della supervisione umana nella gestione dei sistemi ad alto rischio. Difatti, l'art. 14 della proposta impone al fornitore o utilizzatore della macchina di adottare delle misure tecniche ed organizzative (come, ad esempio, strumenti di interfaccia uomo-macchina)[50] ritenute idonee a garantire un livello di controllo e intervento umano adeguato al fine di prevenire o ridurre al minimo i rischi connessi. Tali misure sono funzionali ad una piena comprensione delle capacità e limiti del sistema, il cui funzionamento deve essere monitorato per cogliere possibili segnali di disfunzione o anomalie ed eventualmente correggerli. Così, attraverso la previsione di un intervento umano di profondità variabile e direttamente proporzionale all'intensità e alla natura dei rischi generati dalla macchina, la proposta mira non solo a prevenire o governare il rischio della realizzazione di effetti pregiudizievoli, ma altresì ad individuare un soggetto responsabile qualora tale rischio si concretizzi ed egli risulti inadempiente rispetto ai propri obblighi di sorveglianza.

3.2. *Il problema del controllo dei sistemi di IAG: un compito impossibile?*

È sul quadro normativo appena tracciato che si innesta, da ultimo, la questione del governo dei rischi da IAG. Molte discussioni e proposte di eurodeputati si sono concentrate sull'opportunità di inserire o meno tale tecnologia nella categoria di AI ad alto rischio, mostrando subito una certa difficoltà di integrazione.

Tra le proposte di emendamento al testo del Regolamento più discusse va menzionata quella avanzata dal Consiglio europeo il 6 dicembre 2022, che, con il suo Orientamento Generale sulla Proposta della Commissione[51], definisce per la prima volta la categoria generale della *general purpose* IA come quei modelli in grado di svolgere un'ampia varietà di compiti per i quali non erano stati specificamente addestrati (art. 1 bis). Definizione, questa, che comprende anche ChatGPT e simili sistemi generativi. Questo emendamento, apparentemente innocuo, è diventato in breve il nucleo della regolamentazione delle IAG, nonché una delle disposizioni più contestate della proposta. Questo perché la versione del regolamento presentata dal Consiglio stabilisce che qualsiasi IAG che può essere utilizzato per un'applicazione ad alto rischio debba soddisfare tutti i relativi requisiti previsti dalla proposta[52].

Il problema posto da una simile soluzione è chiaro: proprio perché sono di uso generale, le IAG si prestano a uno sconfinato numero di applicazioni. In pratica, dunque, ogni IAG

[47] Vi rientrano, in particolare, i sistemi in grado di manipolare il comportamento umano attraverso tecniche subliminali, quelli che consentono ai governi di attribuire un "punteggio sociale", nonché i sistemi di identificazione biometrica remota in spazi accessibili al pubblico.
[48] Per i sistemi ad alto rischio, la proposta prevede obblighi di qualità dei *dataset* che alimentano il sistema (art. 10), documentazione (art. 11), registrazione degli eventi (art. 12) e trasparenza (art. 13), funzionale alla valutazione dei rischi ex ante (art. 9) e alla sorveglianza umana (art. 14), oltre che alla prevenzione di discriminazioni, nonché di affidabilità (art. 15).
[49] Per una completa disamina di tali principi, v. Giannini (2022), p. 16 ss.
[50] Tale capacità di controllo ed intervento sono meglio esplicitati al paragrafo 4 dell'art. 14, laddove tali misure servono a supportare tutta una serie di azioni indicate da questa disposizione.
[51] Per le modifiche proposte dal Consiglio, v. il Comunicato stampa del 6 dicembre 2022 pubblicato sul sito www.consilium.europa.eu.
[52] Art. 4b della proposta come modificata dall'orientamento generale del Consiglio.

sarà qualificata come sistema ad alto rischio. Di conseguenza, il fornitore sarà chiamato a predisporre un sistema di gestione del rischio efficace per tutti i possibili usi del sistema - un compito che rasenta l'impossibile, data la quantità di applicazioni potenziali, e la cui complessità è destinata ad aumentare con quella di tali modelli. Non si comprende, infatti, come il fornitore possa elencare tutte le possibili applicazioni, determinare *ex ante* i rischi per tutti i diritti e beni giuridici coinvolti e sviluppare strategie di prevenzione o mitigazione rispetto ad un modello linguistico (come GPT) il cui utilizzo potrebbe spaziare dalla creazione di una chatbot per l'assistenza clienti di un sito web alla fornitura di un canale di contatto riservato per denunciare violenze e abusi.

D'altra parte, tale problematica si ripercuote anche – e con maggior vigore – sulla posizione dell'utilizzatore. È evidente il rischio che dietro questa soluzione si celi una scelta politica ultraresponsabilista, volta ad estendere il ruolo e i doveri di controllo dell'utilizzatore in maniera del tutto irrealistica: in che misura sussiste un potere materiale ed effettivo di intervento in capo a tale soggetto? È opportuno gravare l'utilizzatore di un vero e proprio obbligo giuridico di controllo e intervento rispetto all'attività di un sistema di IAG? Ove si ritenga di procedere in tal senso, l'utilizzatore potrebbe essere ritenuto responsabile degli eventi avversi derivanti dal malfunzionamento dell'IAG, in quanto riconducibili al malgoverno (o omesso governo) della fonte di rischio.

Nel prosieguo di queste riflessioni avremo modo di constatare l'inammissibilità pratica di un simile obbligo a carico dell'utilizzatore e, dunque, l'impossibilità teorica di costruire una sua responsabilità a titolo di colpa.

4. Il dilemma della praticabilità del diritto penale d'evento: variazioni sul tema della responsabilità da IAG.

4.1. *Profili di imputazione dolosa.*

Immaginiamo il seguente scenario:

La Società Alpha ha fornito alla chatbot un grande dataset di notizie finanziarie e di informazioni su società quotate in borsa. ChatGPT, utilizzando il suo algoritmo di apprendimento automatico, è stato in grado di identificare una società, la Beta Inc., che stava per annunciare un importante accordo commerciale che avrebbe avuto un impatto significativo sul valore delle sue azioni. La chatbot ha quindi effettuato l'acquisto di grandi quantità di azioni della Beta Inc. Sennonché, successivamente si scopre che l'informazione che ChatGPT ha utilizzato per identificare questa opportunità d'investimento era in realtà informazione privilegiata, ovvero informazione riservata non ancora resa pubblica e non disponibile per il mercato, che era stata precedentemente sottratta da un ex dipendente della Beta Inc. che aveva accesso a queste informazioni in quanto insider.

Questo caso – che forse collocheremmo nel quasi-futuribile, ma che ad avviso di chi scrive è destinato ad assumere un rilievo applicativo sempre maggiore nel futuro prossimo – rappresenta un valido punto di partenza per avviare una riflessione circa la possibilità di isolare un soggetto e/o centro di interessi cui riferire gli eventi avversi (di danno o di pericolo) eventualmente indotti dall'agente artificiale generativo.

A questo riguardo, è utile partire da un'osservazione di carattere generale, forse banale, ma certamente fondamentale al fine di sgombrare il campo da possibili equivoci. Una IAG non può *de iure condito* essere essa stessa centro di imputazione della responsabilità penale, poiché non è un agente nel senso penale del termine[53]. In generale, una chatbot (ma il discorso è riproducibile per ogni agente artificiale) non agisce ma è agito: esso non ha la capacità di agire in modo consapevole e volontario, che sono caratteristiche fondamentali dell'agire responsabile. Ne deriva che, almeno per il momento e nel prossimo futuro, una chatbot non potrà avere alcuna personalità giuridica, restando uno strumento nelle mani dell'uomo.

[53] Benché meritevole di approfondimento, la questione è indipendente da quella attinente alla responsabilità dell'umano dietro la macchina. Per un breve riassunto del dibattito dottrinale in materia si rinvia, *ex multis*, a Basile, (2019), p. 27 ss.; nonché, da ultimo, Consulich (2022), p. 1020 ss.

Veniamo, dunque, all'analisi dei profili della responsabilità penale della persona (fisica o giuridica) dietro la macchina. I criteri di individuazione della responsabilità dell'utilizzatore possono essere teoricamente ricondotti allo schema dell'autorìa, a quello della responsabilità concorsuale o a quello dell'omissione di controlli finalizzati all'impedimento di eventi illeciti.

Anzitutto, è possibile inquadrare l'ex dipendente della Beta Inc. come autore del reato di abuso di informazioni privilegiate? A tal proposito, l'imputazione presuppone che tale soggetto, "essendo in possesso di informazioni privilegiate[54], acquista, vende o compie operazioni (per conto proprio o di terzi) su strumenti finanziari avvalendosi di quelle stesse informazioni, oppure comunica a terzi tali informazioni, ovvero fornisce consigli sulla base di esse"[55]. Sennonché, a ben vedere, l'attribuzione del fatto illecito si scontra in questo caso con l'assenza di un meccanismo di imputazione della responsabilità all'uomo, allorché questi non sia autore diretto del fatto, ma sfrutti a fini illeciti l'interazione con una forma di IAG. Sebbene il soggetto in questione abbia indebitamente sottratto un'informazione privilegiata, egli non ha tuttavia effettuato direttamente l'operazione di acquisto delle azioni; né, d'altra parte, può sostenersi che egli abbia compiuto il fatto "per mezzo" di un mero strumento informatico.

Sotto questo profilo, il rapporto di strumentalità uomo-macchina va in qualche modo riletto quando riferito a sistemi di IAG, non essendo più limitato ad una dimensione puramente meccanicistica. Al contrario, tale rapporto si arricchisce di un'ulteriore dimensione "creativa", costituita dall'autonomia operativa del sistema generativo: più aumenta la "quota" di autonomia della macchina nel concretizzare il progetto criminoso dell'umano, più la distanza tra fatto concreto compiuto dalla prima e generiche istruzioni lesive inserite dal secondo è destinata ad aumentare[56]. Così, sebbene sia verosimile ipotizzare che l'ex dipendente di Beta Inc. abbia sottratto l'informazione al fine di trarne profitto, sarà comunque la macchina a definire materialmente il *quomodo* del progetto illecito con modalità non sempre prevedibili. Di conseguenza, la prova dell'elemento soggettivo in capo al soggetto umano diviene tanto più problematica quanto maggiore è il *quantum* di fatto tipico compiuto automaticamente dalla macchina senza la copertura dell'elemento soggettivo dell'individuo[57], atteso che potrebbe risultare carente una piena rappresentazione e volizione di tutti gli elementi della fattispecie di reato in mancanza di una completa consapevolezza circa l'evoluzione della condotta algoritmica. L'estremo limite di rimprovero, dunque, potrebbe essere limitato soltanto alle condotte poste in essere con dolo eventuale, ma anche in questi casi si registrerebbero tensioni con il principio di responsabilità personale e colpevole a causa della difficoltà di derivare tale stato mentale dalla rappresentazione "sopravvenuta" in ordine all'evento illecito *singulatim* perfezionato nei suoi elementi essenziali (*tempus* e *modus*) da un altro "soggetto".

Né, d'altra parte, tali difficoltà paiono superabili facendo ricorso allo schema della responsabilità concorsuale. Proprio il concorso di persone è lo strumento invocato più di frequente per tentare di fornire soluzione ai problemi di qualificazione del fatto compiuto da un agente artificiale[58]. In particolare, quest'ultimo fungerebbe da autore materiale di un reato progettato dalle prime. Sennonché, come è stato opportunamente notato[59], l'utilizzazione dello schema concorsuale è destinata ad assumere una valenza assai limitata in questi casi, a causa della difficoltà di ritenere che l'umano sia concorso nel reato commesso da un "altro" soggetto. A ben vedere, tale opzione è logicamente scorretta, poiché l'agente artificiale, come detto, non essendo dotato di una soggettività giuridica propria, non si pone rispetto all'individuo come invece questo fa ad esempio nei confronti di persona non imputabile o non punibile *ex* art. 111 c.p. In altri termini, non siamo in presenza di due soggetti distinti di cui uno in rapporto di funzionalità rispetto all'altro, ma di un unico soggetto (quello umano) che si avvale di un mezzo ad elevata complessità tecnologica per realizzare i propri obiettivi. Pertanto, nessun concorso di persone è ipotizzabile tra uomo e macchina.

[54] Per informazione privilegiata (detta anche *price sensitive*) si intende un'informazione specifica di contenuto determinato, di cui il pubblico non dispone, concernente strumenti finanziari o emittenti di strumenti finanziari, che, se resa pubblica, sarebbe idonea a influenzarne sensibilmente il prezzo.
[55] Art. 184 D.lgs n. 58/1998 come articolo modificato dalla Legge n. 238/2021. Si rinvia per un'analisi approfondita della fattispecie a Sgubbi et al. (2013).
[56] Consulich (2022), cit., 1035.
[57] *Ibidem*.
[58] Si fa riferimento qui alle dottrine di provenienza angloamericana della *innocent agency* o della *perpetration by another*, spesso invocate per prefigurare un possibile concorso di persone, tra quelle fisiche e quelle artificiali. Nella dottrina continentale, soprattutto quella di stampo tedesco, invece, si può richiamare la dottrina dell'autore mediato. Per un'analisi approfondita, Consulich (2022), p. 1033 ss.
[59] *Ibidem*.

Proprio la ridotta capacità operativa dei due criteri ora esaminati potrebbe indurre verso la costruzione di una responsabilità colposa dell'operatore conseguente alla violazione di un obbligo giuridico di impedire eventi illeciti, similmente a quanto potrebbe già accadere per il conducente di un'auto a guida semiautonoma rispetto agli eventi avversi da questa cagionati.

4.2. *Profili di imputazione colposa.*

Se l'imputazione dolosa, come visto, è tendenzialmente disattivata dalla distanza tra fatto concreto compiuto dall'agente artificiale e condotta tenuta dall'operatore, quella colposa sembra *prima facie* promettere risultati migliori, poiché a rilevare sarebbe un'omessa supervisione della fonte di rischio costituita dall'IA stessa. Così, in casi come quello sopra descritto, ove sussista un potere-dovere di controllo e intervento in capo all'utilizzatore sulle funzioni esercitate dalla macchina, ben potrebbe configurarsi un addebito di responsabilità ex art. 40, comma II c.p. per il mancato impedimento di eventi avversi causati dalla macchina a fronte di un prevedibile fallimento della stessa. Un esempio chiarirà il punto.

Si prenda il caso classico delle auto a guida semiautonoma, ossia veicoli che possono realizzare tutte le manovre necessarie per la guida ma che presuppongono la costante supervisione del conducente[60]. Quest'ultimo, pur non partecipando attivamente alla guida del veicolo, sarà chiamato ad intervenire ogniqualvolta il sistema di IA gli notifichi una richiesta esplicita in tal senso. Secondo alcuni autori, tale richiesta attiverebbe una posizione di garanzia del conducente chiamato a riprendere il controllo della vettura al fine di gestire una situazione di rischio ed impedire il verificarsi di eventi avversi derivanti dal malfunzionamento della macchina[61]. L'attribuzione dell'evento illecito non impedito potrà dunque fondarsi sulla disciplina del comma II dell'art. 40 c.p., avendo l'utilizzatore tenuto un comportamento *lato sensu* omissivo in violazione di un obbligo giuridico di controllo e intervento rispetto a un agire di mano dell'agente artificiale[62].

Tuttavia, se da un lato i "tradizionali" sistemi di IA ad oggi prevalentemente in uso, progettati per coadiuvare ma non sostituire l'umano nel compimento di certe attività (come appunto la guida su strada), non sembrano sottrarsi (ancora) al controllo umano, sì da atteggiarsi a meri strumenti nelle mani dell'uomo, le cose sono destinate a complicarsi laddove a causare l'evento avverso sia un sistema di IAG dotato di un grado di autonomia tendenzialmente piena e completa. Si confronti il caso dell'auto a guida semiautonoma con il seguente scenario:

La Società Gamma ha deciso di utilizzare una IAG per assistere i clienti nelle loro transazioni finanziarie, come il trasferimento di denaro, il pagamento delle bollette e simili. La chatbot è stata addestrata su un vasto insieme di dati sulle transazioni finanziarie ed è stato progettato per comprendere e rispondere a una vasta gamma di domande relative alle finanze. Un giorno, un cliente contatta la chatbot attraverso il sito web dell'azienda per chiedere informazioni sul trasferimento di una grossa somma di denaro su un conto estero. La chatbot risponde alla richiesta fornendogli le informazioni e le istruzioni necessarie per iniziare il trasferimento. Tuttavia, durante questa conversazione, la chatbot non riesce a verificare correttamente l'identità del cliente, causando il trasferimento del denaro su un conto estero associato a frodi e operazioni di riciclaggio di denaro.

In questo caso, la "novità" rispetto al passato recente, che è data dalla capacità dei nuovi sistemi di IAG di affrancarsi progressivamente dalla persona umana che la controlla e di assumere una gestione operativa sempre più autonoma, rende difficile stabilire *a priori* a quale persona fisica sia da ascrivere il fatto di riciclaggio di denaro posto in essere dalla macchina. Ciò è reso difficile, se non impossibile, anzitutto dalla frammentazione delle responsabilità lungo la catena di approvvigionamento dell'agente artificiale, ossia il cd. problema degli "attori mul-

[60] Per un'approfondita disamina della tematica delle auto a guida autonoma, si veda per tutti Cappellini (2019), nonché Picotti (2021), e i rimandi dottrinali ivi contenuti.
[61] Così Cappellini (2019), pp. 334-336.
[62] Si ripropone qui l'annoso problema dell'individuazione dell'esatto confine tra azione commissiva e omissiva in ambito colposo, dovuto, come noto, alla presenza di una componente omissiva in ogni condotta colposa nonché al comune carattere normativo di omissione e colpa. Così Viganò (2013), cit., 391. Così, con riguardo al caso dell'auto a guida autonoma, l'omissione del controllo da parte del conducente potrebbe ben rilevare non come omissione in sé rispetto all'agire dell'IA, quanto piuttosto come violazione delle ordinarie regole sulla circolazione stradale (mantenere il controllo del veicolo) inserita in una condotta complessivamente commissiva (la guida del veicolo). Tuttavia, preme qui sottolineare che laddove l'autonomia della macchina è tendenzialmente completa (come nel caso dei sistemi di IAG), la condotta di omissione di controllo e/o intervento avrà carattere complessivo indiscutibilmente omissivo, essendosi l'utilizzatore limitato a sorvegliare un'attività "altrui".

tipli"[63]. Data l'elevata complessità tecnica del loro processo di sviluppo, tali sistemi sono spesso sviluppati all'interno di una rete plurisoggettiva in cui intervengono una molteplicità di individui, organizzazioni, componenti e processi chiamati a confrontarsi con una quantità di scenari vastissima e potenzialmente indefinita: difficile, dunque, che si riesca a identificare il soggetto (o i soggetti) responsabili per la cellula funzionale da cui è scaturito il difetto concretizzatosi in illecito[64]. In questo scenario, caratterizzato da una molteplicità di soggetti potenzialmente coinvolti nella produzione dell'evento avverso, la responsabilità penale potrà essere frazionata e il legame di causa ed effetto rischia di diluirsi in una semplice influenza. In altri termini, l'azione causativa del fatto illecito potrebbe essere ricondotta tanto all'utilizzatore, quanto a un difetto di programmazione, di costruzione, o di informazione, eventualmente interagenti *pro quota* alla stregua di concause, nel contesto di una vera e propria *web of causation*[65].

Ma, anche ipotizzando di riuscire a superare le difficoltà connesse all'esatta individuazione del singolo (o dei singoli) soggetto umano responsabile, residuerebbe comunque il problema di fondo dell'improbabile sussistenza in capo allo stesso di un effettivo potere-dovere di controllo e intervento sulle funzioni esercitate dalla macchina. Per un verso, infatti, tali sistemi mettono sotto scacco il loro creatore, che precipita nella desolante condizione di aver creato agenti artificiali che possono rilasciare rischi non schermati, nella piena consapevolezza di non poter far nulla per "prevedere l'imprevedibile" ed evitare che questo possa accadere[66]; per altro verso, essi riducono il ruolo dell'utilizzatore a quello di mero controllore di un'attività della macchina del tutto indipendente, se non addirittura a quello di mero fruitore passivo di un servizio automatizzato, privo persino della possibilità di interferire con l'azione artificiale[67]. Di conseguenza, se a livelli di automazione più basilari la persistenza di un effettivo potere-dovere di intervento in capo all'utilizzatore garantisce che vi sia sempre un soggetto garante in grado di impedire che un malfunzionamento della macchina cagioni danni altrimenti evitabili, lo scenario muta sostanzialmente in relazione ai sistemi di IAG tali da escludere tendenzialmente (se non del tutto) la stessa materiale possibilità di un intervento correttivo dell'uomo sulle scelte della macchina.

Infatti, in linea di principio, l'imposizione di un obbligo di agire presuppone che l'agente sia consapevole delle circostanze che determinano il prevedibile fallimento del sistema ed abbia il potere di impedire la verificazione dell'evento attraverso una condotta esigibile. Sotto il primo profilo, si fa riferimento al problema della "riconoscibilità", da parte del controllore, dell'avaria e, dunque, del momento a partire dal quale è necessario intervenire. Vista la difficile leggibilità del comportamento artificiale e l'assenza di un meccanismo corrispondente all'*override button* delle auto a guida autonoma, la possibilità che il supervisore riesca ad entrare nel merito del processo algoritmico, individuare l'anomalia e correggerla "in corsa" rischia di rimanere un'ipotesi remota. Al contrario, e più verosimilmente, questi tenderà a fare affidamento sulle decisioni del sistema, tanto più se questo è stato certificato, a meno che non abbia motivi specifici per ritenere che esso sia malfunzionante, o che non sia in grado di incorporare nella sua valutazione elementi ulteriori ed esterni al sistema stesso. Così, un addebito di responsabilità a titolo omissivo ben potrebbe configurarsi in caso di omessa attivazione a fronte di un fallimento del sistema che sia prevedibile – in astratto, a causa dell'inadeguatezza dei meccanismi di controllo preventivi, ovvero in concreto, per via di circostanze di fatto anomale – e che renda inoperante l'affidamento dell'uomo circa il funzionamento dello stesso in conformità al protocollo preventivamente stabilito per l'uso di quella macchina[68]. Si pensi, ad esempio, al caso in cui una chatbot istighi qualcuno a realizzare azioni che mettano a rischio la sua integrità fisica. In questa ipotesi, a rilevare sarebbe un'omessa o insufficiente supervisione, volta a inibire quelle operazioni che non rientravano più nel protocollo di funzionamento del sistema, a patto che le cause del fallimento fossero conosciute o conoscibili.

Si tratta però – lo si può ben intuire – di ipotesi perlopiù marginali. Infatti, l'opacità e

[63] Nella dottrina italiana, il tema del c.d. *many hands problem* è segnalato da Magro (2020), p. 3.
[64] Consulich (2022), cit., 1049.
[65] L'espressione è di Piergallini (2020), cit., 1762.
[66] *Ivi*, p. 1749, che definisce questa condizione paradossale del creatore come "prevedibilità dell'imprevedibilità".
[67] Così Cappellini (2023), p. 29.
[68] Sebbene, infatti, vi siano sistemi e procedure di controllo tali da impedire al chatbot di dire, consigliare o fare azioni sbagliate o illecite, gli utenti hanno in più occasioni dimostrato come tali sistemi di controllo possano essere furbescamente aggirati Ad esempio, chiedendo al programma di generare una sceneggiatura di un film che parla di come occultare un cadavere o rapinare una banca è un modo per eludere il suo rifiuto di rispondere a una richiesta diretta su fatti che possono implicare una condotta penalmente rilevante. Sul punto, Europol Innovation Lab (2023), cit., 5.

l'enorme potenziale applicativo dei sistemi IAG rende assai difficile comprendere come l'individuo posto a sorveglianza della macchina possa, per tutti i tipi di applicazioni della stessa, esercitare un efficace intervento correttivo o inibitorio rispetto a operazioni anomale sulla base di una imperfetta comprensione delle capacità, limiti e output del sistema. Il riconoscimento che un tale intervento vale al più per limitare "a cose fatte" gli effetti lesivi del malfunzionamento, ma si rivela inefficace per una tutela completa "in corsa" dei beni aggredibili dall'IAG, rappresenta solo il frutto di una corretta valutazione della speciale complessità tecnica della materia.

L'effetto complessivo, così, è che tale problematica conduce alla sostanziale inammissibilità pratica di un obbligo di controllo e intervento a carico dell'operatore e, dunque, all'impossibilità teorica di costruire una sua responsabilità a titolo di colpa.

4.3. *La responsabilità da reato degli enti: societas (cum machina) delinquere potest?*

Constatata la tendenziale impossibilità di individuare un individuo dotato di un congruo coefficiente di colpevolezza che possa rispondere del fatto dell'IAG, non resta che esplorare un'ultima via: quella della responsabilità da reato della persona giuridica[69].

In linea di principio, quando il fatto dell'agente artificiale si verifica nell'ambito di un'organizzazione complessa e non si individuino i soggetti umani responsabili all'interno dell'impresa, dovrebbe potersi formulare un rimprovero a titolo di colpa di organizzazione all'ente, che si sia avvalso dell'IAG in assenza di idonee cautele, ai sensi dell'art. 8 del d.lgs. 231/2001[70].

Sennonché, neppure questa soluzione è immune da rilievi, né tantomeno può ritenersi risolutiva di ogni questione. Anzitutto, va sottolineato che, sebbene racchiuda i prodromi di una forma di responsabilità autonoma ed esclusiva dell'ente, quella ex art. 8 è in realtà un'imputazione ancora concettualmente vicariale, cioè fondata sulla prova dell'obiettiva realizzazione di un fatto illecito da parte di un individuo non imputabile, punibile o individuato[71]. Pertanto, mentre può ben configurarsi una responsabilità dell'ente per il caso in cui si sa che un reato è stato commesso, ma non lo si può accertare perché non si riesce a identificare il suo autore, non è affatto scontato che se si possa ricorrere alla disciplina ex art. 8 nel caso in cui si sa in radice che un reato *non* è stato commesso per via della difficoltà di imputare l'evento avverso a un individuo che, pur eventualmente identificato, non partecipa più in alcun modo dell'azione della macchina.

Si tratterebbe qui, in sostanza, di una forma di imputazione diretta ed originaria della *societas* per il "fatto proprio" dell'agente artificiale[72]. Un'ipotesi, questa, che non solo

esula, in linea di principio, dall'ambito di applicazione della disciplina ex art. 8, ma che rischia altresì di trasformarsi in una forma di responsabilità sostanzialmente oggettiva dell'ente, che collega automaticamente la mancata individuazione del soggetto umano responsabile ad una carenza organizzativa[73]. Pertanto, ogni eventuale sforzo in tale direzione in un'ottica *de iure condendo* dovrebbe perlomeno garantire che il giudizio di colpevolezza dell'ente sia fondato sull'accertamento del nesso tra evento avverso e carenza organizzativa[74].

Per il momento, comunque, non si può non pervenire alla conclusione di una scarsissima capacità di tutela del diritto penale rispetto ai rischi rilasciati dall'IAG, sia con riferimento alle persone fisiche che a quelle giuridiche. Preso atto della difficile compatibilità di siffatta materia con i canoni del diritto penale, occorre ora affrontare il discorso volto a comprendere in che modo i rischi rilasciati da questa nuova tecnologia vadano governati e, soprattutto, se possa ancora spettare un ruolo al diritto penale.

[69] La proposta di imputare in capo all'ente gli eventi illeciti commessi da sistemi di IA conta già diversi contributi, sia nella dottrina angloamericana che in quella continentale. Per tutti, Mazzacuva (2021); Diamantis (2020); Diamantis (2021).
[70] Art. 8 D.lgs. 8 giugno 2001, n. 231, "Autonomia delle responsabilità dell'ente".
[71] Questa tesi è sostenuta da Pulitanò (2002), p. 963.
[72] Cfr. Consulich (2018), p. 197 ss., il quale sostiene la necessità di una forma di responsabilità indipendente in capo all'ente, la cui sussistenza richieda la management failure e la oggettiva sussistenza di un fatto di reato, senza la mediazione della colpevolezza di una persona fisica.
[73] In questi termini si esprime Piergallini (2020), p. 1756 ss.
[74] Per un approfondimento dei principali snodi dogmatici relativi alla struttura dell'illecito penale dell'ente come delineato dall'art. 8 del d.lgs. 231/2001, v. Paliero (2008).

5. Alla ricerca di un (pur limitato) ambito di utilizzo del diritto penale.

5.1. *Verso un approccio regolativo proattivo.*

Scartata sia perché impraticabile, sia perché ben poco proficua, la via di una risposta punitiva strutturata secondo i canoni classici del diritto penale d'evento; scontato, in ogni caso, un forte ridimensionamento delle aspettative dei possibili risultati ottenibili dall'intervento penale, la residua via percorribile diviene obbligata. Essa non può che andare nella direzione di un diritto di stampo proattivo in grado di intercettare i rischi e governare in anticipo le problematiche connesse ai sistemi di IAG, secondo un'impostazione che ispira la stessa proposta di Regolamento UE[75].

Quest'ultima, difatti, sembra orientata verso una strategia preventiva che mira a coinvolgere direttamente gli operatori nel campo dell'IA nella determinazione delle regole da rispettare nello sviluppo e nell'utilizzo di sistemi intelligenti[76]. A tal proposito, sono due gli aspetti da considerare. In primo luogo, come spiegato dalla Commissione europea nella relazione introduttiva alla proposta, il fornitore di sistemi di IA ad alto rischio è tenuto, ex art. 16, a rispettare i requisiti stabiliti dal capo 2, con la precisazione che "le soluzioni tecniche precise atte a conseguire la conformità a tali requisiti possono essere previste mediante norme o altre specifiche tecniche o altrimenti essere sviluppate in conformità alle conoscenze ingegneristiche o scientifiche generali, a discrezione del fornitore del sistema di IA"[77]. In secondo luogo, l'art. 17 specifica che la conformità ai requisiti del regolamento dovrà essere assicurata attraverso l'adozione di un sistema di gestione della qualità.

Come si vede, la strategia adottata dalla proposta consiste nel lasciare libertà decisionale al fornitore di sistemi di IA in ordine al *quomodo* della gestione del rischio: sarà quest'ultimo a "scegliere il modo in cui soddisfare i requisiti che lo riguardano, tenendo conto dello stato dell'arte e del progresso tecnologico e scientifico nel settore"[78].

Ad avviso di chi scrive, dunque, la sfida per il futuro dell'AI Act sarà quella di applicare una simile strategia di tipo proattivo nel governo dei rischi rilasciati dall'IAG, adattandola opportunamente alle specificità di tale tecnologia. Questo risultato potrebbe essere conseguito tramite l'imposizione di obblighi diretti agli utilizzatori di sistemi di IAG, che ne circoscrivano, indirizzandola, la facoltà di adattamento dei requisiti del Regolamento alle specificità dell'applicazione in uso e della realtà organizzativa. Così, ad esempio, sarà l'ente creditizio che utilizzi un'IAG per assistere i clienti nelle loro operazioni finanziarie a dover predisporre un adeguato apparato organizzativo idoneo all'individuazione, valutazione e comunicazione alle competenti autorità del livello di rischio, nonché all'eventuale adozione di misure di contenimento – e non il fornitore, spesso non in condizione di fornire una copertura di tutela preventiva in relazione a tutti i rischi rilasciati dall'intera gamma di possibili usi del sistema. In questo modo, non solo si evita una regolamentazione proibitiva e inefficiente alla fonte, che potrebbe soffocare l'evoluzione tecnologica, ma si garantisce altresì all'utilizzatore libertà decisionale in merito al modo in cui soddisfare i requisiti che lo riguardano, sia adattandoli specificamente ai caratteri e ai rischi connessi ai sistemi IAG ed alle nuove casistiche che questi indurranno, sia se necessario, sviluppandone di nuovi.

Si introdurrebbero, così, dei veri e propri obblighi di autodisciplina che dovranno essere presidiati da un apparato di sanzioni di varia entità e natura, anche penale, adeguato e funzionale alla tutela degli interessi coinvolti, nel quadro di una *regulated self-regulation*.

5.2. *Prospettive de iure condendo.*

In un simile contesto di stampo proattivo, il diritto penale può ancora trovare adeguato

[75] Su questa stessa linea già Piergallini (2020), cit., 1746. Cfr. anche La Vattiata (2022) e Mobilio (2020).
[76] *Ivi*, p. 401 ss.
[77] *Relazione introduttiva alla proposta*, para. 5.2.3.
[78] *Ibidem*.

spazio per un'azione efficace e non simbolica, strettamente raccordata alla disciplina extra-penale in materia, a patto però di porre corrette condizioni a base del suo intervento. Tali condizioni afferiscono, da un lato, alla tipologia delle sanzioni, dall'altro ai soggetti responsabili (persone fisiche ma anche enti).

Quanto alla tipologia delle sanzioni, preso atto dell'ineffettività di tecniche sanzionatorie dipendenti dalla concretizzazione di un evento lesivo (che il più delle volte sfugge alla capacità di previsione dell'agente umano), la legislazione penale dovrà ripiegare verso modelli di incriminazione fortemente condizionati dall'approccio preventivo o anche solo cautelativo della normativa extra-penale, al fine di rafforzarne l'osservanza[79]. In quest'ottica, la via indubbiamente più immediata è quella di ricorrere a reati di mera condotta e, quindi, di pericolo presunto[80]. Il ruolo del diritto penale, dunque, si "semplifica" nel punire l'inosservanza dei suddetti obblighi di autodisciplina e comunicativi nonché delle misure la cui adozione venga imposta dalle autorità di settore.

Così, ripercorrendo parallelamente l'*iter* extra-penale, le fattispecie penali in questione potranno concernere anzitutto i sistemi IAG rientranti nella categoria del "rischio inaccettabile", che impedisce qualsiasi pratica di IAG in settori o per scopi specificamente indicati dal legislatore, data la loro intrinseca pericolosità. In siffatti ambiti, si tratta in sostanza di sanzionare la violazione dell'eventuale divieto di impiegare tali sistemi in determinati settori o per certi scopi ovvero in assenza delle autorizzazioni prescritte per il suo utilizzo.

Per quanto riguarda, invece, le applicazioni di IAG consentite ma connotate da un rischio alto, la responsabilità dell'operatore potrebbe fondarsi sulla mancata realizzazione di efficaci meccanismi preventivi di protezione idonei alla valutazione e prevenzione dei rischi tecnologici, non ancora degenerati in eventi avversi, come pure l'omessa tempestiva attivazione di misure di sicurezza in caso di segnali di allarme[81]. Ad esse potrebbero affiancarsi, da una parte, ipotesi di responsabilità ex art. 2638 c.c. in versione "algoritmica", volte a sanzionare le omesse o false comunicazioni rese all'autorità amministrativa eventualmente preposta di informazioni rilevanti per la gestione del rischio, come ad esempio gli indicatori di performance del sistema nonché le anomalie ed i danni verificatisi durante la sua attività[82]. Dall'altra parte, strategie di indagine e di gestione del rischio, coordinate dai decisori amministrativistici, ma il più possibile condivise con gli operatori del settore nelle diverse fasi dello sviluppo e utilizzo di sistemi di IAG. Lungo tale direzione, per il diritto penale si profila una funzione "servente", vale a dire di rinforzo di decisioni prese altrove secondo lo schema di un diritto penale "ingiunzionale"[83].

In definitiva, un sistema ben noto e sperimentato già in vari settori (*in primis* il mercato finanziario) che si caratterizza, da un lato, per la presenza di reati, commissivi ed omissivi, ma sempre di mera condotta; e, dall'altro, per la natura sostanzialmente sanzionatoria di un siffatto diritto penale ossia per un ruolo di vigilanza – e non di controllo sociale – dei comportamenti e delle iniziative di conformazione che assicuri la duplice esigenza di assicurare un uso responsabile e sicuro della tecnologia e, al tempo stesso, di costruire una cornice giuridica che non si riveli un ostacolo all'innovazione.

Venendo ora al discorso sulla tipologia dei soggetti responsabili, punto d'avvio è il fatto che la violazione delle prescrizioni extra-penali di settore, l'omessa o falsa comunicazione e così via, possono essere astrattamente realizzate e, quindi, imputate sia alle persone fisiche che a quelle giuridiche.

Così, con riferimento alla responsabilità delle persone fisiche, non v'è dubbio che la pena detentiva debba essere mantenuta anche per questi reati, proprio per la sua particolare efficacia dissuasiva. Che poi, come già segnalato, possano presentarsi obiettive difficoltà nell'individuazione del destinatario del precetto e, quindi, della persona fisica responsabile nell'ambito di

[79] Diversi sono i contributi che richiamano questa esigenza, per tutti: Consulich (2022), cit., 105; Troncone (2022), cit., 3298.
[80] Per l'analisi in chiave sistematica di tale espressione, sia consentito il rinvio a Perini (2010), p. 398 ss.
[81] Così Consulich (2022), cit., 1051.
[82] Rubricato "Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza", l'art. 2638 c.c. comma 1 punisce il comportamento di "amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazione, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, sono puniti con la reclusione da uno a quattro anni".
[83] Già sperimentato in ambito ambientale e infortunistico, il modello ingiunzionale non segue lo schema classico "se fai A allora B", bensì quello ben diverso secondo cui "ti ingiungo di fare A e se non fai A, allora B". Cfr. Piergallini (2020), cit., 1773, che parla a tal riguardo di "*cooperative compliance*". Più in generale, Marinucci (2005), p. 55.

strutture societarie complesse o, più in generale, della catena di approvvigionamento del prodotto artificiale, non muta, a ben vedere, i termini della questione. Che siffatto problema venga risolto a livello interpretativo o che, di contro, sia il legislatore a fissare i criteri per l'individuazione del soggetto responsabile all'interno dell'ente o della catena di approvvigionamento, è questione aperta ad ogni soluzione possibile, purché però rimangano ben fermi i requisiti ed i criteri dell'imputazione penale senza ricorso ad inaccettabili presunzioni o automatismi in sede di accertamento della colpevolezza.

Per quanto riguarda, invece, le persone giuridiche, è incontestabile la necessità di sottoporre anche esse a sanzione in caso di violazione dei precetti stabiliti per l'utilizzo di sistemi di IAG. Un sistema sanzionatorio efficace in questo settore sarà verosimilmente incentrato sul rimprovero indirizzato agli enti, e ciò per una ragione molto semplice: la complessità del fenomeno comporterà un progressivo spostamento dell'attenzione circa l'individuazione dei centri di responsabilità verso le organizzazioni complesse, unici soggetti che riassumono l'insieme delle competenze tecnico-specialistiche necessarie a gestire anticipatamente i rischi connessi a tali sistemi nonché adempiere agli eventuali oneri imposti in termini di adozione di misure conformative e di sostenimento dei relativi costi. Che poi, anche qui, la questione del *quomodo* venga risolta a livello interpretativo, attraverso la disciplina dell'art. 8 d.lgs. 231/2001, o che, di contro, sia il legislatore a prevedere una responsabilità diretta e originaria della persona giuridica per fatti dell'agente artificiale individuati in modo svincolato dal reato della persona fisica, è tema di tale respiro da non poter certo essere affrontato in questa sede.

6. Riflessioni conclusive e problemi aperti.

Sebbene i progressi nel campo dell'IA siano fonte di notevoli benefici per l'uomo, la percezione di vivere in una società del rischio è aumentata in maniera esponenziale. L'irruzione dell'IAG ne accentua i profili di iper-modernità, alimentando un'angoscia diffusa nei confronti di sistemi che, se da un lato sono sviluppati sul presupposto di superare le capacità cognitive umane, dall'altro rischiano di fomentare eventi potenzialmente avversi che sfuggono alla comprensione e al controllo umano; e proprio la paura per una tecnologia che, statisticamente parlando, è causa di incidenti poco o comunque meno frequenti di altre tecnologie meno avanzate con le quali, invece, conviviamo tranquillamente, sembrerebbe costituire il vero segno (meglio: paradosso) dei tempi.

Si impone, ancora una volta, una difficile decisione sui rischi in cui la paura dell'ignoto tecnologico gioca un ruolo decisivo, orientando le scelte compiute a livello regolativo verso criteri, anche estremi, di precauzione, a scapito dei protagonisti umani più immediatamente coinvolti nonché, in ultima analisi, dell'innovazione stessa. Come si è visto, infatti, la tentazione di individuare potenziali colpevoli cui addossare i danni indotti dalla macchina – al fine di ripristinare la fiducia verso la tecnologia – rischia di condurre a scelte politiche "ultraresponsabiliste"[84] e derive sul piano penalistico. In questo senso, se la prospettiva di imboccare la scorciatoia del diritto penale di evento – ricorrendo ad esempio alla tradizionale nozione di posizione di garanzia – è accattivante per la sua funzione di rassicurazione (o esorcismo) sociale, essa finisce però per definire un mero centro di accollo di responsabilità in caso di eventi avversi, senza in realtà che ciò presupponga una reale rimproverabilità nei confronti di un umano ormai privo di un reale ed effettivo potere di governo ed intervento sull'attività algoritmica[85].

Di conseguenza, preso atto della scarsissima capacità di tutela dello strumento in questo settore, si è tentato di tracciare brevemente alcune linee guida per un possibile (sia pur limitato) intervento del diritto penale a contrasto dei rischi da ignoto tecnologico che eviti il ricorso a schemi presuntivi e ad irreali oneri di controllo. Ma non pochi e di diversa natura gli interrogativi che le prospettate soluzioni sollevano in punto di legittimità ed efficacia del pur ridimensionato intervento penale rispetto ai rischi da ignoto tecnologico.

Anzitutto, un interrogativo cruciale, affiorato durante la discussione, concerne l'individuazione del limite legittimo dell'anticipazione della tutela penale, ossia la soglia sulla quale può essere correttamente collocato il primo avamposto penalistico. Il tema, come è evidente, si innesta sul piano dei principi, in specie quello di *extrema ratio* e di offensività di beni giuridici

[84] Così Cappellini (2023), cit., 15.
[85] Sulla stessa linea già Consulich (2022), cit., 1050; Piergallini (2020), cit., 1758.

concretamente individuati. Sotto il primo profilo, appare invero opportuno che la sanzione penale non copra l'intera disciplina amministrativa ma sia impiegata in via residuale in funzione della gravità della violazione. Ciò varrebbe, ad esempio, per le ipotesi di reato concernenti le omesse o false comunicazioni all'autorità di settore e l'inosservanza degli obblighi cautelari di autodisciplina.

D'altra parte, è incontestabile che in questi casi è ben difficile parlare di protezione di beni giuridici, perché in realtà la tutela penale tende ad appuntarsi sul procedimento. Pertanto, nella tipizzazione di un sistema sanzionatorio rispettoso dell'offensività sarà – come è ovvio – centrale il ruolo del bene giuridico individuato quale referente del presidio penale. Ciò evoca la necessità di ricercare le coordinate di un bene giuridico "ad ampio spettro" di nuovo conio, intermedio tra la mera difformità tecnica e gli altri interessi potenzialmente vulnerati dall'azione degli agenti artificiali, attorno al quale costruire la legislazione penale di settore[86]. A tal proposito, si può forse ricorrere a quell'affidabilità (o trustworthiness) della macchina, già eretta a nucleo della strategia europea di gestione del rischio da IA[87]. Tale interesse gode di autonoma rilevanza nella misura in cui condiziona i diritti dei singoli, nel senso che la tutela degli interessi individuali e collettivi deve necessariamente derivare dalla garanzia che l'IA sia in grado di comportarsi secondo ciò che è stabilito nelle sue specifiche. In questa chiave fondativa, il principio della *trustworthiness* può a giusto titolo divenire il bene giuridico di riferimento di futuri interventi volti alla costruzione di una rete normativa – anche ma non solo penalistica – in relazione all'IAG e, dunque, la ragione fondante della punizione di coloro che attentino ad essa e (dolosamente o colposamente) ne riducano la portata a danno dei consociati. Ad ogni modo, si potrebbe discutere a lungo se una simile evoluzione sia commendevole allorché, pur rimediando all'ineffettività di tecniche sanzionatorie dipendenti dalla concretizzazione di un evento lesivo (che il più delle volte sfugge alla capacità di previsione dell'agente umano), retroceda al tempo stesso l'evento a mera condizione obiettiva di punibilità, con eccessiva anticipazione della soglia di tutela.

Ancora sul piano dei principi, non può sfuggire certo all'attenzione il fatto che un qualche prezzo si viene a pagare anche rispetto alla legalità sotto il profilo della riserva di legge e della determinatezza. Difatti, è evidente come la disciplina di un fenomeno così carico di effetti dirompenti non potrà che risultare dalla combinazione di una pluralità di fonti eterogenee: norme sovranazionali, etiche, tecniche e strumenti di *self-regulation*[88]. In un simile contesto, è necessario assicurarsi che la determinatezza della norma penale non sia vanificata dalla funzione servente del penale rispetto alla prescrizione amministrativa, allorché quest'ultima non abbia i caratteri di sufficiente determinatezza. Questo rischio di compressione della legalità dovrà essere evitato già nella formulazione del precetto extra-penale, attraverso un incremento di determinatezza e capacità orientativa della prescrizione extra-penale che si vuole sanzionare penalmente, nonché evitando la creazione di norme penali in bianco che, come tali, facciano rinvio, per la determinazione del precetto, *tout court* alla norma extra-penale.

In definitiva, quelle appena elencate sono tutte questioni aperte che meriterebbero un più approfondito esame, al pari dei molti altri interrogativi che popolano un settore di frontiera i cui pericoli sono solo apparentemente lontani e futuristici. Un diritto penale effettivo – pur nei modesti limiti più volte ribaditi – è infatti condizione sia per contribuire a soddisfare realmente il bisogno di tutela dei singoli, sia per dare certezza agli operatori economici che necessitano di un sistema stabile di regole e di responsabilità per pianificare e programmare l'attività di impresa.

Ciò che, però, va chiaramente ribadito è la necessità che, anche in questi casi, rimangano ben fermi i requisiti ed i criteri dell'imputazione penale, evitando il ricorso a inaccettabili stravolgimenti del paradigma colposo. Posto di fronte alla ricerca di un difficile equilibrio tra nuove esigenze di tutela e classici equilibri di sistema, il diritto penale può trovare adeguato spazio e un'azione efficace e non simbolica solo se non arretra rispetto all'esigenza di porre corrette condizioni a base del suo intervento.

[86] È dello stesso avviso Troncone (2023), cit., 3301.
[87] Prima della proposta altri documenti di *soft law* avevano sancito il principio della *trustworthiness*. Per tutti: *Building Trust in Human-Centric Artificial Intelligence*, COM(2019) 168; Gruppo di esperti ad alto livello sull'intelligenza artificiale (2018).
[88] Piergallini (2020), cit., 1770.

Bibliografia

Abbott, Ryan e Sarch, Alex (2019): "Punishing artificial intelligence: legal fiction or science fiction. Is law computable?", in *UC Davis Law Review*, 53, p. 323 ss.

Basile, Fabio (2019): "Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine", in *Diritto Penale e Uomo*, 10.

Bathaee, Yavar (2018): "The Artificial Intelligence Black Box and the Failure of Intent and Causation, in Harvard Journal of Law & Technology", 31, p. 889 ss.

Beck, Susanne (2017): "Google Cars, Software Agents, Autonomous Weapons Systems. New Challenges for Criminal Law", in Hilgendorf, Eric, e Seidel, Uwe (eds.), *Robotics, Autonomics and the Law* (Nomos), pp. 227-251.

Beck, Ulrich (1986), *La società del rischio. Verso una seconda modernità* (Roma).

Caldwell, M., Andrews, J.T.A., Tanay, T., e Griffin, L.D (2020): "AI-enabled future crime", in *Crime Science,* 9 (1), 14.

Cappellini, Alberto (2019): "Profili penalistici delle *self-driving cars*", in *Diritto Penale Contemporaneo*, 2, pp. 325-353.

Cappellini, Alberto (2023): "Reati colposi e tecnologie dell'IA", in Balbi, Giuliano, Esposito, Andreana, Manacorda, Stefano e De Simone, Federica (eds.): *Diritto penale e intelligenza artificiale. Nuovi Scenari* (Torino, Giappichelli), pp. 19-32.

Castronuovo, Donato (2012): *Principio di precauzione e diritto penale: paradigmi dell'incertezza nella struttura del reato* (Roma, Aracne).

Chiang, Ted (2023): "ChatGPT Is a Blurry JPEG of the Web", *New York Times*.

Chomsky, Noam (2023): "The False Promise of ChatGPT", *New York Times*.

Consulich Federico (2018): "Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato", in *Banca borsa titoli di credito*, 2, pp. 195-234.

Consulich, Federico (2018): "Il principio di autonomia della responsabilità dell'ente. Prospettive di riforma dell'art. 8", in *Rivista 231*, 4.

Consulich, Federico (2022): "*Flash Offenders.* Le Prospettive di *Accountability* Penale nel Contrasto alle Intelligenze Artificiali Devianti", in *Rivista Italiana di Diritto e Procedura Penale*, pp. 1015-1055.

Contissa, Giuseppe, Galli, Federico, Godano, Francesco e Sartor, Giovanni (2021): "Il regolamento europeo sull'IA", in *Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, Vol. 14/2, pp. 387-409.

Diamantis, Mihailis (2020): "The Extended Corporate Mind: When Corporations Use AI to Break the Law", in *North Carolina Law Review*, 98, pp. 893 ss.

Diamantis, Mihailis (2021): "Algorithms Acting Badly: A Solution from Corporate Law", in *The George Washington Law Review*, Vol. 89 No. 4.

Europol Innovation Lab (2023), *The criminal use of ChatGPT – a cautionary tale about large language models*, in ww.europol.europa.eu.

Future of Life Institute (2023), *Pause Giant AI Experiments: An Open Letter*, in futureoflife.org.

Garante per la Protezione dei Dati personali (2023): "Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori", in www.garanteprivacy.it.

Giannini, Alice (2022): "Intelligenza artificiale, *human oversight* e responsabilità penale: prove d'impatto a livello europeo", in *Criminalia*.

Gruppo di esperti ad alto livello sull'intelligenza artificiale (2018): *Orientamenti etici per un'IA affidabile*.

Hacker, Phillip, Engel, Andreas e List, Theresa (2023): "Understanding and Regulating ChatGPT, and Other Large Generative AI Models", in *Verfassungsblog on Constitutional Matters*.

Hao, Karen (2018): "What is machine learning?", *MIT Technology Review.*

Kaplan, Jerry (2016): *Artificial Intelligence: what everyone needs to know* (Oxford).

King, Thomas, Aggarwal, Nikita, Taddeo, Mariarosaria, e Floridi, Luciano (2020): "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions", in *Science and Engineering Ethics*, 89, pp. 1-36.

Lagioia, Francesca, e Contissa, Giuseppe (2020): "The strange case of dr. Watson: Liability implications of ai evidence-based decision support systems in health care", in *European Journal of Legal Studies*, vol. 12(2), pp. 245-290.

Lana, Alessio (2021), "Alexa sfida una bimba a inserire una moneta nella presa elettrica: Amazon aggiorna il software", in *Corriere della sera*.

La Vattiata, Federico (2022): "La responsabilità penale per danni da intelligenza artificiale alla prova del processo", in Giordano, Rosaria, Panzarola, Andrea, Police, Aristide, Preziosi, Stefano, e Proto, Massimo (eds.): *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia* (Milano, Giuffrè), pp. 695-712.

Latronico, Vincenzo (2022): "Salvati dagli errori", in *Il Post*.

Legg, Shane e Hutter, Marcus (2007): "A collection of definitions of intelligence", in *Frontiers in Artificial Intelligence and Applications*, Vol. 157, pp. 17-24.

Madani, Ali, Krause, Ben, e Greene, Eric (2023): "Large language models generate functional protein sequences across diverse families", *Nature Biotechnology.*

Magro, Maria Beatrice (2019): "Robot, cyborg e intelligenze artificiali", in Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo, e Papa, Michele (eds.): *Trattato di diritto penale - Cybercrime* (Torino, Utet Giuridica), pp.1179-1212.

Magro, Maria Beatrice (2020): "Decisione umana e decisione robotica. Un'ipotesi di responsabilità da procreazione robotica", in *La legislazione penale*.

Manes, Vittorio (2020): "L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia", in Ruffolo, Ugo (editor): *Intelligenza artificiale - Il diritto, i diritti, l'etica* (Giuffrè, Milano), pp. 547-564.

Marinucci, Giorgio (2005): "Innovazioni tecnologiche e scoperte scientifiche: costi e tempi di adeguamento delle regole di diligenza", in *Rivista italiana di diritto e procedura penale*, 48/1, pp. 29-59.

Mazzacuva, Federico (2021): "The Impact of AI on Corporate Criminal Liability: Algorithmic Misconduct in the Prism of Derivative and Holistic Theories", in Vermuelen, Gert, Peršak, Nina e Recchia, Nicola (eds.): *Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice* (Antwerpen), pp. 143 ss.

McCarthy, John (2007): "What is Artificial Intelligence?", www.formal.stanford.edu.

Minelli, Camilla (2022): "La responsabilità "penale" tra persona fisica e corporation alla luce della Proposta di Regolamento sull'Intelligenza Artificiale", in *Diritto penale contemporaneo – Rivista trimestrale*, 2.

Mobilio, Giuseppe (2020): "L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica", in *Rivista di BioDiritto*, 2, pp. 401-424.

Muller, Vincent e Bostrom, Nick (2016): "Future progress in AI: a survey of expert opinion", in Muller, Vincent (editor), *Fundamental issues of AI* (Oxford, Springer), pp. 553-571.

Pagallo, Ugo (2013): *The Laws of Robots: Crimes, Contracts and Torts* (Springer).

Pagallo, Ugo e Quattrocolo, Serena (2018): "The impact of AI on criminal law, and its twofold procedures", in Barfield, Woodrow e Pagallo, Ugo (eds.), *Research Handbook on the Law of Artificial Intelligence* (Cheltenham-Northampton), pp. 385-410.

Paliero, Carlo Enrico (2008): "La Società punita: del come, del perché e del per cosa", in *Rivista italiana di diritto e procedura penale*, pp. 1516-1545.

Panattoni, Beatrice (2021): "Intelligenza artificiale: le sfide per il diritto penale nel passaggio dall'automazione tecnologica all'automa artificiale", in *Diritto dell'Informazione e dell'Informatica*, 2, pp. 317-368.

Perini, Chiara (2010): *Il concetto di rischio nel diritto penale moderno* (Giuffré, Milano).

Perini, Chiara (2017): "Adattamento e Differenziazione della Risposta Punitiva nella Società Del Rischio", in Morgante, Gaetana (editor), *Il diritto penale di fronte alle sfide della «Società del rischio». Un difficile rapporto tra nuove esigenze di tutela e classici equilibri di sistema* (Giappichelli, Torino), pp. 455-472.

Perrigo, Billy (2023): "OpenAI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic", in *Time*.

Picotti, Lorenzo (2021): "Profili di responsabilità penale per la circolazione di veicoli a guida autonoma", in Catenacci, Mauro, Rampioni, Roberto e Nico D'Ascola, Vincenzo(eds.): *Studi in onore di Antonio Fiorella* (RomaTre), I, pp. 813-837.

Piergallini, Carlo (2011): "Attività produttive, decisioni in stato di incertezza e diritto penale", in Donini, Massimo e Pavarini, Massimo (eds.): *Sicurezza e Diritto Penale* (Bologna), pp. 358 ss.

Piergallini, Carlo (2020): "Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?", in *Rivista italiana di diritto e procedura penale*, 4, pp. 1743-1772.

Piva, Daniele (2022): "Machina discere, (deinde) delinquere et puniri potest", in Giordano, Rosaria, Panzarola, Andrea, Police, Aristide, Preziosi, Stefano, e Proto, Massimo (eds.): *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia* (Milano, Giuffrè), pp. 681-693.

Pulitanò, Domenico (2002): *Responsabilità amministrativa per i reati delle persone giuridiche* (voce), in *Enc. Dir. Agg.*, VI (Milano).

OpenAI (2019), *Language Models are Unsupervised Multitask Learners*, in openai.com.

Romanò, Leonardo (2022): "Intelligenza artificiale come prova scientifica nel processo penale: una sfida tra *machine-generated evidence* e equo processo", in Canzio, Giovanni, e Luparia, Luca (eds.), *Prova scientifica e processo penale* (CEDAM), 24.

Rosenblatt, Kalhan (2023): "ChatGPT passes MBA exam given by a Wharton professor", *NBC News*.

Ruffolo, Ugo (2021): "*Machina delinquere potest?* Responsabilità ed "illeciti" (anche penali?) della "persona elettronica" e tutele per gli agenti software autonomi", in Ruffolo, Ugo (editor), *XXVI Lezioni di Diritto dell'Intelligenza Artificiale* (Torino, Giappichelli), pp. 295-310.

Ruga Riva, Carlo (2006): "Principio di precauzione e diritto penale. Genesi e contenuto della colpa in contesti di incertezza scientifica", in Dolcini, Emilio e Paliero, Carlo Enrico (eds.), *Scritti in onore di Marinucci*, vol. II, pp. 1743 ss.

Salvadori, Ivan (2021): "Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale", in *Rivista italiana di diritto e procedura penale*, 1, pp. 83-118.

Sample, Ian (2023): "Science journals ban listing of ChatGPT as co-author on papers", *The Guardian*.

Sartor, Giovanni (1996): *Intelligenza artificiale e diritto: un'introduzione* (Milano, Giuffrè).

Sgubbi, Filippo, Fondaroli, Desirèe e Tripodi, Andrea (2013): *Diritto penale del mercato finanziario. Abuso di informazioni privilegiate, manipolazione del mercato, ostacolo alle funzioni di vigilanza della Consob, falso in prospetto* (Cedam).

Stella, Federico (2003): *Giustizia e Modernità. La Protezione dell'innocente e la Tutela delle Vittime* (Milano, Giuffrè).

Stortoni, Luigi (2004): "Angoscia tecnologica ed esorcismo penale", in *Rivista italiana di diritto e procedura penale*, 1, pp. 71-89.

Surden, Harry e Williams, Mary-Anne (2016): "Technological Opacity, Predictability, and Self-Driving Cars," in *Cardozo Law Review*, 38, pp. 121-181.

Tripodi, Andrea Francesco (2022), "Uomo, *societas*, *machina*", in Piergallini, Carlo, Mannozzi, Grazia, Sotis, Carlo, Perini, Chiara, Scoletta, Marco e Consulich Federico (eds.), *Studi in Onore di Carlo Enrico Paliero* (Milano, Giuffré), pp. 1187-1203.

Troncone, Pasquale (2022): "Il sistema dell'intelligenza artificiale nella trama grammaticale del diritto penale. Dalla responsabilità umana alla responsabilità delle macchine pensanti: un inatteso *return trip effect*", in *Cassazione Penale*, 9, pp. 3287-3304.

Ubertis, Giulio (2020): "Intelligenza artificiale, giustizia penale, controllo umano significativo", in *Sistema Penale*, 4, p. 75-88.

Viganò, Francesco (2013): "Il rapporto di causalità nella giurisprudenza penale", in *Diritto Penale Contemporaneo*.

Speciale su "sicurezza dello stato e poteri investigativi paralleli"

Especial sobre "seguridad del estado y facultades investigativas paralelas"

Special on "State Security and Parallel Investigative Powers"

Speciale su "Sicurezza dello Stato e poteri investigativi paralleli". Premessa

Especial sobre "Seguridad del Estado y facultades investigativas paralelas". Premisa

Special on "State security and parallel investigative powers". Introduction

Donatella Curtotti
Professore ordinario di Diritto processuale penale – Coordinatrice del Corso di laurea in Scienze investigative – Università di Foggia
donatella.curtotti@unifg.it

Indagini preliminari, Terrorismo, Reati informatici

Investigaciones preliminares, Terrorismo, Delitos informáticos

Pre-Trial Investigation, Terrorism, Cybercrimes

Abstracts

La dimensione transnazionale e cibernetica delle nuove minacce alla sicurezza dei cittadini e dello Stato stanno determinando una trasformazione degli equilibri tra il sistema repressivo e il sistema preventivo, generando inediti scambi di informazioni e interazioni investigative tra settori un tempo impermeabili. Questo fenomeno è agevolato da alcuni fattori: le legislazioni sovranazionali, la criminalizzazione delle condotte preparatorie, la centralità dei servizi di intelligence, la creazione di organismi comuni di indagine e la recente istituzione della Agenzia per la cybersicurezza. L'obiettivo di questo Speciale è indagare, sulla base della normativa vigente le dinamiche di questi poteri investigativi paralleli, evidenziandone le potenzialità, le criticità e le ripercussioni sui diritti di libertà e, in particolare, sulla tenuta di principi e regole del processo penale, nel quale confluiscono gli esiti di tali attività investigative.

Las dimensiones transnacional y cibernética de las nuevas amenazas a la seguridad de los ciudadanos y del Estado están determinando una transformación del equilibrio entre el sistema represivo y el sistema preventivo, generando intercambios de información e interacciones investigativas sin precedentes entre sectores otrora impermeables. Este fenómeno se ve facilitado por una serie de factores: la legislación supranacional, la tipificación como delito autónomo de conductas preparatorias, la centralidad de los servicios de inteligencia, la creación de organismos conjuntos de investigación y la reciente creación de la Agencia de Ciberseguridad. El objetivo de este Especial es indagar, con base en la legislación vigente, la dinámica de estas facultades investigativas paralelas, destacando sus potencialidades, puntos críticos y repercusiones sobre los derechos de libertad y, en particular, sobre la observancia de principios y normas de la juicio penal, en el que confluyen los resultados de estas actividades investigativas.

The transnational and cybernetic dimension of the new threats to the security of citizens and the State are determining a transformation of the balance between the repressive system and the preventive system, generating unprecedented exchanges of information and investigative interactions between once impermeable sectors. This phenomenon is facilitated by a number of factors: supranational legislation, the criminalization of preparatory conduct, the centrality of intelligence servicesand the recent establishment legislation, the dynamics of these parallel investigative powers, highlighting their potential, criticalities and repercussions on the rights of freedom and, in particular, on the keeping of principles and rules of the criminal trial, in which the results of these investigative activities converge.

In Italia, il tema delle investigazioni preventive e di sicurezza sembra non incidere in maniera significativa sulle logiche del rito penale e del procedimento probatorio[1]. Nella stessa misura, le criticità che investono il tema sembrano interessare lo studioso italiano solo marginalmente, come effetto del richiamo di istituti ben più noti e centrali, e con uno sguardo "di confine" rispetto ad una fase collocata assai prima dell'inizio del procedimento penale, a cui il legislatore ha scelto di negare ogni accesso in termini di utilizzabilità.

Se questa prospettiva poteva essere valida nel 1988 ed anche nei due decenni a seguire, oggi si ritiene che possa risultare "miope" perché, da un lato, non vede come le indagini proattive[2] abbiano assunto un ruolo centrale nell'attività investigativa delle procure e, dall'altro, si scontra con il potenziamento di una fase, quella preventiva e di sicurezza, che rappresenta la protagonista indiscussa del futuro "anche" della giustizia penale.

Va da sé che le implicazioni processuali, un tempo "di confine", perdono la loro originaria dimensione e le problematicità rispetto a norme, principi, garanzie individuali e di accertamento, si irrobustiscono e complicano.

Prima di affrontare le difficoltà di ordine strettamente procedurale, pare doverosa una riflessione di più ampio respiro, inerente al peculiare momento storico-politico che il Paese sta attraversando e dal quale dipende l'interesse sempre più crescente verso l'inedito mondo della prevenzione.

É ben noto agli addetti ai lavori che il terrorismo internazionale e le minacce cybernetiche stanno determinando una trasformazione degli equilibri tra sistema repressivo e preventivo-securitario, spinti dall'esigenza di far crescente l'interazione investigativa così come gli inediti scambi di informazione tra i due "comparti".

In questo contesto, il sistema penale sembra che stia rispondendo attraverso un mutamento dei suoi tradizionali connotati ideologici e strutturali (quelli che, da sempre, lo hanno caratterizzato), arrivando a superare l'idea, di matrice retributiva, per cui il suo unico fine è la repressione della fattispecie criminogena attraverso l'accertamento del fatto e la punizione del colpevole. Così, se per secoli la giustizia penale ha esercitato una funzione terapeutica – sviluppando tutte le sue potenzialità nel ricostruire il reato e nell'applicare le pene, con più o meno tradizionali mezzi di accertamento e coazione –, la tendenza più recente è attribuire alla giustizia penale anche una funzione preventiva, di anticipazione del crimine, organizzando la risposta statale secondo modalità, forme e tempi nuovi che allontanano il sistema penale dalla sua immagine tradizionale.

Non esiste più, in sostanza, solo il diritto penale della colpevolezza, ma anche (e soprattutto) quello della sicurezza (o prevenzione) e della neutralizzazione del pericolo, nella convinzione che sia preferibile "evitare le malattie piuttosto che curarle e guarirle"[3].

Se questo è un dato di fatto, non si è altrettanto sicuri di essere al cospetto di una "perdita" o di un "depauperamento" del diritto; forse sarebbe meglio parlare di trasformazione[4]. Si apre uno scenario inedito e si paventa una sfida nuova per il processual-penalista.

C'è chi parla di "trasmutazione poliziesca del procedimento penale"[5], chi, invece, di un'inevitabile trasformazione del sistema che non cancella del tutto i suoi tratti costitutivi quanto a principi generali, ma rompe la sua immagine unitaria, pressata dall'emersione di diversi sottosistemi normativi sorretti da logiche speciali[6].

A prescindere dal diverso modo di concepire il fenomeno, non c'è dubbio che si stia delineando un nuovo sistema di lotta alla criminalità che arretra i suoi argini ad una fase *pre*-procedimentale, scongiurando *ab origine* il rischio di compimento del reato: pericoli, immaginari o presunti, finiscono per giustificare un intervento "correttivo" preventivo, al fine di scongiurare danni devastanti.

Il motore trainante dell'arretramento del sistema penale verso forme di anticipazione del

[1] Per una diversa e più matura impostazione sistemica dei rapporti tra Intelligence e organi di polizia, v. Lowenthal (2022), nonché Andrew et all (2019).
[2] Così definite nella *Risoluzione del XVIII Congresso internazionale di diritto penale,* Istanbul, 20–27 settembre 2009.
[3] Bobbio (2015), p. 23.
[4] Cfr., Militello (2017), p. 5, per cui «[P]più che un abbandono del volto tradizionale del sistema penale, il quale non cancella del tutto i suoi tratti costituivi quanto a principi generali, impianto codicistico e tavola dei beni tutelati, si delinea quantomeno una sua trasformazione, nel senso di una rottura della sua immagine unitaria, pressata dall'emersione di diversi sottosistemi normativi sorretti da logiche speciali e diverse rispetto al ceppo principale».
[5] Così Negri (2016), p. 3.
[6] In questo senso, Di Bitonto (2012), p. 1181.

danno e neutralizzazione dell'offesa, risiede nelle scelte di politica criminale internazionale che, nell'ottica di *"prevent and suppress terrost acts"*, risultano sempre più incentrate sull'ampliamento della sfera operativa degli strumenti di prevenzione sia in termini quantitativi che qualitativi.

Senza voler ripercorrere nel dettaglio tutte le tappe dell'evoluzione della legislazione internazionale *ante delictum,* l'emblema del cambiamento può essere rinvenuto nella Risoluzione del Consiglio di Sicurezza ONU n. 2178 del 24 settembre 2014, con cui viene – per la prima volta – disposta l'incriminazione di una serie di condotte preparatorie alla commissione di attentati terroristici.

Parallelamente, la neutralizzazione delle minacce terroristiche rappresenta una priorità assoluta per l'Unione europea. Si pensi alla *Dichiarazione dei membri del Consiglio europeo* del 12 febbraio 2015, nella quale si esprime la necessità di garantire la sicurezza dei cittadini attraverso "la condivisione delle informazioni e la cooperazione operativa, anche tramite *Europol* e *Eurojust*". Analogamente, nella *Dichiarazione comune dei ministri degli Affari interni dell'UE sui recenti attentati terroristici in Europa* del 13 novembre 2020, oltre all'esigenza di favorire la circolazione delle informazioni tra Servizi d'*intelligence* e Forze di polizia, emerge la necessità che "i servizi di sicurezza degli Stati membri approfondiscano la loro cooperazione". Ancora, si pensi alle *Conclusioni del Consiglio europeo* del 10-11 dicembre 2020 sulle scelte strategiche per la prevenzione dei fenomeni di radicalizzazione e del cyberterrorismo, in cui l'Unione esprime l'esigenza di "intensificare lo scambio informativo quale tecnica di neutralizzazione del terrorismo internazionale". Non è un caso che il 14 dicembre 2022 la presidenza del Consiglio e il Parlamento europeo abbiano raggiunto un accordo provvisorio per migliorare lo scambio di informazioni nei casi di terrorismo con lo scopo di modernizzare e digitalizzare la cooperazione giudiziaria transfrontaliera.

Questa nuova cultura investigativa, imperniata sulla circolazione di informazioni, si riflette inevitabilmente nell'ordinamento interno.

Il legislatore nazionale si muove in questa direzione preventiva offrendo soluzioni che indicizzano bisogni di una tutela diversa della sicurezza con un'anticipazione dell'intervento *ante delictum.* Solo a titolo esemplificativo, la riforma del sistema penale operata nel biennio 2015-2016 (d.l. 7/2015 e l. 153/2016) si prefigge l'obiettivo di anticipare la soglia della punibilità alle condotte riparatorie rispetto al compimento di gravi delitti, e, al contempo, di allargare le maglie dei poteri di controllo sociale da parte degli organi inquirenti.

Non solo. L'esigenza di prevenire il compimento del fatto di reato è il *fil rouge* che spinge il legislatore alla complessa modifica del Codice antimafia (l. 17 ottobre 2017, n. 161), al fine di potenziare il ricorso al duttile strumento delle misure di prevenzione personali e patrimoniali, ampliandone a dismisura l'area operativa. Si pensi, da ultimo, agli strumenti di prevenzione collaborativa introdotti dal d.l. 6 novembre 2021, n. 152, con lo scopo di ampliare lo spettro operativo delle misure antimafia che, come ricordato, hanno registrato un aumento costante negli ultimi anni[7].

La tendenza ad arretrare la risposta penale alla fase prodromica al compimento del reato determina un'inevitabile conseguenza: l'asse investigativo tende a spostarsi progressivamente sul versante preventivo-securitario, sulla scia di quanto sta accadendo negli altri Paesi europei. Strumenti di tradizione processualista frammisti a mezzi di indagine inediti assurgono a protagonisti delle nuove investigazioni proattive, condotte al fine di neutralizzare il compimento del fatto di reato allorquando sussista un fondato sospetto di incombente realizzazione dell'illecito.

Curiosamente, alla trasformazione in senso preventivo del sistema penale non corrisponde la creazione di strumenti investigativi (di tipo giuridico) *ad hoc* da impiegare in fase preventiva.

Come noto, il codice di rito contempla solo una forma di investigazione preventiva, più prossima al procedimento penale, rappresentata dalle "*Intercettazioni e controlli preventivi sulle comunicazioni*", allocabili al confine tra la fase preventiva e quella repressiva, in una "zona grigia" di passaggio dall'una all'altra sfera operativa. Nonostante la recente riforma che ha caratterizzato l'istituto delle captazioni e dei controlli preventivi d'*intelligence*[8], si sente come persa l'occasione per procedere alla tipizzazione delle altre *species* di indagini preventive che, pur non trovando espressa regolamentazione, risultano assai utili nella prevenzione del crimine.

[7] D'Angelo e Varraso (2022), p. 1.
[8] L.29 dicembre 2022, n. 197, recante "*Bilancio di previsione dello Stato per l'anno finanziario 2023 e bilancio pluriennale per il triennio 2023-2025*", in *Gazz. uff.,* 29 dicembre 2022, n. 303.

Se non si registra particolare attenzione al tema delle tecniche di indagine proattiva così come ai ruoli e alle attività dei Servizi nazionali d'Intelligence (di cui, invece, alcuni Paesi europei e lo stesso Consiglio d'Europa hanno colto il peso in termini di connessioni e coordinamenti investigativi con l'a.g.), il legislatore mostra maggiore sensibilità con riferimento alla previsione di nuovi organismi comuni di indagine con compiti di coordinamento tra la fase preventiva e quella giudiziaria. Infatti, è stata recentemente istituita l'Agenzia per la cybersicurezza con compiti di resilienza e sicurezza in ambito informatico. Altrettanto recente è la scelta di potenziare le funzioni attribuite all'Agenzia nazionale per la sicurezza del volo (ANSV), autorità investigativa che mira a garantire la sicurezza dell'aviazione civile dello Stato italiano.

Sicuramente, la previsione di organismi autonomi, chiamati a svolgere inchieste preventive per la tutela della sicurezza nazionale e dei cittadini, è un dato di grande rilevanza perché contribuisce a fornire una "regolamentazione" alle attività compiute per scopi di prevenzione, ma, inevitabilmente, acuisce il rischio dei c.d. poteri investigativi paralleli, in cui gli attori perdono la propria identità sull'altare dell'efficacia della risposta statale.

In questo quadro magmatico, caratterizzato dalla compresenza di molteplici soggetti con compiti di investigazione, gli equilibri di potere tra i protagonisti delle tradizionali indagini preliminari risultano alterati, ingenerando una confusione di ruoli assai "pericolosa"; una compenetrazione di funzioni che altera gli equilibri classici del procedimento penale.

A questo punto, due considerazioni.

Per un verso, si è al cospetto di un "nuovo" genere di prevenzione; una prevenzione 2.0 che, in spregio ai *dicta* normativi che impongono una netta separazione tra *pre* e *post* procedimento, spinge per una circolazione probatoria di dati e per un'implementazione delle indagini proattive che, inevitabilmente, si ripercuotono sugli esiti procedimentali, sia investigativi che dibattimentali.

Si intende dire che oggi, in conseguenza del terrorismo internazionale e delle recenti minacce cibernetiche, il confine tra prevenzione e repressione è molto più labile. Ci si muove ai suoi bordi incorrendo in invasioni, osmosi, interferenze, intersezioni; trasformazioni che la comunità internazionale sollecita ritenendole imprescindibili per un efficace contrasto al crimine e che gli Stati in parte stanno già attuando attraverso inedite forme di circolazione di informazioni e nuove architetture strutturali[9]. Queste trasformazioni alterano ancora l'attuale assetto tra i due piani di azione, rispondenti, da sempre, a logiche diverse[10]. Rigide, trasparenti, controllabili, quelle giudiziarie. Inevitabilmente più agili, duttili, con regole e contorni molto meno nitidi, quelle preventive[11].

Per un altro verso, queste inedite investigazioni richiedono allo studioso del processo penale di prendere atto della trasformazione del rapporto rito penale/investigazioni preventive, di verificare se tale evoluzione congedi definitivamente l'idea del processo penale e dei suoi protagonisti come strumento di attuazione di diritti fondamentali, e, infine, della possibilità di modificare l'attuale assetto normativo aprendosi ad una circolazione probatoria inedita che tocchi non solo il procedimento penale ma anche l'attività preventiva.

Questa sfida, è bene dirlo sin da subito, non è quella di valutare l'opportunità ideologica di tale cambiamento. Purtroppo, in Italia, le scelte ideologiche (di politica criminale) non anticipano mai le modifiche "di fatto", piuttosto le seguono e finiscono per dipendere dai risultati (danni o successi) cui queste portano. Oggi, le modifiche ci sono, le trasformazioni si stanno attuando, sotto la pressione del legislatore sovranazionale, delle nuove *chances* investigative offerte dal progresso tecnico-scientifico, delle emergenze terroristiche e cibernetiche che impegnano il sistema in una risposta inedita, delle modifiche strutturali e funzionali di organi e istituzioni. Al cospetto di queste trasformazioni, analogamente a quanto già accaduto in un recente passato sul fronte della prova tecnico-scientifica, lo studioso del processo penale è chiamato ad interpellarsi sulla flessibilità del sistema repressivo, sulla sua tenuta in termini di compatibilità con i valori fondamentali cui il rito si ispira, sulla "copertura" normativa verso forme nuove di collaborazione con organi e funzioni estranei alla giustizia penale. Più in generale, prova a testare la legittimità della trasformazione funzionale cui assiste e, eventualmente, la necessità di un intervento legislativo correttivo.

In questo Speciale dedicato alla "*Sicurezza dello Stato e ai poteri investigativi paralleli*", si è inteso fare alcune riflessioni sul tema, con l'obiettivo di indagare, sulla base della normativa

[9] Volendo, Curtotti (2018), pp. 435-449.
[10] Così, Kostoris (2016), p. XVI.
[11] Illuminati (2010), p. VII.

vigente, i rapporti tra indagini preventive e procedimento penale, evidenziandone le potenzialità, le criticità e le ripercussioni sui diritti di libertà e, in particolare, sulla tenuta di principi e regole del processo, nel quale confluiscono gli esiti di tali attività investigative.

Le riflessioni non possono che partire da un inquadramento di tipo "politico" del fenomeno, all'interno delle dinamiche legislative europee, mettendo in risalto le criticità emerse negli ultimi anni, anche in termini di mancata armonizzazione e difficoltà di cooperazione internazionale (Angela Procaccino).

Si procede, poi, ad analizzare l'istituto delle intercettazioni preventive di polizia (art. 226 disp. att. c.p.p.) e d'*intelligence* (art. 5, d.l. 144/2005), che rappresenta l'emblema del rischio della sussistenza di poteri investigativi paralleli (Wanda Nocerino). Come meglio si dirà, l'art. 226 disp. att. c.p.p. regola una fase investigativa di tipo preventivo in cui la presenza dei Servizi di *intelligence* interagisce attivamente con gli organi e con le finalità del procedimento penale: seppur il legislatore impedisce l'uso delle informazioni acquisite in fase preventiva in seno al processo penale sotto forma di prova, allo stato dell'arte, i risultati delle intercettazioni preventive trovano un impiego "indiretto" nel processo, agevolando una circolazione atipica di informazioni che si ripercuote sugli esiti investigativi e (finanche) dibattimentali. In questo contesto, occorre soffermarsi sul dettato normativo che, soprattutto a seguito della recente riforma operata con l. 197/2022, lascia scoperta un'ampia gamma di attività che fluttuano tra i due comparti, in una zona grigia dai contorni normativi assenti o, comunque, poco chiari.

Si procede, infine, ad analizzare le competenze e le attribuzioni di alcuni organismi indipendenti che operano in fase preventiva, ossia l'Agenzia per la cybersicurezza (Federico Niccolò Ricotta) e l'Agenzia nazionale per la sicurezza per il volo (Ottavia Murro). Lo scopo è quello di comprendere i delicati rapporti che tali organismi intrattengono con Procura della Repubblica e di individuare le criticità che caratterizzano l'attività da essi svolta soprattutto in ragione dell'inevitabile osmosi probatoria dei risultati investigativi ottenuti in fase preventiva nell'ambito del processo penale.

Bibliografia

Andrew, C., et all (2019): *Secret Intelligence* (London, Routledge).

Bobbio, Norberto (2015): *Dalla struttura alla funzione. Nuovi studi di teoria del diritto* (Roma, Laterza).

Curtotti, Donatella (2018): "Procedimento penale e *intelligence* in Italia: un'osmosi inevitabile, ancora orfana di regole", *Processo penale e giustizia,* 3, pp. 435-449.

D'Angelo, Giovanni e Varraso, Gianluca (2022): "Decreto legge n. 152/2021 e le modifiche in tema di documentazione antimafia e prevenzione collaborativa", *Sistema penale online.*

Di Bitonto, Maria Lucia A. (2012): "Terrorismo internazionale, procedura penale e diritti fondamentali in Italia", *Cassazione penale,* pp. 1181-1207.

Kostoris, Roberto E. e Viganò, Francesco (2016): "Il "nuovo" pacchetto antiterrorismo, tra prevenzione, contrasto in rete e centralizzazione delle indagini", in Kostoris, Roberto E. e Viganò, Francesco (editor), *Il nuovo pacchetto antiterrorismo* (Torino, Giappichelli), p. XV.

Illuminati, Giulio (2010): "Presentazione", in Illuminati, Giulio (editor), *Nuovi profili del segreto di Stato e dell'attività di* Intelligence (Torino, Giappichelli), p. V-VIII.

Lowenthal, Mark M. (2022): *Intelligence: from secrets to policy* (Singapore, Sage).

Militello, Vincenzo (2017): "Terrorismo e sistema penale: realtà, prospettive, limiti", *Diritto penale contemporaneo – Rivista trimestrale*, 1, pp. 3-10.

Negri, Daniele (2016): "La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)", *Archivio penale*, 1, pp. 44-54.

Agenzia per la *cybersicurezza* nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria

Agencia Nacional de Ciberseguridad, Seguridad de la República italiana e investigación judicial

National Cybersecurity Agency, Security of Italian Republic and Judicial Investigation

Federico Niccolò Ricotta
Assegnista di ricerca nell'Università degli Studi di Foggia
federico.ricotta@unifg.it

Reati informatici, Indagini preliminari
Delitos informáticos, Investigaciones preliminares
Cybercrimes, Pre-Trial Investigation

Abstracts

Il contributo analizza il ruolo e le funzioni della nuova Agenzia per la cybersicurezza, con particolare riferimento al rango della sicurezza cibernetica, all'applicabilità della disciplina prevista per il sistema di informazione per la sicurezza della Repubblica, alle indagini di sicurezza e alle possibili sovrapposizioni con i poteri dell'Autorità Giudiziaria.

El artículo analiza el papel y las funciones de la nueva Agencia de Ciberseguridad, con especial referencia al rango de la ciberseguridad, la aplicabilidad de la normativa prevista para el sistema de información de seguridad de la República, las investigaciones de seguridad, y los posibles solapamientos con las competencias de la Autoridad Judicial.

The paper analyzes role and functions of the new Cybersecurity Agency, with particular reference to the rank of cybersecurity, the applicability of the regulations provided for the Republic's security information system, security investigations, and possible overlaps with the powers of the Judicial Authority.

Sommario

1. Introduzione.

L'incremento delle minacce nel dominio cibernetico e la complicazione del quadro-geopolitico globale hanno accresciuto l'esposizione della Repubblica Italiana al pericolo di attacchi di natura informatica alle infrastrutture critiche, ai servizi e alle funzioni essenziali. Le principali capacità nazionali di risposta, analisi, vigilanza e prevenzione nel dominio cibernetico[1], transitoriamente affidate alle competenze del Sistema di informazione per la Sicurezza della Repubblica, sono oggi trasferite all'Agenzia per la cybersicurezza nazionale (ACN)[2], alla quale la legge attribuisce un complesso di poteri certificativi, investigativi e sanzionatori necessari al perseguimento della propria missione istituzionale.

L'assetto istituzionale e normativo in materia di cybersicurezza solleva almeno tre ordini di quesiti. Il primo riguarda la natura dell'Agenzia cyber: c'è da chiedersi se l'Agenzia sia un'agenzia di *intelligence*; e, in caso di risposta positiva, quali siano le regole da applicare, tenendo conto sia delle garanzie previste dalla legge 3 agosto 2007 n. 124 (la legge sul sistema di informazione per la sicurezza della Repubblica e sulla nuova disciplina del segreto di Stato), sia di quelle stabilite dal codice di procedura penale. Inoltre, sul presupposto che ogni attacco informatico è potenzialmente un crimine, occorre ulteriormente domandarsi se i poteri investigativi attribuiti all'Agenzia possano innescare sovrapposizioni con quelli dell'autorità giudiziaria.

2. Le istituzioni a salvaguardia della sicurezza cibernetica.

L'attuale disciplina in materia di sicurezza cibernetica è contenuta essenzialmente in tre principali testi normativi che definiscono il sistema a livello europeo e nazionale[3]: la direttiva (UE)2016/1148 del 6 luglio 2016, la cd. NIS – "*Network and information security*", per l'adozione di misure al fine raggiungere elevati standard nella sicurezza delle reti e dei sistemi informativi all'interno dell'Unione e recepita in Italia dal d.lgs. 18 maggio 2018, n. 65[4]; il decreto-legge 21 settembre 2019 n. 105, così come convertito dalla legge 18 novembre 2019, n. 133, ed i successivi decreti attuativi[5], che hanno introdotto il perimetro nazionale di sicurezza cibernetica; il decreto-legge 14 giugno 2021 n. 82, convertito con modificazioni con la legge 4 agosto 2021 n. 109[6], che ha definito l'attuale architettura nazionale di cybersicurezza,

[1] Lo "spazio cibernetico" è definito come «*l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi. Esso dunque comprende internet, le reti di comunicazione, i sistemi su cui poggiano i processi informatici di elaborazione dati e le apparecchiature mobili dotate di connessione di rete*» cit. Presidenza del Consiglio dei Ministri (2013), p. 10.

[2] Ai sensi dell'art. 1 del decreto-legge 14 giugno 2021 n. 82, convertito con modificazioni dalla l. 4 agosto 2021, n. 109, per cybersicurezza deve intendersi l'insieme delle attività necessarie alla protezione dalle minacce informatiche di reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

[3] Completano il quadro delle disposizioni UE rilevanti il Regolamento UE 2019/881, il cd. "*Cybersecurity Act*", che ha portato all'istituzione dell'Autorità Nazionale di Certificazione della Cybersicurezza la Direttiva n. 2018/1972, il cd. Codice Europeo delle Comunicazioni Elettroniche, recepito nell'ordinamento italiano dal d. lgs. 8 novembre 2021, n. 207, che ha modificato le disposizioni introdotte nel d.lgs. 259/2003. Per un approfondimento v. Carotti (2020), p. 629 ss.; Renzi (2021), p. 538 ss.

[4] La NIS è stata sostituita dalla cd. NIS 2, la Direttiva (UE) 2022/2555 che ha ulteriormente innalzato i presidi necessari all'identificazione, la valutazione e la mitigazione del rischio cibernetico.

[5] Così come interpolato dal d.l. n. 162/2019 in materia di proroga dei termini e altre disposizioni sulla pubblica amministrazione. In attuazione del d.l. n. 105/2019 sono stati adottati il DPCM 30 luglio 2020, n. 131, concernente criteri e modalità per l'individuazione dei soggetti inclusi nel perimetro nazionale di sicurezza cibernetica, e il DPCM 14 aprile 2021, n. 81 sulle modalità per la notifica nel caso di incidenti riguardanti beni ITC. Si veda in particolare il dossier del servizio studi del Senato della Repubblica, *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*, 11 novembre 2019, disponibile su documenti.camera.it.

[6] Il d.l. n. 105/2019, in particolare, individua le amministrazioni pubbliche, enti ed operatori pubblici e privati che hanno sede nel territorio

provvedendo al riordino e all'accentramento delle competenze in seno all'Agenzia per la cybersicurezza nazionale.

Più specificamente gli articoli 1, 2, 3 e 4 del d.l. n. 82/2021 definiscono la struttura del sistema nazionale di sicurezza cibernetica, vale a dire il complesso di organi e strutture, tra di loro autonomi, che si coordinano e interagiscono fra loro per assolvere all'insieme delle determinazioni necessarie alla difesa e alla resilienza digitale dello Stato nel dominio cibernetico.

Al vertice del sistema è posto il Presidente del Consiglio dei ministri, a cui la legge attribuisce l'alta direzione e la responsabilità generale delle politiche di cybersicurezza[7], con la facoltà di delegare le funzioni che non gli sono conferite in via esclusiva all'Autorità Delegata per il Sistema di informazione per la sicurezza della Repubblica. Presso la Presidenza del Consiglio è stato istituito il Comitato interministeriale per la cybersicurezza (CIC), l'organismo cui sono attribuite funzioni di vigilanza, consulenza e proposta nell'ambito delle politiche in ambito cybernetico[8]6; infine, il sistema si completa con l'Agenzia per la cybersicurezza nazionale e, in seno ad essa, il Nucleo per la cybersicurezza e gestione della crisi[9] ed il *Computer Security Incident Response Team* Italia, il CSIRT.

3. Sicurezza nazionale, architettura nazionale per la cybersicurezza e Sistema di informazione per la sicurezza della Repubblica.

L'adozione del d.l. 14 giugno 2021 n. 82, così come convertito in legge, ha rinnovato l'attuale architettura nazionale di sicurezza cibernetica su quattro grandi pilastri di competenze tra loro diversificate ma comunicanti[10]: la cybersicurezza e la resilienza nello spazio cibernetico, affidata all'Agenzia per la cybersicurezza nazionale; la raccolta e l'analisi informativa, affidata al Sistema di informazione per la sicurezza della Repubblica; la difesa e la sicurezza militare dello Stato, affidata al Ministero della Difesa; la prevenzione e il contrasto dei reati, di competenza delle forze di polizia e dell'autorità giudiziaria.

Prima della definizione del perimetro di sicurezza nazionale e dell'istituzione dell'Agenzia *cyber*[11], la tutela della Repubblica dall'imperversare delle minacce nel dominio cibernetico era affidata all'attività istituzionale svolta dal Dipartimento delle Informazioni per la sicurezza, il DIS, l'organo di coordinamento del Sistema di informazione per la sicurezza della Repubblica, che disponeva di risorse e capacità adeguate all'incarico[12]: un ruolo di supplenza che il DIS ha transitoriamente mantenuto sino all'entrata in vigore della nuova architettura nazionale di cybersicurezza[13].

nazionale che rientrano nel perimetro di sicurezza, e che per questo sono tenuti al rispetto di obblighi e delle misure in funzione di tutela della sicurezza nazionale (v. in tal senso art. 1 comma 2 del menzionato decreto-legge).

[7] Le attribuzioni in materia cyber si aggiungono all'alta direzione e alla responsabilità generale della politica dell'informazione per la sicurezza che l'art. 1, c. 1, lett. a della legge n. 124/2007 già conferisce al Presidente del Consiglio dei Ministri.

[86] Fanno parte del CIC il Presidente del Consiglio (che lo presiede); l'Autorità delegata, ove istituita; e, secondo la nomenclatura richiamata dalla legge, il Ministro degli affari esteri e della cooperazione internazionale; il Ministro dell'interno; il Ministro della giustizia; il Ministro della difesa; il Ministro dell'economia e delle finanze; il Ministro dello sviluppo economico; il Ministro della transizione ecologica; il Ministro dell'università e della ricerca; il Ministro delegato per l'innovazione tecnologica e la transizione digitale; il Ministro delle infrastrutture e della mobilità sostenibili.

[9] Il nucleo è presieduto dal direttore o dal vicedirettore generale dell'ACN ed è composto dal Consigliere militare del Presidente del Consiglio, e da un rappresentante di DIS, AISI, AISE, di ciascuno dei ministeri del CIC e del Dipartimento della protezione civile. Limitatamente alla trattazione di informazioni classificate, anche da un rappresentante dell'Ufficio centrale per la segretezza (istituito presso il DIS, ai sensi dell'articolo 9 della legge n. 124 del 2007).

[10] Il concetto di "difesa" cyber, che allude al complesso delle attività che insistono sulla preparazione delle capacità di natura militare e alla difesa dalle aggressioni di mano straniera e statuale, è oggi aggiornato e incorporato in quello concettualmente più ampio di "*resilienza cibernetica*", che come si vedrà a brevissimo sintetizza un novero di attribuzioni e responsabilità *urbi et orbi* deputate al rafforzamento delle capacità nazionali di resistenza cibernetica, negli ambiti essenziali per gli interessi strategici della nazione, in termini non soltanto di risposta all'incidente, ma di prevenzione, sviluppo tecnologico, formazione ed informazione negli ambiti pubblici e privati. In particolare, in Azzarone (2015c), p. 86 s. è contenuta un'ampia analisi della galassia delle possibili minacce nel dominio cyber, come in materia di comunicazioni mobili, telefonia Voip, *open source software* (Oss), infrastruttura bitcoin, sistemi satellitari, *Internet of things* e automobili di nuova generazione.

[11] De Gennaro (2011); Azzarone (2014a), pp. 62 – 76; Azzarone (2014b), pp. 36 – 47; Azzarone (2014c); Azzarone (2015a), pp. 88 – 98; Azzarone (2015b), pp. 124 – 132; Azzarone (2015c), pp. 84 – 94.

[12] Dal canto suo, il comparto di informazione per la sicurezza della Repubblica già da tempi non sospetti ha colto la rilevanza del dominio cyber tra le attività strategiche di interesse per la sicurezza nazionale, potenziando le proprie capacità anche in termini di cyber-intelligence (o CYBINT) e quindi di raccolta e analisi informativa pensata e adattata alle specificità del dominio operativo cibernetico Caligiuri (2016), p. 23 s.; Gori (2016), p. 87 s.

[13] Già la strategia nazionale per la sicurezza dello spazio cibernetico, delineata con il Decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013, definiva il quadro strategico per individuare i profili di minaccia per i sistemi e le reti di interesse nazionale, distribuendo

In effetti, la minaccia *cyber* ha da sempre avuto l'attitudine a incidere in modo trasversale in tutti i settori che la legge n. 124/2007 definisce come di interesse istituzionale dell'attività dell'*intelligence*, racchiusi nel prisma del concetto di sicurezza nazionale[1418]. Sicché, da un punto di vista di sistema, la considerazione più rilevante da cui partire è il rango della sicurezza cyber e la sua appartenenza allo spettro delle responsabilità di Alta direzione delle politiche di sicurezza nazionale che sono attribuite in via ordinaria al Presidente del Consiglio dei ministri[15].

Non c'è dubbio che la sicurezza nel dominio cibernetico sia una delle espressioni del moderno concetto di sicurezza nazionale[16], con il quale individuiamo quel novero di valori indispensabili sui quali si basa la stessa sopravvivenza della Repubblica come comunità di istituzioni e di cittadini e quelle indefettibili necessità ultra-individuali legate al mantenimento delle condizioni essenziali per tenere una nazione unita e proteggerne lo sviluppo[17].

Questa modernità della sicurezza nazionale si coglie in ragione del fatto che, a fianco delle esigenze più tradizionali quali la difesa dello Stato democratico e delle istituzioni poste dalla Costituzione a suo fondamento, sono state individuate nuove aree di intervento, quali l'economia, l'industria, l'energia o la tecnologia, segnando il passaggio ad una nuova era[18]: quella dell'emancipazione da una dimensione della sicurezza che era circoscritta allo Stato-apparato, dove è lo Stato stesso ad essere il monopolista dei beni giuridici da proteggere, ad una sicurezza che abbraccia lo Stato-comunità e tutte le sue plurime, trasversali, espressioni in campo sociale, industriale, economico e scientifico, e, da ultimo, nondimeno cibernetico.

Tanto è vero che il pregiudizio alla sicurezza nazionale è stato di recente cristallizzato nell'art. 1 del D.P.C.M. n. 131 del 20 luglio 2020, che lo declina come "danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale".

Ad una nozione pluralista e multiforme della sicurezza nazionale corrisponde, nei fatti, una certa omogeneità nella struttura delle articolazioni deputate a garantirla: l'architettura cyber sembra essere stata mutuata da quella del Sistema di informazione per la sicurezza della Repubblica, così come definito dalla legge n. 124/2007[19]. In entrambi i casi l'organo apicale, centro delle responsabilità e dei poteri in materia di sicurezza della Repubblica, è il Presidente del Consiglio, il "crocevia istituzionale" dell'intero sottosistema di organismi e di autorità, con il potere di impartire direttive per la sicurezza (anche cyber) ed emanare disposizioni per l'organizzazione e il funzionamento delle agenzie; l'autorità delegata per il Sistema di informazione può ricevere le deleghe presidenziali in materia di sicurezza cibernetica; anche per il sistema cyber è prevista la vigilanza del Comitato parlamentare per la sicurezza della Repubblica (il COPASIR)[20], c'è il Comitato interministeriale e, infine, mentre per il comparto di sicurezza ci sono due agenzie con competenze all'interno (AISI) ed all'esterno (AISE) dei confini della Repubblica, per la sicurezza cibernetica c'è l'ACN che assolve le principali funzioni a carattere operativo, al cui interno, in seno al nucleo di gestione della crisi, siedono i referenti delle agenzie del comparto di sicurezza[21].

in particolari ruoli e compiti in materia di difesa cyber tra i soggetti pubblici del sistema di informazione per la sicurezza della Repubblica.

[1418] V. le relazioni del DIS al Parlamento a partire dal 2017 e Gori (2014), pp. 5 – 29.

[15] V. Corte Cost., sentenza 24 maggio 1977, n. 86; v. per tutti Valentini (2008), p. 40 ss.; Giupponi (2010a), *Luigi Arcidiacono*, p. 1677 ss.; Giupponi (2010b), *Nuovi profili*, p. 53 ss.; Caia (2022), p. 1037 ss.

[16] La sicurezza nazionale è il più recente approdo di un lungo cammino evolutivo politico, normativo e sociale, naturale riflesso della storia, piuttosto fibrillante, della Repubblica Italiana, che ha visto avvicendarsi diverse interpretazioni, figlie del loro tempo, su quali fossero i valori supremi da difendere: la ragion di Stato, la *salus rei publicae*, la sicurezza politica ed infine la sicurezza nazionale, ognuno di quali rappresenta, con sfumature diverse di significato, i valori supremi della Repubblica da proteggere. Per un approfondimento Kostoris (1964), p. 2 ss.; Grevi (1976 - 2012), p. 659 ss.; Grevi (1978), p. 230 ss.; Pizzetti (1978), p. 81; Mosca (1985), p. 190 ss.; Barile (1987), p. 29; Conso (1979), p. 179; Pisa (1977), p. 1206; Di Bitonto (2006), p. 253. s.; Mosca et al. (2008), *passim*; Bonzano (2010a), p. 5 ss.; Giupponi (2010a), p. 1677 ss.; Giupponi (2010b), p. 57 s.; Bonzano (2011); Morrone (2010), p. 12; Mosca (2012), p. 21; Maffettone S. e Melidoro D. (2015); Giupponi (2017), p. 856 ss.; Mosca (2018), p. 5 s.; Mosca (2018b); Mosca (2019), p. 152; Caligiuri (2021); Giupponi (2023), p. 1149 ss.; Bifulco (2023), p. 1096 ss.; Salvi (2023), p. 248 ss.; Volendo anche Ricotta (2023a).

[17] V. Corte Cost., sentenza 23 febbraio 2012, n. 40, v. Pace (2015), p. 1727.

[18] De Gennaro (2019), p. 85.

[19] Per i riferimenti sull'attuale organizzazione del Sistema di Informazione per la Sicurezza della Repubblica (SISR) v. Mosca *et al* (2008), Montagnese A. e Neri C. (2016), p. 5 ss.; Caia G. e Bresciani P. (2021), p. 329 ss.; Caia (2022), p. 1037 ss.

[20] L'art. 5, c. 6, del d. l. n. 82/2021 precisa che il Copasir, ai sensi dell'art. 31, comma 3, della legge 3 agosto 2007, n. 124 "può chiedere l'audizione "del direttore generale dell'Agenzia su questioni di propria competenza (art. 5, co. 6).

[21] Art. 8 del decreto-legge n. 82/2021.

La contiguità tra i sistemi è quindi evidente per struttura e per ragion d'essere, ma, come si vedrà nel paragrafo che segue, il legislatore non ha inteso qualificare l'Agenzia come di informazione per la sicurezza per ragioni che attengono alle mansioni istituzionali che è chiamata a svolgere, richiamando di conseguenza funzioni diverse (quindi non raccolta informativa a spettro variabile per scopi di sicurezza) e soprattutto un sistema di regole ordinarie e non speciali che diversamente contraddistinguono l'attività dei servizi di informazione per la sicurezza.

Cionondimeno, la convergenza del sistema cyber verso il Presidente del Consiglio e sotto l'usbergo delle responsabilità e dei poteri di alta direzione in materia di politiche di sicurezza dello Stato ha certamente una rilevanza perché, in ipotesi di rischio alla sicurezza nazionale, gli interessi, le libertà (*i.e.* economiche) o i poteri concorrenti (*i.e.* giudiziari) sono destinati ad essere soddisfatti in via recessiva, o addirittura a soccombere rispetto all'esercizio dei poteri politici presidenziali.

4. L'Agenzia per la cybersicurezza nazionale: un'agenzia di *intelligence* oppure no?

L'art. 5 del D.L. n. 82/2021 ha istituito l'Agenzia per cybersicurezza nazionale a tutela degli interessi nazionali nel capo della cybersicurezza. L'ACN è l'Autorità nazionale per la cybersicurezza, con personalità giuridica di diritto pubblico, dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, guidata da un direttore generale[22], che è l'organo di gestione nominato dal Presidente del Consiglio e al quale riferisce unitamente all'Autorità delegata, e consta di un vicedirettore e di un collegio dei revisori dei conti.

L'ACN è investita dalla legge del ruolo di nodo centrale per la cybersicurezza, l'unica Autorità nazionale per la difesa e la resilienza cibernetica[23], competente per tutto un ampio spettro di attività a carattere regolamentare e investigativo: per la promozione e lo sviluppo di competenze e capacità tecnologiche, essa assume le iniziative idonee alla valorizzazione della crittografia e alla qualificazione dei servizi *cloud*, all'effettiva capacità di prevenire, rilevare e fornire risposte a incidenti e attacchi informatici, allo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche e al raccordo tra le diverse amministrazioni dello Stato con competenze in materia di cybersicurezza.

Nel definire gli scopi istituzionali dell'ACN, dall'originario testo dell'art. 5 del decreto-legge n. 82/2021, è stato espunto in sede di conversione il riferimento alla tutela della sicurezza nazionale nello spazio cibernetico[24]. Come anticipato, la volontà legislativa, quindi, pare essere quella di collocare l'ACN al di fuori del comparto informativo di sicurezza, per ragioni che si radicano in esigenze di carattere operativo: *in parte qua* il DIS ha transitoriamente svolto un doppio ruolo di supplenza in materia di difesa e prevenzione dei rischi informatici, essendosi occupato dell'approvvigionamento informativo e della risposta in caso di minacce o incidenti alle infrastrutture critiche della nazione, svolgendo al contempo funzioni ispettive nei confronti degli enti vigilati all'interno perimetro di sicurezza e di coordinamento dell'attività dei ministeri coinvolti[25].

Risulta evidente che il complesso delle mansioni attribuite oggi all'Agenzia cyber sia esorbitante rispetto alle funzioni istituzionali tradizionalmente affidate al comparto informativo per la sicurezza[26]: se diversamente fosse, si rischierebbe di gravare sulle capacità operative del

[22] Nominato tra i soggetti che possono essere nominati segretario generale della Presidenza del Consiglio, vale a dire magistrati delle giurisdizioni superiori, professori universitari di ruolo, dirigenti generali dello Stato, avvocati dello Stato o estranei alla pubblica amministrazione, purché in possesso di documentata esperienza nella gestione dei processi di innovazione. L'incarico dura 4 anni ed è rinnovabile una sola volta per non più di altri 4 anni.

[23] L'istituzione dell'Agenzia cyber ha consentito di risolvere la frammentazione delle competenze tra autorità diverse (Ministero dello sviluppo economico, Presidenza del Consiglio, DIS e Agenzia per l'Italia digitale).

[24] L'originario testo dell'art. 5 del decreto-legge 14 giugno 2021, n. 82, recitava "E' istituita, a tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico, l'Agenzia per la cybersicurezza nazionale".

[25] Un ruolo assai determinante, tanto è vero che al fine di assicurare la prima operatività dell'Agenzia cyber è stato previsto che il personale del DIS addetto alla sicurezza cibernetica venga messo a disposizione dell'Agenzia ed impiegato nelle attività oggetto di trasferimento. V. Art. 17 del decreto-legge 14 giugno 2021, n. 82. V. anche Salvi (2022), p. 10.

[26] L'eccentricità delle funzioni dell'ACN rispetto a quelle di informazione per la sicurezza in senso stretto si può ricavare dalla sistematica: con la riforma attuata con la l. n. 124/2007, istitutiva dell'attuale Sistema di informazione per la sicurezza della Repubblica (SISR), il legislatore

sistema, motivo per il quale è stato necessario affidare a una agenzia *ad hoc* compiti che idealmente coprono tutto lo spettro delle attività necessarie a garantire una tutela ottimale nel dominio *cyber*.

Da una diversa prospettiva, le ragioni di una differenziazione circa la natura dell'Agenzia è essenziale sul piano delle attività che è chiamata a condurre. Gli organismi di informazione per la sicurezza agiscono secondo un modello unico nel suo genere, che coniuga una tendenziale libertà delle forme nei modi della raccolta informativa e nell'attività operativa con la pressoché totale segretezza dell'intero comparto circa l'attività, i mezzi, le strutture, il personale, le finanze, regole e protocolli interni. Modello, quest'ultimo, che difficilmente potrebbe contraddistingue l'Agenzia Cyber, la cui attività ha invece una spiccata proiezione esterna.

Così, inaugurando l'ACN, si è costituito un unico ente regolatore di diritto pubblico che, poiché collocato al di fuori del sistema di informazione per la sicurezza della Repubblica, garantisce maggiore trasparenza, efficacia e garanzia nei rapporti tra enti pubblici e con i soggetti privati, soprattutto in sede di esercizio dei poteri ispettivi e di vigilanza.

Quindi, se da un lato gli interessi in materia cibernetica rientrano nello spettro delle attribuzioni in materia di sicurezza nazionale che fanno capo al Presidente del Consiglio dei ministri, dall'altro, il legislatore non ha inteso qualificare l'agenzia come un organismo di informazione per la sicurezza, e quindi non le ha attribuito tutta una serie di prerogative speciali e derogatorie che diversamente caratterizzano l'attività di quest'ultimo comparto[27]. Da qui, se ne possono trarre alcune conseguenze: l'Agenzia agisce su mandato del Presidente del Consiglio ma secondo il paradigma procedimentale ordinario, dovendosi escludere l'applicazione della speciale normativa prevista dalla legge n. 124/2007 al di fuori di quelle disposizioni, come in materia di poteri presidenziali e segreto di Stato, che hanno portata generale.

5. *Segue*. L'inapplicabilità della speciale disciplina in materia di attività di informazione per la sicurezza della Repubblica.

Una delle conseguenze dell'esclusione dell'Agenzia *cyber* dal novero degli organismi che compongono il Sistema di informazione per la sicurezza è la sostanziale inapplicabilità della speciale disciplina prevista dalla legge n. 124/2007, oltreché delle numerose disposizioni del codice di procedura penale poste a tutela delle speciali funzioni del comparto informativo per la sicurezza[28].

Una prima, sostanziale, differenza si riscontra sul piano della segretezza. Pressoché ogni aspetto dell'attività, delle scelte e dell'organizzazione degli organismi di informazione per la sicurezza è coperto, o è assoggettabile, al segreto di Stato[29]. Diversamente, l'Agenzia non è vincolata allo stesso regime di segretezza in ragione delle funzioni che la legge le attribuisce, in particolare quelle di vigilanza ed ispezione, che per essere esercitate richiedono lo svolgimento di attività palesi ed una certa *discovery* informativa.

---

ha inteso conferire piena autonomia alle funzioni dei Servizi, separando in via ordinaria l'attività di informazione per la sicurezza da quella preventiva e repressiva tipica delle forze di polizia (vista l'evidente contiguità tra quest'ultime funzioni, la separazione limita potenziali sovrapposizioni v. (Gambacurta (2008b), p. 304 ss.; Giupponi (2009), p. 2 s.; Caia (2022), p. 1045). La peculiare natura della funzione amministrativa specializzata dell'informazione per la sicurezza (v. Caia (2022), p. 1037 ss.), risulta determinante poiché si riverbera anche sul piano delle finalità rispetto alle quali anche le attività operative possono essere compiute: i Servizi operano esclusivamente sul piano della raccolta informativa per finalità di tutela della sicurezza nazionale, che è attività più ampia della funzione preventiva e svolta dalle forze di polizia (v. Jemolo (1995)) Per contro, l'autorità di pubblica sicurezza ha un ambito di competenza generalizzata in materia di prevenzione e repressione: è quindi questa l'autorità preposta in via ordinaria a ricorrere a misure attive, a carattere operativo, adottate in funzione di tutela fattiva della sicurezza pubblica. La legge n. 801/1977 aveva istituito appositi Servizi per le *informazioni e la sicurezza*, mentre l'assetto oggi definito dalla l. n. 124/2007 richiama per i Servizi l'attività di *informazione per la sicurezza*. La differenza tra queste due diverse formulazioni non è meramente lessicale: con servizi di *informazione e sicurezza* si intendeva richiamare l'attribuzione ai Servizi di poteri per il compimento di azioni operative dirette a tutelare la sicurezza interna; viceversa, con attività di *informazione per la sicurezza* la riforma ha inteso ribadire la centralità dei compiti informativi (v. in particolare Giupponi (2009), p. 2 s), separandoli da quelli di sicurezza in senso stretto che spettano in via principale alle autorità di pubblica sicurezza.

[27] Si tratta di una soluzione in linea con le funzioni attribuite all'Agenzia, tant'è che i provvedimenti adottati dall'Agenzia cyber sono sindacabili innanzi al Giudice Amministrativo, vista l'aggiunta all'art. 135 del codice del processo amministrativo, in materia di competenza funzionale inderogabile del Tar Lazio, sede di Roma, a giudicare "le controversie aventi ad oggetto i provvedimenti dell'agenzia per la cybersicurezza nazionale".

[28] *Infra* in questo §.

[29] Sono suscettibili di apposizione del segreto di Stato pressoché tutte le informazioni sull'attività e l'organizzazione degli organismi di informazione per la sicurezza V. in particolare l'art. 5 del D.P.C.M. dell'8 aprile 2008.

Resta comunque invariato il potere-dovere di proteggere tutte quelle informazioni sensibili che si generano nel corso dell'attività istituzionale, secondo le regole ordinarie previste dalla legge n. 124/2007: ogni qual volta si origini un'informazione che non deve essere divulgata per ragioni di sicurezza[30], il personale si adopera per garantirne la riservatezza ed informare il Presidente del Consiglio e l'Organizzazione Nazionale per la sicurezza affinché sia apposto il segreto di Stato o una classifica di segretezza. Questo vale anche nei rapporti con l'accertamento condotto in parallelo dall'autorità giudiziaria, alla quale il segreto di Stato può essere opposto secondo le regole di applicazione generale previste dal codice di procedura penale e dalla legge n. 124/2007[31].

Discorso diametralmente opposto deve essere fatto per la comunicazione della notizia di reato, *ex* art. 23 della l. n. 124/2007, e per l'applicazione delle speciali garanzie funzionali contenute all'art. 17 della legge n. 124/2007[32] e agli artt. 256 *bis*[33] e 270 *bis*[34] c.p.p.: si tratta di disposizioni eccezionali che, come tali, non possono essere applicate in via estensiva.

6. *Segue*. La comunicazione della notizia di reato.

La questione delle esigenze connesse alla tutela della sicurezza nazionale assume particolare rilievo in relazione dell'obbligo di denunciare la notizia di reato prescritto all'art. 331 c.p.p. per tutti i pubblici ufficiali e gli incaricati di pubblico servizio che, nell'esercizio delle loro funzioni, abbiano conoscenza di un reato perseguibile di ufficio.

Nel sistema di informazione per la sicurezza, ragioni di stretta necessità correlate al perseguimento delle relative funzioni istituzionali consentono ai direttori delle agenzie che compongono il Sistema di ritardare la comunicazione della notizia di reato (art. 23 l. n. 124/2007).

Poiché il potere di ritardare la comunicazione della *notitia criminis* risulta essenzialmente legato a ragioni di sicurezza nazionale, potrebbe accadere che anche nel sistema cyber sorga la necessità di non comunicare tempestivamente la notizia di reato per non compromettere l'azione dell'Agenzia o aggravare la crisi: c'è allora da domandarsi se per l'ACN questo sia possibile in assenza di una specifica disposizione di legge.

Nell'attività di informazione per la sicurezza, ai sensi dell'art. 23 l. n. 124/2007[35] il personale del contingente speciale ex art. 21 della l. n. 124/2007 non riveste la qualifica, salvo il caso di concessione temporanea, né di agente/ufficiale di pubblica sicurezza né di polizia giudiziaria, risultando di conseguenza sgravato da tutta una serie di adempimenti e obblighi

[30] Vige in materia di segreto di Stato una regola generale, cardine del sistema: pubblici ufficiali, incaricati di pubblico servizio o impiegati pubblici hanno l'obbligo di non divulgare e di mantenere il riserbo sulle notizie coperte da segreto di Stato, sancito in via generale all'art. 41 legge n. 124/2007 rubricato "Divieto di riferire riguardo a fatti coperti dal segreto di Stato.

[31] In particolare, alle disposizioni in materia di tutela del segreto di Stato nel corso dell'attività acquisitiva degli elementi di prova dichiarativa (art. 202 c.p.p.) o documentale (artt. 256 s. c.p.p.). In via generale, il segreto di Stato viene sempre tutelato, a prescindere da dove si generi la notizia riservata o da chi ne sia in possesso: sicché, ogni qual volta la legge tutela la segretezza dell'informazione, dovrà applicarsi la relativa disciplina. Con particolare riferimento all'accertamento penale, il dovere di tutelare il segreto di Stato si declina in tutti i principali momenti dell'acquisizione probatoria, prescrivendo specifiche regole che hanno la funzione di non compromettere né il segreto né tantomeno le attribuzioni del Governo. Quando il segreto è opposto, l'autorità giudiziaria interpella il Presidente del Consiglio affinché confermi o meno il segreto di Stato, e nelle more della decisione ha il dovere di astenersi da qualsiasi condotta volta all'acquisizione della notizia per la quale è stato opposto il segreto. v. Bonzano (2008), p. 24 ss.; Bonzano (2011), p. 586 ss.; v. anche Spangher (1993), p. 471 ss.; Cerruti (2013), p. 35 s.; Dell'anno (2020), p. 220; Bonzano (2023), p. 3649 ss.; volendo anche Ricotta (2023b).

[32] L'art. 17 della l. n. 124/2007 prevede che gli appartenenti agli organismi di informazione non siano punibili qualora ricorrano ad azioni punite come reato ma indispensabili per le finalità di sicurezza, purché autorizzati e non si tratti di condotte espressamente escluse dalla speciale causa di giustificazione (artt. 17 e 18 e l. n. 124/2007) v. Mosca (2008), p. 235 ss.; Mosca (2018a), p. 115 ss.; Caia (2022), p. 1047 s.

[33] L'art. 256-*bis* c.p.p. prescrive una speciale procedura di acquisizione documentale custodita presso le sedi delle agenzie che afferiscono al sistema di informazione per la sicurezza della Repubblica e che sia sottoposta a segreto di Stato: il pubblico ministero non può procedere coattivamente né alla perquisizione né al sequestro, ma deve trasmettere necessariamente un previo ordine di esibizione avendo cura di specificare gli incartamenti di interesse investigativo e i motivi per cui sta procedendo. L'ordine di esibizione instaura una procedura controllata di divulgazione: se non è apposto il segreto di Stato e i documenti esistono, il pubblico ministero può esaminare la documentazione in sede con la collaborazione del personale dell'agenzia. Questo significa che, impregiudicato il segreto di Stato, il divieto di attività coercitive di perquisizione e sequestro di iniziativa dell'organo dell'accusa nei confronti dell'Agenzia non dovrebbe essere *tout court* applicabile, se non limitatamente ai luoghi e alle funzioni che vedono la diretta partecipazione dei Servizi, come nel nucleo per la cybersicurezza e gestione della crisi v. Dell'anno (2022), p. 224 s.; Rivello (2023a), p. 3381 – 3383.; Rivello (2023b), p. 3383 - 3385.

[34] Non può ritenersi applicabile la specifica disciplina dell'art. 270-*bis* c.p.p. sulla inutilizzabilità delle intercettazioni qualora siano state captate comunicazioni di servizio tra appartenenti al Sistema di informazione per la sicurezza. La norma accorda infatti la garanzia della regola di esclusione probatoria seguendo un criterio funzionale e soggettivo: soltanto le conversazioni di servizio che non abbiano natura squisitamente privata, purché provengano da interlocutori che appartengono al sistema di informazione per la sicurezza. Bonzano (2023), p. 3649 ss.; Dell'anno (2020), p. 228 s.

[35] V. Gambacurta (2008a), p. 287 ss.

tipici di quest'ultime funzioni (e.g. il dovere di intervento e di arresto obbligatorio in flagranza) nonché, con particolare riferimento alla P.G., dalla subordinazione al pubblico ministero.

L'esclusione di quest'ultime qualifiche non significa che il personale non sia da considerarsi, comunque, un pubblico ufficiale (alla stregua dei criteri dell'art. 357 c.p.p.): per questo, l'art. 23 l. n. 124/2007 non elimina *tout court* l'obbligo di denuncia dei fatti che costituiscono reato, ma stabilisce, in deroga al regime ordinario, una procedura *ad hoc*: se nell'ambito dell'attività informativa emergono fatti che costituiscono un reato, in un primo passaggio interno il personale comunica l'esistenza del reato ai direttori delle rispettive agenzie o al direttore generale del DIS, che a loro volta hanno l'obbligo di comunicarla alla polizia giudiziaria (e non direttamente al pubblico ministero), che a sua volta ne cura la successiva trasmissione all'ufficio di Procura. A differenza che nel regime ordinario, in questo caso la trasmissione della notizia e delle relative informazioni può essere intempestiva qualora sia strettamente necessario al perseguimento delle finalità istituzionali del Sistema di informazione: previa autorizzazione del Presidente del Consiglio, l'art. 23 della l. n. 124/2007 consente ai già citati direttori di ritardare la comunicazione della notizia di reato.

La *ratio* dell'art. 23 della l. n. 124/2007 è quella di garantire la reciproca autonomia ed equilibrare i rapporti tra potere esecutivo e giudiziario, aprendo al contempo un canale di comunicazione che serve ad acquisire elementi utili a fini investigativi salvaguardando le prerogative degli organismi di informazione[36]. L'evidente specialità della disciplina, legata all'esercizio delle funzioni di informazione per la sicurezza, a rigore di logica non ne consente l'estensione all'ACN, i cui funzionari, in assenza di una disposizione analoga all'art. 23 della l. n. 124/2007 ed in virtù della propria qualifica di pubblici ufficiali, sono tenuti a comunicare, sempre e senza ritardo, la notizia di reato al pubblico ministero o alla polizia giudiziaria.

Si potrebbe sostenere che, anche in assenza di una disciplina *ad hoc*, ragioni di sicurezza nazionale legate al dominio cibernetico consentirebbero al Presidente del Consiglio, nell'esercizio dei suoi poteri di Alta direzione, di intervenire per evitare o limitare la diffusione di una notizia avvalendosi dello strumento della secretazione, che avrebbe l'effetto, diretto o indiretto, di non portare a conoscenza dell'autorità giudiziaria fatti dai quali si potrebbe trarre l'esistenza di un reato.

Si tratta, tuttavia, di una questione particolarmente delicata, come tale refrattaria a soluzioni *tranchant*. Questo perché, nell'ottica della disciplina della l. n. 124/2007, l'esigenza di segretezza è insita nell'informazione o nella notizia della quale è pericolosa *ex se* la diffusione, a prescindere dal soggetto che la origina o che dovrebbe esserne il destinatario[37]: se ne ricorrono i presupposti, e ci si trova al di fuori delle ipotesi di segreto vietato[38], pressoché tutto può essere sottoposto a segreto di Stato.

Al tempo stesso, il meccanismo dell'art. 23 della l. n. 124/2007 disciplina un procedimento evidentemente eccezionale, in deroga al dovere generale stabilito per i pubblici ufficiali e gli incaricati di pubblico servizio ex art. 331 c.p.p., che si muove sul terreno del delicato equilibrio tra poteri dello Stato e del necessario rispetto dell'autonomia e delle diverse attribuzioni del potere esecutivo e di quello giudiziario[39]: il solo fatto che la menzionata disposizione esista, in altre parole, avrebbe la conseguenza di non lasciare spazi a meccanismi di ritardata comunicazione della *notitia criminis* al di fuori di quelli già espressamente previsti dalla legge. Del resto, se il segreto è pur sempre la condizione naturale dell'attività investigativa, quello di Stato si contraddistingue per essere l'*extrema ratio* e non uno strumento ordinario di gestione della crisi.

7. I poteri investigativi dell'Agenzia per la cybersicurezza nazionale e le indagini dell'autorità giudiziaria.

Se da un lato la legge n. 124/2007 continua a costituire il paradigma normativo per il complesso delle attività legate alla politica informativa di sicurezza, dall'altro, il d. l. n. 82/2021

[36] Cfr. Gambacurta (2008a), p. 292.
[37] Per la cd. "concezione ontologica" del segreto di Stato *cfr*. Corte Cost., sentenza 3 aprile 2009, n. 106; v. Bonzano (2010b), p. 301 ss.; v. anche Pace (2015), p. 1719 ss.; in generale, sull'apposizione del segreto di Stato, v. Scandone (2008), p. 499 ss.; Bonzano (2008), p. 17 ss.; Giupponi (2010a), p. 1684 ss.; Caia (2022), p. 1037 ss.; volendo, anche Ricotta (2023a).
[38] Ex art. 39 c. 11 l. n. 124/2007 e art. 204 c.p.p.
[39] V. Gambacurta (2008a), pp. 291-292.

ha il pregio di cristallizzare un sistema di difesa e resilienza informatica *ad hoc*, chiamato ad operare, per ragioni di sistema, in sinergia con il comparto di informazione per la sicurezza e sotto l'egida del Presidente del Consiglio nel suo ruolo di organo di vertice delle politiche di sicurezza dello Stato, ma con competenze, mezzi e funzioni altamente specializzate in virtù del dominio operativo e delle specifiche attribuzioni dell'ACN.

La capacità di prevenire e rilevare attacchi e minacce alle infrastrutture digitali, così come quella di vigilare sugli enti allo scopo di monitorare la corretta attuazione e implementazione delle misure di natura tecnica e organizzativa, accertare le violazioni e irrogare eventuali sanzioni, l'art. 7 del d.l. n. 82/2021 attribuisce all'Agenzia un complesso di poteri autoritativi di natura amministrativa, funzionali alla sorveglianza, al controllo sul rispetto degli obblighi sugli enti inseriti nel perimetro di cyber-sicurezza o destinatari delle direttive NIS. A questi poteri, si sommano quelli previsti dall'art. 41 del Codice delle comunicazioni elettroniche, che ribadiscono il potere dell'Agenzia cyber di verificare l'adeguatezza organizzativa e indagare i casi di mancata conformità alle prescrizioni tecnico-organizzative ed i relativi effetti sulla sicurezza delle reti e dei servizi.

Questa funzione di vigilanza si esplica necessariamente attraverso l'esercizio di tutta una serie di poteri a carattere ispettivo/investigativo, come il potere di richiedere l'esibizione o la trasmissione di dati, notizie e documenti, invitare il soggetto vigilato a comparire per fornire indicazioni o procedere all'esecuzione di accessi, ispezioni e verifiche[40].

Poteri che l'agenzia esercita in proprio, ma anche avvalendosi della collaborazione delle Forze di Polizia, anche alla luce dello stretto coordinamento con il nucleo di Polizia di Stato e delle telecomunicazioni e del CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche)[41].

Poiché ogni possibile attacco informatico può costituire anche un crimine penalmente sanzionato[42], è altamente probabile che l'investigazione dell'Agenzia *cyber* si intersechi con quella dell'Autorità giudiziaria: una volta che è emersa la notizia di reato, a rigore di logica i pubblici ufficiali dell'ACN dovrebbero tempestivamente comunicarla all'autorità giudiziaria, il pubblico ministero iscriverla nel relativo registro, anche nel caso in cui sia ignoto l'autore del reato, e conseguentemente avviare formalmente le indagini preliminari.

Rilevano allora due profili di interesse: le garanzie applicabili all'investigazione amministrativa una volta che sia emersa una notizia di reato; la possibile sovrapposizione tra ACN e Procura della Repubblica, alla luce del fatto che entrambe hanno competenze e responsabilità in materia di investigazioni ma manca, nel decreto, una norma che le coordini.

8. Cenni sulla migrazione dei risultati dell'inchiesta amministrativa e sull'art. 220 disp. att. c.p.p.

Il passaggio dall'attività di investigazione amministrativa all'indagine preliminare del pubblico ministero è regolato in via generale dall'art. 220 disp. att. c.p.p.[43], a norma del quale "quando nel corso di attività ispettive o di vigilanza previste da leggi o decreti emergono indizi di reato, gli atti necessari per assicurare le fonti di prova e raccogliere quant'altro possa servire per l'applicazione della legge penale sono compiuti con l'osservanza delle disposizioni

[40] Così l'art. 13 della legge 24 novembre 1981 n. 689. Si v. Sorbello (2016), p. 128; v. anche Furgiuele (2020), p. 147 ss.

[41] L'art. 7 d.l. n.82/2021 specifica ulteriormente che le funzioni dell'agenzia sono esercitate nel rispetto delle attribuzioni delle altre amministrazioni dello Stato, e in particolare del Ministro dell'interno che è l'autorità nazionale di pubblica sicurezza. In questo caso il riferimento al Ministro dell'Interno valorizza la funzione principale del dicastero, e cioè quella di garantire l'ordine e la sicurezza pubblica, dalla quale scaturiscono competenze specifiche in termini sia di polizia giudiziaria che di polizia di sicurezza. Peraltro, è proprio all'interno di tale Ministero che opera il principale raccordo operativo dell'ACN con le forze di polizia in caso di minacce, attacchi e criminalità informatica, vale a dire il Centro Nazionale Anticrimine. Peraltro, è proprio all'interno di tale Ministero che opera il principale raccordo operativo dell'ACN con le forze di polizia in caso di minacce, attacchi e criminalità informatica, vale a dire il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (il CNAIPIC), l'organo istituito allo scopo di garantire la sicurezza e la regolarità dei servizi di telecomunicazione e delle infrastrutture critiche di interesse nazionale dall'art. 7-*bis,* c. 1 del DPR n. 144/2005.

[42] Del resto, l'adesione alla convenzione di Budapest ha consentito l'introduzione, a livello dell'Unione Europea, di un modello normativo comune per il contrasto alla criminalità informatica, che ha di fatto consentito di criminalizzare qualsiasi condotta che costituisca un attacco informatico a una infrastruttura critica v. Cadoppi *et al.* (2019).

[43] Si v. Nobili (1984), p. 376 s.; Kostoris (1990), p. 73 s.; Orlandi (1992), p. 93; Fumu (1992), p. 100 s.; Cesari (1993), p. 214 s.; Scalfati (2020), p. 1 ss.; Furgiuele (2020), p. 141 s.; Galantini (2022), p. 999 ss.; Galluccio Mezio (2023a), p. 3712 s.

del codice"[44].

La norma non codifica un vero e proprio passaggio di consegne tra indagine amministrativa e penale, poiché nel rispetto delle reciproche attribuzioni i due procedimenti possono proseguire in parallelo[45], ma segna un momento, l'emersione della notizia di reato, a partire dal quale risulta necessario che gli elementi investigativi vengano raccolti con l'osservanza delle regole del rito, per non frustrare o aggirare le relative garanzie[46].

L'art. 220 disp. att. c.p.p. costituisce una regola di legittimità dell'acquisizione delle fonti di prova[47] e ne condiziona la futura utilizzabilità nel processo penale se, nel corso dell'attività amministrativa, non sono state rispettate le garanzie prescritte dalla legge.

Il richiamo dell'art. 220 disp. att. c.p.p. alle attività ispettive e di vigilanza non deve essere interpretato in senso restrittivo ma estensivo, poiché non si limita a richiamare due particolari tipi di accertamento ma il generale esercizio di poteri istruttori di natura amministrativa, nell'ambito del quale emerga la conoscenza di un fatto che abbia rilevanza penale[48].

La conseguenza della violazione dipende dalle regole che sono previste garanzie che la legge prescrive per ciascun atto investigativo, come la facoltà di nominare e farsi assistere da un difensore nel momento in cui si rendono dichiarazioni[49] (ex artt. 63 e 350 c.p.p.) o nel corso di una perquisizione o di un accertamento tecnico irripetibile[50], secondo la disciplina del codice a cui l'art. 220 disp. att. c.p.p. rimanda[51].

La regola aurea è che quanto più si applicano garanzie difensive alle attività extra-procedimentali, tanto più si garantisce il *continuum* tra procedura amministrativa e investigazione penale. Così per l'acquisizione degli elementi di prova valgono certamente le regole di procedura penale ai fini dell'utilizzabilità e le garanzie procedimentali per i mezzi di ricerca della prova e, soprattutto, per gli accertamenti investigativi, con particolare riferimento a quelli che comportino una modificazione irreversibile dell'oggetto di prova.

Nella prospettiva di un possibile futuro dibattimento, sarà necessario garantire, chiunque sia l'autorità che materialmente conduce in quel momento le indagini e procede ai necessari accertamenti di natura tecnica, la partecipazione dell'interessato laddove sia possibile ed il rispetto dei protocolli forensi per assicurare affidabilità e controllabilità dell'elemento di prova raccolto. L'Agenzia *cyber* è del resto pensata per svolgere accertamenti ad alto livello di professionalità tecnica, che può corroborare ricorrendo anche ad enti terzi, pubblici o privati, dotati

[44] Alla disposizione richiamata fa da naturale *pendant* l'art. 223 disp. att. in materia di analisi e campionamenti non rivedibili, per le quali sono prescritte garanzie difensive e partecipative dell'interessato. L'art. 223 disp. att. è infatti legato all'art. 220 disp. att. da un rapporto di *genus ad speciem*, prescrivendo una particolare procedura garantita da applicare laddove, nel corso delle attività di ispezione e vigilanza contemplate all'art. 220 disp. att., si renda necessario procedere per la prima volta ad esami o a analisi non ripetibili, oppure, laddove sia materialmente possibile, l'interessato domandi all'autorità amministrativa la revisione delle analisi già effettuate cfr. Galluccio Mezio (2023b), p. 3725 ss.

[45] Kostoris (1990), p. 81; Mazza (2000), p. 1280 s.; Bontempelli (2009), p. 130 s.; Rampioni (2019), p. 241.

[46] Nobili (1984), p. 376; Ubertis (1992), p. 431; Furgiuele (2020), p. 145.

[47] Cass., Sez. III, 18 novembre 2014, n. 4919; Cass., Sez. III, 10 febbraio 2010, in *C.E.D. Cass.* n. 246599; Cass., Sez. V, 23 settembre 2004, n. 43542, in *questa rivista*, 2006, p. 2542.; contra si v. Furgiuele (2020), p. 159. Inoltre, l'osservanza di tale previsione rileva anche ai fini della eventuale illiceità disciplinare o addirittura penale derivante da quanto accaduto nel corso dell'attività ispettiva o di vigilanza.

[48] Il collegamento tra le due inchieste si fonda quindi sull'emersione di indizi di reato, vale a dire nella possibilità di "attribuire rilevanza penale al fatto che emerge dall'inchiesta amministrativa e nel momento in cui emerge, a prescindere dalla circostanza che esso possa essere riferito ad una persona determinata" (cit. Cass., Sez. Un., 28 novembre 2001, n. 45477, in *Giur. it.*, 2002, pag. 1235), vale a dire che siano emersi tutti gli elementi costitutivi (Cass., Sez. III, 4 giugno 2019, n. 31223, in *C.E.D. Cass.* n. 276679): una volta emersi gli indizi, si deve ritenere che sia stata avviata sostanzialmente una indagine penale, a prescindere che sia già stata formulata e iscritta la notizia di reato nel registro del pubblico ministero o siano già state individuate le norme di legge che si assumono violate (Cass., Sez. III, 24 settembre 2001, in *Giur. it*., 2002, pag. 1035; v. Cesari (1993), p. 215; Mazza (2000), p. 1280 s; Sorbello (2016), p. 134.). La semantica dell'art. 220 disp. att. mira evidentemente ad escludere la regola nelle ipotesi in cui vi sia soltanto un mero sospetto, e quindi dell'emersione di una situazione di fatto che si contraddistingue per una capacità argomentativa e dimostrativa minore, perché l'ipotesi del fatto si basa soltanto su intuizioni soggettive o è priva di riscontri oggettivi o, qualora presenti, anche questi siano insufficienti. Sulla differenza tra indizio e sospetto si veda Ubertis (1995), p. 296 s; con specifico riferimento al fatto che l'utilizzo del termine emersione indicherebbe nell'art. 220 disp att. c.p.p. uno stato embrionale dell'indizio di reato v. Furin (1999), p. 2722 s. È discusso invece se "indizi di reato" sia una formula equivalente a "notizia di reato", v. Kostoris (1990), p. 83; Orlandi (1992), p. 156;, oppure no v. Aprati (2010), p. 17 s. Va da sé che il fatto di reato così qualificato impone la sua comunicazione al pubblico ministero ai sensi dell'art. 347 c.p.p. (Paulesu (2023), p. 1509 ss.): *in parte qua*, seguendo le regole generali, gli operatori dell'Agenzia, a cui la legge attribuisce espressamente la qualifica di pubblico ufficiale nell'esercizio delle loro funzioni di ispezione e vigilanza, sono da considerare come ufficiali di polizia giudiziaria quantomeno ai fini dell'acquisizione della notizia di reato.

[49] Sul diritto al silenzio nei procedimenti amministrativi si v. Caneschi (2020), p. 579 ss.; Sforza (2022), p. 83 s.; Bonzano (2023), p. 47 s.

[50] L'art. 223 disp. att. prevede che qualora nel corso di attività ispettive o di vigilanza si devono eseguire analisi per le quali non è prevista la revisione, deve essere dato avviso all'interessato del luogo e dell'ora dove le analisi avranno luogo, affinché possa presenziare o farsi assistere da una persona di fiducia. In questo caso, se l'accertamento non rivedibile, vale a dire laddove l'oggetto dell'analisi sia soggetto a modificazione irreversibile, consentiva di integrare soggettivamente l'assunzione della prova con la presenza dell'interessato, che in presenza di indizi di reità doveva già qualificarsi come sottoposto ad indagine, si cristallizzerà l'inutilizzabilità nel momento in cui si sia proceduto in difetto dell'avvisto ex art. 360 c.p.p.

[51] Furgiuele (2020), p. 160.

di comprovate capacità operative. Lo spirito della normativa vuole incentivare la cooperazione delle società in funzione di evolvere le competenze di azione e prevenzione, a beneficio del sistema. Va da sé che, come già accade quando nell'inchiesta penale il pubblico ministero si avvale di privati nello svolgimento di attività che richiedono competenze particolari, essi agiscono sotto la direzione e la responsabilità del soggetto pubblico[52].

9. La concorrenza investigativa.

È già stato anticipato come lo spirito della normativa sia quello di incentivare la cooperazione tra diverse autorità. Le competenze sono ripartite su quattro pilastri, *cyber-defence, cyber-intelligence*, *cyber*-resilienza e *cyber-investigation*, attribuite a istituzioni differenti secondo un criterio di specializzazione delle funzioni: il ministero della difesa si occupa della difesa in senso stretto nel dominio *cyber*; il comparto di informazione per la sicurezza raccoglie e analizza le notizie, elabora e dissemina le informazioni, e si adopera per le azioni operative più opportune; l'Agenzia *cyber* investiga e adotta provvedimenti di ripristino e futura risposta; i reparti di polizia specializzata procedono alle indagini di polizia giudiziaria sotto la direzione dell'autorità giudiziaria, che esercita l'azione penale se ravvisa ipotesi di reato.

È dunque possibile che l'intervento congiunto dell'Agenzia e della Procura possa generare attriti, alla luce del fatto che entrambe, nonché le diverse forze di polizia che ne coadiuvano l'attività, hanno certamente competenze e responsabilità in materia di investigazioni, ma non c'è perfetta sovrapponibilità o concomitanza di interessi.

L'Agenzia è pensata per un intervento di immediata prossimità. Verosimilmente, essendo il punto di contatto che per primo riceve la notifica dell'incidente, è la prima autorità che interviene, e deve giungere sulla scena non appena la crisi si manifesta o l'incidente accade con il compito di ricostruire tempestivamente le cause dell'accadimento prima che i dati o gli elementi utili si disperdano o vengano irrimediabilmente compromessi, e soprattutto ripristinare il sistema, evitare ulteriori pregiudizi, attuali e futuri, alla sicurezza delle reti e dei sistemi. L'Agenzia assolve quindi ad una triplice funzione ripristinatoria, investigativa e di creazione di futura sicurezza.

La Procura invece nutre un interesse meno tecnico, non di sicurezza in senso stretto, che è la proiezione dei propri doveri istituzionali di acquisire e assicurare le fonti di prova in funzione dell'accertamento, quindi nell'ottica di costituirsi elementi spendibili nel procedimento e nel processo penale.

Un esempio, seppur potenzialmente virtuale[53], di conflitto tra autorità potrebbe accadere se si verificasse una stasi dell'attività di indagine cyber provocata dall'esecuzione di un provvedimento di sequestro di dispositivi, dei sistemi o di parte degli impianti coinvolti nell'inchiesta. Una stasi che non gioverebbe all'Agenzia, perché la sua funzione non è soltanto accertare le cause della crisi, ma anche evitare il propagarsi di ulteriori pregiudizi all'integrità e alla sicurezza: per ragioni di necessità l'Agenzia potrebbe intervenire per ripristinare lo *status quo ante* evitando ulteriori compromissioni della sicurezza e coinvolgendo soltanto successivamente l'ufficio di Procura. Questo vale anche se l'intervento tempestivo dell'Agenzia sacrifica elementi utili per le indagini penali o se la situazione non consente il rispetto delle garanzie del rito (e quindi, beninteso, la spendibilità probatoria degli elementi raccolti in difformità dal codice di rito).

A differenza che in altre investigazioni di sicurezza[54], come quelle in ipotesi di disastro

[52] Per i profili circa la commistione investigativa tra pubblico e privato nel processo penale si rimanda a Cesari (2021), p. 1174 s.

[53] Seppur, si deve osservare, che la stessa natura critica delle infrastrutture difficilmente farebbe sorgere la necessità, da parte del pubblico ministero, di sequestrare l'intero impianto o adottare un provvedimento che provochi la sostanziale stasi dell'infrastruttura, con gravi ripercussioni sulle relative funzioni cruciali.

[54] Una situazione di concorrenza investigativa fra autorità amministrativa e giudiziaria, molto vicina a quella appena descritta, ricorre in caso di disastro aereo che riporti delle vittime tra personale di bordo o passeggeri. Sorgono in questo caso diverse necessità: comprendere le cause dell'evento ed evitare che si replichino nel tempo, attraverso attività d'investigazione ultra-specializzate al fine di assicurare le fonti di prova e risultati quanto più attendibili possibile, che prende il nome di "inchiesta di sicurezza", che l'art. 2 del regolamento UE n. 996/2010 definisce come "un insieme di operazioni svolte da un'autorità investigativa per la sicurezza ai fini della prevenzione degli incidenti ed inconvenienti, che comprende la raccolta e l'analisi di dati, l'elaborazione di conclusioni, la determinazione della causa o delle cause e/o di fattori concorrenti e, ove opportuno, la formulazione di raccomandazioni in materia di sicurezza". Al riguardo, è stata istituita in Italia, con il d.lgs. n. 66/1999 (come modificato dal dpr. n. 189/2010 e dal regolamento UE n. 996/2010), una agenzia *ad hoc* che opera in condizioni di terzietà, l'Agenzia nazionale per la sicurezza del volo (ANSV) con poteri investigativi e sanzionatori; per un approfondimento v. Franchi (2015), pp. 3 ss.;

aereo, nell'architettura cyber non c'è un meccanismo che regoli l'indagine amministrativa con quella penale, disciplinando il coordinamento dei rispettivi atti istruttori o prevedendo regole che attribuiscano espressa preferenza all'una o all'altra inchiesta, evitando sovrapposizioni o conflitti.

In assenza di meccanismi formali[55], in questo specifico contesto il rango della sicurezza cibernetica, nel prisma della sicurezza nazionale, costituisce una direttrice di coordinamento: quando esigenze di sicurezza nazionale lo rendono necessario, le prerogative connesse ai poteri di alta direzione delle politiche di sicurezza, legittimano l'Agenzia ad un pieno intervento, che può svolgersi, ove necessario, *inaudita altera parte*, o con un coinvolgimento successivo dell'ufficio di Procura.

Nondimeno, il conflitto è per lo più potenziale, perché in concreto è proprio il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (il CNAIPIC) a fare da cerniera tra i due organi, assicurando la sinergia tra investigazione amministrativa e attività di polizia giudiziaria.

Bibliografia

Aprati, Roberta (2010): *La notizia di reato nella dinamica del procedimento penale* (Napoli, Jovene)

Azzarone, Raffaele (2014a): "Cyber vademecum (Parte I)", *Gnosis*, 1, pp. 62 – 76

Azzarone, Raffaele (2014b): "Cyber vademecum (Parte II)", Gnosis, 3, pp. 36 – 47

Azzarone, Raffaele (2014c): "Cyber vademecum (Parte III)", *Gnosis*, 4, pp. 34 – 46

Azzarone, Raffaele (2015a): "Cyber vademecum (Parte IV)", *Gnosis*, 2, pp. 88 – 98

Azzarone, Raffaele (2015b): "Cyber vademecum (Parte V)", *Gnosis*, 3, pp. 124 – 132

Azzarone, Raffaele (2015c): "Cyber vademecum (Parte VI)", Evoluzione della minaccia", *Gnosis*, 4, pp. 84 - 94

Barile, Paolo (1987): "Democrazia e segreto", *Quaderni costituzionali*, 1, pp. 29 - 50

Bifulco, Raffaele (2023): "voce Segreto e potere politico", in Cartabia, Marta e Ruotolo, Marco (editors): *Enc. dir., I tematici, V – Potere e Costituzione* (Milano, Giuffrè), p. 1096 - 1121

Bontempelli, Manfredi (2009): *L'accertamento amministrativo nel sistema processuale penale* (Milano, Giuffrè)

Bonzano, Carlo (2008): "La nuova tutela penale del segreto di Stato: profili sostanziali e processuali. Commento a l. 3 agosto 2007 n. 124", *Diritto penale e processo,* 1, pp. 24-35

Bonzano, Carlo (2010a): *Il Segreto di Stato nel processo penale* (Padova, Cedam)

Bonzano, Carlo (2010b): "La Consulta "suggerisce" una tutela oggettiva ed assoluta del segreto di Stato nel processo penale", *Diritto penale e processo*, 16, 3, pp. 301 - 314

Ferro (2015), p. 53 ss. e Murro (2023). Nell'ambito dell'aviazione civile, però, sono state messe a punto regole che valorizzano l'autonomia delle inchieste tecniche o di sicurezza sugli incidenti e l'impermeabilità della procedura giudiziaria rispetto agli esiti conoscitivi delle *safety investigations* (In argomento si rinvia a Di Bitonto (2017), p. 3804 ss.). Ad esempio, gli investigatori dell'ANSV possono accedere immediatamente e liberamente al luogo dell'incidente e, previa comunicazione al P.M., anche al luogo dove sono custodite le prove sottoposte a sequestro per esaminarle. Il previo accordo con il P.M. è previsto soltanto nell'ipotesi in cui debbano essere svolti accertamenti tecnici irripetibili e qualora la persona sottoposta alle indagini abbia fatto riserva di incidente probatorio: nel primo caso, il P.M. ha diritto di prendere parte all'atto e di concordare con l'ANSV le modalità tecniche dell'atto, devolvendo la risoluzione del conflitto al Presidente dell'ANSV e al Procuratore della Repubblica competente per le indagini. Niente di analogo, invece, pare essere previsto con riguardo alle investigazioni dell'Agenzia per la cybersicurezza.

[55] Secondo Salvi (2022), pp. 14-15, il problema della regolazione dei rapporti tra l'Agenzia cyber, il comparto di informazione per la sicurezza e l'autorità giudiziaria «*non può essere affrontato in termini di primazia dell'accertamento penale, come forse un tempo si sarebbe fatto*».

Bonzano, Carlo (2011): "voce Segreto di Stato (Dir. Proc. Pen.)", in Gaito, Alfredo (a cura di): *Digesto delle Discipline Penalistiche, Aggiornamento VI* (Torino, UTET), pp. 586 – 623

Bonzano, Carlo (2022): "Matière pénale e diritto al silenzio: la Consulta mette un punto fermo … o quasi", *Diritto penale e processo*, 28, 1, pp. 47 - 60

Bonzano, Carlo (2023): "Commento all'art. 270-bis c.p.p.", in Giarda, Angelo e Spangher, Giorgio (a cura di): *Codice di procedura penale commentato* (Milano, Wolters Kluver), pp. 3649 - 3654

Bonzano, Carlo (2023): "Commento all'art. 202 c.p.p.", in Giarda, Angelo e Spangher, Giorgio (editors): *Codice di procedura penale commentato I* (Milano, Wolters Kluver), pp. 2860 - 2874

Cadoppi, Alberto, Canestrari, Stefano, Manna, Adelmo e Papa, Michele eds (2019): *Trattato di Diritto penale. Cybercrime* (Torino, Giappichelli)

Caia, Giuseppe (2022): "voce Servizi di Informazione", in *Enc. dir., I tematici, III – Funzioni Amministrative* (Milano, Giuffrè), pp. 1037 – 1052

Caia, Giuseppe e Bresciani, Pier Francesco (2021): "Le istituzioni della sicurezza in Italia", in Panebianco, Angelo (editor): *Democrazia e sicurezza. Società occidentali e violenza collettiva* (Bologna, Il Mulino), pp. 319 - 355

Caligiuri, Mario (2021): *Intelligence e diritto. Il potere invisibile delle democrazie* (Soveria Mannelli, Rubbettino)

Caligiuri, Mario (2016): "Il dilemma della cyber intelligence", *Gnosis*, 2, pp. 22 – 29

Caneschi, Gaia (2020): "Nemo tenetur se detegere anche nei procedimenti amministrativi sanzionatori? La parola alla Corte di giustizia", *Cassazione penale*, 2, pp. 579 – 587

Carotti, Bruno (2020): "Sicurezza cibernetica e Stato-Nazione. Decreto legge 21 settembre 2019, n. 105, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133", *Giornale di diritto amministrativo*, 5, pp. 629 - 641

Cerruti, Alessandra (2013): "Delle condizioni soggettive dell'opposizione del segreto di Stato: vecchi problemi, nuovi bilanciamenti, medesimi limiti", *Giurisprudenza Italiana*, 1, pp. 35 – 42

Cesari, Claudia (1993): "Atti del procedimento amministrativo e processo penale tra limiti del codice e urgenze della prassi", C*assazione penale*, 1, pp. 143 - 145

Cesari, Claudia (2021): "L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite", *Revista Brasileira de Direito Processual Penal*, 3, pp. 1167 – 1187

Conso, Giovanni (1979): "Relazione di sintesi", in *Segreti e prova penale*, *Atti del Convegno di Studio Enrico De Nicola (Ferrara 1978)* (Giuffrè, Milano), pp. 195 - 211

De Gennaro, Gianni (2011): "Cultura della sicurezza e attuazione della riforma", *Gnosis,* 2, pp. 3 - 14

De Gennaro, Gianni (2018): "Intelligence, imprese private e nuove tecnologie digitali", in *I primi 20 anni: riflessioni sulla frontiera della conoscenza. Phronesis. Ventennale d'*intelligence, III, (Roma, Eurilink University press), pp. 83 - 94

Dell'anno, Pierpaolo (2020): "Le attività di intelligence", in Scalfati, Adolfo (editor): *Pre-invesitgazioni (espedienti e mezzi)* (Torino, Giappichelli), pp. 207 - 235

Di Bitonto, Maria Lucia (2006): "Raccolta di informazioni e attività di intelligence", in Kostoris, Roberto e Orlandi, Renzo (editors), *Contrasto al terrorismo interno e internazionale* (Torino, Giappichelli), pp. 253 – 264

Di Bitonto, Maria Lucia (2017): "Professione medica e procedimento penale: le novità dopo la legge n. 24/2017", *Cassazione penale*, 10, pp. 3799 - 3808

Ferro, Giovanni Battista, (2015): "L'inchiesta di sicurezza e l'inchiesta (rectius l'indagine) dell'autorità giudiziaria: una insopprimibile contradiction in adiecto?", in Franchi, Bruno e Vernizzi, Simone (editors): *Prevenzione degli incidenti aerei. La nuova normativa internazionale e dell'unione europea* (Torino, Giappichelli), pp. 53 - 60

Franchi, Bruno (2015): "Inchieste di sicurezza, indagini dell'Autorità giudiziaria: problematiche applicative del regolamento UE n. 996/2010", in Franchi, Bruno e Vernizzi, Simone (editors): *Prevenzione degli incidenti aerei. La nuova normativa internazionale e dell'unione europea* (Torino, Giappichelli), pp. 3 - 38

Fumu, Giacomo (1992): "Sub art. 220 disp. att. e coord.", in Chiavario, Mario (editor): *Commento al nuovo codice di procedura penale - la normativa complementare – II – Norme di coordinamento e transitorie* (Torino, Giappichelli) pp. 73 - 85

Furgiuele, Alfonso (2020): "Le investigazioni extrapenali di natura "mista"", in Scalfati, Adolfo (editor): *Pre-invesitgazioni (espedienti e mezzi)* (Torino, Giappichelli), pp. 141 - 162

Furin, Novelio (1999): "Diritto di difesa, indizi, sospetti e l'art. 220 disp. att. c.p.p.", *Cassazione penale,* 9, pp. 1634 – 1635

Galantini, Novella (2022): "La circolazione della prova nei rapporti tra procedimento tributario e procedimento penale", *Rivista italiana di diritto e procedura penale*, 3, pp. 999 - 1013

Galluccio Mezio, Gaetano (2023a): "Sub art. 220 disp. att. coord.", in Giarda, Angelo e Spangher, Giorgio (editors): *Codice di procedura penale commentato* (Milano, Wolters Kluver), pp. 3712 - 3717

Galluccio Mezio, Gaetano (2023b): "Sub art. 223 disp. att. coord.", in Giarda, Angelo e Spangher, Giorgio (editors): *Codice di procedura penale commentato* (Milano, Wolters Kluver), pp. 3725 - 3732

Gambacurta, Stefano (2008a): "I rapporti con altri soggetti", in Mosca, Carlo, Gambacurta, Stefano, Scandone, Giuseppe e Valentini, Marco (editors): *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)* (Milano, Giuffrè), pp. 281 - 338

Gambacurta, Stefano (2008b): "I rapporti con le Forze armate e le Forze di polizia", in Mosca, Carlo, Gambacurta, Stefano, Scandone, Giuseppe e Valentini, Marco (editors): *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)* (Milano, Giuffrè), pp. 304 - 323

Giupponi, Tommaso Filippo (2009): "Servizi di informazione e forze di polizia dopo la legge n. 124/2007", in *Astrid Online*, pp. 1 - 10

Giupponi, Tommaso Filippo (2010a): "Servizi di informazione e segreto di stato nella legge n. 124/2007", in Cariola, Agatino, Castorina, Emilio e Ciancio, Adriana (editors): *Studi in onore di Luigi Arcidiacono,* IV (Torino, Giappichelli), pp. 1677 - 1751

Giupponi, Tommaso Filippo (2010b): "La riforma del sistema di informazione per la sicurezza della Repubblica", in Illuminati, Giulio (editor): *Nuovi profili del segreto di Stato e dell'attività di intelligence* (Torino, Giappichelli), pp. 53 - 128

Giupponi, Tommaso Filippo (2017): voce *Segreto di Stato (dir. cost.)*, in *Enc. dir.*, Annali, X, 2 (Milano, Giuffrè), pp. 856 – 881

Giupponi, Tommaso Filippo (2023): "voce Sicurezza e potere", in Cartabia, Marta e Ruotolo, Marco (editors): *Enc. dir., I tematici, V – Potere e Costituzione* (Milano, Giuffrè), pp. 1149 - 1173

Gori, Ugo (2014): "Le nuove minacce cyber", *Informazioni della Difesa*, 6, pp. 5 – 29.

Gori, Ugo (2016): "Interesse nazionale, intelligence e strategie nell'era cibernetica", *Gnosis*, 2, pp. 86 – 93

Grevi, Vittorio (1978): "Segreto di Stato e processo penale. Evoluzione normativa e questioni ancora aperte", in Chiavario, Mario (editor): *Segreto di Stato e giustizia penale* (Zanichelli, Bologna) 1978, pp. 225 - 250

Grevi, Vittorio (2012): "Rapport sur le secret et la procédure en droit italien (1976)", in Giuliani, Livia (editor), *Scritti sul processo penale e sull'ordinamento penitenziario (1930)*, I, II (Padova, CEDAM), pp. 659 – 676

Jemolo, Arturo Carlo (1995): "Diritto d'informazione dello Stato (a proposito di una recente polemica)", *Per Aspera Ad Veritatem*, 1, disponibile su https://gnosis.aisi.gov.it/sito/Rivista1.nsf/ServNavig/2

Kostoris, Roberto E. (1964): *Il segreto come oggetto della tutela penale* (Padova, CEDAM)

Kostoris, Roberto E. (1990): "Sub art. 220 disp. att. e coord.", in Amodio, Ennio e Dominioni, Oreste (editors): *Commentario del nuovo codice di procedura penale. Appendice-Norme di coordinamento e transitorie* (Milano, Giuffrè) pp. 73 - 85

Maffettone, Sebastiano e Melidoro, Domenico (2015): "Democrazia e segreto", *Gnosis*, 3, pp. 12 - 19

Mazza, Oliviero (2000): "L'utilizzabilità processuale del verbale di constatazione redatto dalla Guardia di Finanza", *Corriete tributario*, 23, 18, pp. 1280 - 1287

Montagnese, Alfonso e Neri, Claudio (2016): *L'evoluzione della sicurezza nazionale in Italia*, in *sicurezzanazionale.gov*, disponibile su www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/02/evoluzione-sicurezza-nazionale-Montagnese-Neri.pdf, pp. 1 - 55

Morrone, Andrea (2010): "Il nomos del segreto di Stato", in Illuminati, Giulio (editor): *Nuovi profili del segreto di Stato e dell'attività di intelligence* (Torino, Giappichelli), p. 3 - 52

Mosca, Carlo (1985): "Segreto di Stato e attività dei Servizi di sicurezza", *Rassegna della giustizia militare*, pp. 189 - 209

Mosca, Carlo (2012): *La sicurezza come diritto di liberà. Teoria generale delle politiche della sicurezza* (Padova, Cedam)

Mosca, Carlo (2018): "Democrazia e sistema di intelligence negli ultimi quarant'anni. Profili normativi", in *I primi 20 anni: riflessioni sulla frontiera della conoscenza. Phronesis. Ventennale d'*intelligence, III (Roma, Eurilink University press), pp. 23 - 44

Mosca, Carlo (2018a): "Il sistema di informazione per la sicurezza della Repubblica e le garanzie funzionali", in Caligiuri, Mario e Valentini, Marco (editors): *Materiali di intelligence. Dieci anni di studi 2007-2017* (Soveria Mannelli, Rubbettino), pp. 115 - 133

Mosca, Carlo (2018b): *Democrazia e intelligence italiana. Dieci anni dopo tra cultura, diritto e nuove sfide della democrazia* (Napoli, Editoriale Scientifica)

Mosca, Carlo (2019): "Segreto – Trasparenza", *Gnosis,* 4, pp. 147 - 157

Mosca, Carlo, Gambacurta, Stefano, Scandone, Giuseppe e Valentini, Marco eds (2008), *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)* (Milano, Giuffrè)

Murro, Ottavia (2023): "Le inchieste dell'agenzia nazionale per la sicurezza del volo e i limiti all'attività della polizia giudiziaria", *Diritto penale contemporaneo – Rivista Trimestrale*, questo numero

Nobili, Massimo (1984): "Atti di polizia amministrativa utilizzabili nel processo penale e diritto di difesa: una pronuncia marcatamente innovativa", *Foro italiano*, 107, 2, pp. 375 - 379

Orlandi, Renzo (1992): *Atti e informazioni dell'Autorità amministrativa nel processo penale. Contributo allo studio delle prove precostituite* (Milano, Giuffrè)

Pace, Alessandro (2015): *Stato costituzionale e segreto di Stato: una coesistenza problematica*, in *Giurisprudenza costituzionale*, 60, 5, pp. 1719 – 1738

Paulesu, Pierpaolo (2023): "Sub art. 330 c.p.p.", in Giarda, Angelo e Spangher, Giorgio (editors): *Codice di procedura penale commentato* (Milano, Wolters Kluver), pp. 1509 – 1521

PISA, Paolo (1977): "Il segreto di Stato di fronte alla Corte costituzionale: luci ed ombre in attesa della riforma", *Giurisprudenza costituzionale*, 22, 1, pp. 1206 – 1214

Pizzetti, Francesco (1978): "Principi costituzionali e segreto di Stato", in Chiavario, Mario (editor), *Segreto di Stato e giustizia penale* (Zanichelli, Bologna), pp. 91 - 111

Presidenza del Consiglio dei Ministri (2013): *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, disponibile su www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf

Rampioni, Matteo (2019): "Le c.d. indagini "anfibie": linee di fondo sul controverso legame tra attività ispettive e processo penale", *Processo penale e giustizia*, 1, pp. 232 - 248

Renzi, Andrea (2021): "La sicurezza cibernetica: lo stato dell'arte", *Giornale di diritto amministrativo*, 4, pp. 538 – 548

Ricotta, Federico Niccolò (2023a): "Il segreto di Stato", in Colaiacovo, Guido (editor): *Sicurezza, Informazioni e Giustizia penale* (Pisa, Pacini Giuridica), in corso di pubblicazione

Ricotta, Federico Niccolò (2023b): "Il segreto di Stato nel processo penale", in Colaiacovo, Guido (editor): *Sicurezza, Informazioni e Giustizia penale* (Pisa, Pacini Giuridica), in corso di pubblicazione

Rivello, Pierpaolo (2023a): "Sub Art. 256-bis c.p.p.", in Giarda, Angelo e Spangher, Giorgio (editors): *Codice di procedura penale commentato* (Milano, Wolters Kluver), pp. 3381 – 3383

Rivello, Pierpaolo (2023b): "Sub Art. 256-ter c.p.p.", in Giarda, Angelo e Spangher, Giorgio (editors): *Codice di procedura penale commentato* (Milano, Wolters Kluver), pp. 3383 - 3385

Salvi, Giovanni (2022), "Attuazione della giurisdizione penale nello spazio virtuale e sicurezza nazionale", *Sistema penale*, pp. 1 - 16

Salvi, Giovanni (2023): "Potere e intelligence", in Cartabia, Marta e Ruotolo, Marco (editors): *Enc. dir., I tematici, V – Potere e Costituzione* (Milano, Giuffrè), pp. 248 - 279

Scalfati, Adolfo (2020): "Il fermento pre-investigativo", in Scalfati, Adolfo (editor): *Pre-invesitgazioni (espedienti e mezzi)* (Torino, Giappichelli), pp. 1 – 10.

Scandone, Giuseppe (2008): *Il segreto di Stato nella legge di riforma*, in Mosca, Carlo, Gambacurta, Stefano, Scandone, Giuseppe e Valentini, Marco (editors), *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)* (Milano, Giuffrè), pp. 499 - 558

Sforza, Ilaria (2022): "Il nemo tenetur se detegere nelle audizioni Consob e Banca d'Italia: uno statuto ancora da costruire", *Sistema penale*, 2, pp. 83 - 104

Sorbello, Pietro (2016): "La valutazione di sospetti, indizi e notizie di reato nel passaggio (incerto) dalle attività ispettive alle funzioni di polizia giudiziaria", *Diritto penale contemporaneo*, 2, pp. 125 - 135

Spangher, Giorgio (1990): "Sub *art. 202 c.p.p.*", in Chiavario, Mario (editor), *Commento al codice di procedura penale* (Torino, UTET), pp. 469 – 474

Ubertis, Giulio (1992): "L'utilizzazione dibattimentale di prelievi e analisi di campioni", *Cassazione penale*, 2, pp. 289 - 290

Ubertis, Giulio (1995): "voce Prova in generale", in *Dig. disc. pen.*, Vol. X (Torino, UTET), pp. 296 - 338

Valentini, Marco (2008): *L'ordinamento del sistema politico dell'informazione per la sicurezza*, in Mosca, Carlo, Gambacurta, Stefano, Scandone, Giuseppe e Valentini, Marco (editors), *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)* (Milano, Giuffrè), pp. 23 - 93

Le indagini d'*intelligence* e gli strumenti d'intercettazione preventiva

Investigaciones de inteligencia y herramientas de interceptación preventiva

Intelligence Investigations and Preventive Interception Tools

Wanda Nocerino
Ricercatrice di Diritto processuale penale - Università di Foggia
wanda.nocerino@unifg.it

Indagini preliminari, Intercettazioni, Regole probatorie

Investigaciones preliminares, Interceptación de comunicaciones, Reglas de la prueba

Pre-Trial Investigation, Intrusive surveillance, Rules of evidence

Abstracts

Nel rinnovato contesto criminogeno, le intercettazioni rappresentano lo strumento di indagine più utilizzato dagli investigatori, tanto in fase processuale che in quella preventiva. Se le captazioni giudiziarie sono funzionali all'accertamento del fatto, quelle *ante delictum* sono dirette all'acquisizione di informazioni per neutralizzare reati di particolare allarme sociale, senza trovare impiego nel procedimento penale. Tuttavia, come spesso accade, la prassi non è conforme a quanto teorizzato dal legislatore: allo stato dell'arte, i risultati delle intercettazioni preventive trovano un impiego "indiretto" nel processo, agevolando una circolazione atipica di informazioni che si ripercuote sugli esiti investigativi e dibattimentali. L'autore, dopo essersi soffermato sulle criticità di ordine "processuale" – acuite dalla recente riforma che ha investito le intercettazioni preventive d'intelligence –, analizza le implicazioni sistematiche derivanti dalla compresenza di poteri investigativi paralleli.

Las interceptaciones de comunicaciones son la herramienta de investigación más utilizada por los investigadores, tanto en los procedimientos sancionatorios como en aquellos de prevención. Si las primeras son funcionales a la constatación de un hecho determinado, las interceptaciones preventivas tienen por objeto adquirir información para neutralizar delitos de especial alarma social, no encontrando utilidad en un proceso penal. Sin embargo, como suele ocurrir, la práctica no se ajusta a lo teorizado por el legislador: los resultados de las interceptaciones preventivas encuentran un uso "indirecto" en los procesos judiciales, facilitando una circulación atípica de información que afecta los resultados investigativos. El autor, luego de analizar las cuestiones críticas "procesales", aborda las implicancias sistemáticas derivadas de la coexistencia de facultades investigativas paralelas.

Interceptions are the investigation tools most used by investigators, both in the trial and in the preventive phase. Preventive interceptions are aimed at acquiring information to neutralize serious crimes, without finding use in criminal proceedings. However, as often happens, the practice does not comply with what the legislator theorized: in fact, the results of preventive interceptions find an "indirect" use in the process, facilitating an atypical circulation of information which affects the investigative outcomes and debate. The author, after focusing on the "procedural" critical issues, analyzes the systematic implications deriving from the coexistence of parallel investigative powers.

Sommario

1. 1. prevenzione e il pericolo dei poteri investigativi paralleli.

A fronte della rinnovata fisionomia delle fattispecie criminali – sempre più proiettate alla dimensione cybernetica e transnazionale[1] –, le intercettazioni di conversazioni e comunicazioni rappresentano lo strumento di indagine più utilizzato dagli investigatori. Gli ultimi dati statistici disponibili dimostrano come, nel 2021, i soggetti sottoposti a captazioni sono pari a 70 mila, per un totale di 150.000 intercettazioni autorizzate nell'anno di riferimento[2].

Se questo è il panorama che si prospetta una volta iniziato il procedimento penale, il quadro diventa ancor più allarmante allorquando si volge lo sguardo alla fase preventiva. Da uno studio internazionale emerge, infatti, come l'istituto delle intercettazioni e dei controlli preventivi sulle comunicazioni abbia assunto un ruolo centrale (se non addirittura routinario) nell'attività investigativa giornaliera delle procure italiane[3].

Prima facie, si potrebbe ritenere tale dato poco rilevante ai fini processuali, nella convinzione per cui le investigazioni preventive possano solo "tangere" il procedimento penale, senza incidervi in maniera significativa a fronte della scelta del legislatore di negare ogni accesso – in termini di utilizzabilità – ai risultati acquisiti mediante le indagini proattive nel rito probatorio.

Allo stato, però, vuoi per la trasfigurazione in chiave preventiva del sistema penale, vuoi per lo sfrenato ricorso a strumenti tecnologici che facilitano l'interazione tra pre-procedimento e processo[4], le barriere frapposte tra le investigazioni *ante* e *post delictum* risultano sempre più cedevoli. Va da sé che le implicazioni processuali, un tempo "di confine", perdono la loro originaria dimensione e le problematicità rispetto a norme, principi, garanzie individuali e di accertamento, si irrobustiscono e complicano[5].

Ma, prima ancora di affrontare tali criticità, pare doverosa una riflessione più generale, inerente al rinnovato contesto nel quale il moderno investigatore muove i suoi passi.

Come noto, l'ordinamento processuale sta mutando i suoi connotati essenziali attraverso un'espansione dell'attività di indagine alla fase prodromica al compimento del reato. In effetti, «[P]pensare ad un procedimento penale che si instaura con l'acquisizione della *notitia criminis* è immagine alquanto anacronistica e sicuramente poco aderente alla realtà»[6]: pur non negando che tradizionalmente l'inizio dell'*iter* procedimentale è determinato dall'iscrizione della notizia di reato nell'apposito registro, non è possibile sottacere tutta l'attività preventiva e di ricerca della stessa che, inevitabilmente, indirizza le investigazioni "per" procedere alla sua formazione.

[1] La rivoluzione informatica e tecnologica sta progressivamente determinando un mutamento ontologico delle fattispecie di reato: se, per un verso, la criminalità informatica assume sempre più spesso i connotati della transnazionalità, per l'altro, muta le sue caratteristiche tradizionali per manifestarsi interamente sulla rete (c.d. *cybercrime*) ovvero per il tramite della rete (c.d. *computer crime*). In questo senso Luparia Donati (2009), pp. 475-477.

[2] Dati consultabili su *www.giustizia.it*. Secondo il *Bilancio Sociale 2020-2021*, elaborato dall'Università degli Studi di Napoli "Federico II" di concerto con la procura della Repubblica presso il Tribunale di Napoli, nell'anno 2020 sono state 2.891 le richieste autorizzative che sono arrivate a 4.672 nel 2021. Per le intercettazioni sono stati spesi 11.811.411,09 nel 2020 e 12.785.338,67 nel 2021. Il dato diventa ancor più sorprendente se si considerano i numeri degli altri Paesi europei. Si pensi che in Francia le captazioni autorizzate sono pari a 37.000, mentre in Inghilterra solo 3.800. Non a caso, l'ultima manovra di bilancio (l. 29 dicembre 2022, n. 197), presenta una riduzione delle spese di giustizia per le intercettazioni di 1.575.136 euro annui, a decorrere dal 2023 (art. 880, l. 197/2022).

[3] Secondo uno studio condotto nel 2018 (l'ultimo disponibile in materia di investigazioni preventive), gli strumenti di indagine proattiva più utilizzati in Europa sono le intercettazioni preventive. Cfr. European Union Agency for Fundamental Rights (2018), pp. 1 ss.

[4] Solo a titolo esplicativo, si pensi al captatore informatico o all'*IMSI Catcher,* ossia strumenti ad alto potenziale tecnologico, impiegati tanto in fase preventive che in fase procedimentale, acuendo il rischio di uno sconfinamento processuale dei dati acquisiti *ante delictum*. Più in generale, sull'impatto probatorio derivante dall'uso di tali strumenti, volendo, Nocerino (2021a), pp. 1077-1088.

[5] In questo senso Curtotti (2018), pp. 438-439.

[6] Testualmente Giunchedi (2008), p. 3.

Inevitabile, a questo punto, appare la riqualificazione del concetto di "investigazione", non più solamente intesa come conseguente alla verifica del compimento del fatto tipico e antigiuridico, ma come un'attività condotta anche al di fuori del processo penale e per esigenze diverse da quelle inerenti alla ricostruzione dell'evento criminoso. L'investigatore diventa un soggetto deputato alla ricerca di una verità diversamente concepita, tesa *in primis*, alla raccolta e all'analisi delle notizie apprese attraverso l'attività di sorveglianza sulle comunicazioni e sugli scambi di dati tra gli individui (c.d. attività di acquisizione informativa), per poi confluire nell'elaborazione di strategie di neutralizzazione dell'offesa (c.d. investigazione proattiva in senso stretto).

In questo quadro magmatico, gli equilibri di potere tra i protagonisti delle tradizionali indagini preliminari risultano alterati, ingenerando una confusione di ruoli assai pericolosa: sono gli investigatori (sia Forze di polizia che Servizi d'*intelligence*) a "guidare" le indagini e ad orientare il procedimento penale detenendo il monopolio strategico della mole di informazioni raccolte in autonomia e con largo anticipo rispetto all'intervento dell'autorità giudiziaria.

Ciò non senza conseguenze sull'assetto processuale. La sinergia tra prevenzione e repressione comporta, infatti, il rischio di una convergenza tra organi le cui funzioni sono tradizionalmente separate. Così, l'attività di *intelligence* di raccolta ed elaborazione dei dati acquisiti ai fini di sicurezza diviene ambivalente e, sempre più spesso, attribuita agli organi requirenti (p.m. e p.g.) e, viceversa, le Agenzie di sicurezza si trovano a svolgere attività investigativa che, almeno da un punto di vista teorico, dovrebbe risultare estranea alle stesse.

Va, quindi, preso atto dell'esistenza di "nuovo" genere di prevenzione, in cui i confini tra pre-procedimento e indagini sono assai più labili, quasi svaniti ed evanescenti, ricchi di punti di contatto e di scambio.

In un contesto come quello descritto, l'intervento del giurista appare doveroso oltre che necessario; ciò non solo in ragione della pericolosità che la creazione di poteri investigativi paralleli genera sul procedimento penale ma anche in vista delle sue inevitabili ripercussioni sul complesso di regole e principi che sorreggono l'assetto costituito. Se al legislatore viene richiesto un intervento chiarificatore in materia, la comunità scientifica è chiamata ad evidenziare le criticità del sistema, proponendosi di riportare negli argini delle regole le deviazioni cui assiste, tenendo ben a mente che la contingenza impone un riordino e un rinnovo delle tradizionali categorie esistenti in ragione di un inevitabile mutamento storico, politico e sociale con cui il giurista è chiamato a fare i conti.

2. Dalle intercettazioni "processuali" alle intercettazioni preventive. Similitudini e differenze.

Prima ancora di soffermarsi sulle criticità derivanti dal rischio dei poteri investigativi paralleli, occorre partire dalla comparazione tra l'istituto delle intercettazioni *ante delictum* e l'analoga figura esperibile in fase procedimentale, evidenziandone le similitudini e rimarcandone le considerevoli differenze al fine di evitare erronee commistioni e comprendere la portata della pericolosità dell'ingiustificato travisamento.

Come noto, all'interno del codice di rito non è contenuta alcuna definizione di "intercettazione" e questo vale tanto per quelle disposte nel corso del procedimento penale[7] quanto per quelle preventive[8], ma la lacuna viene colmata in modo pressoché differente.

Se per le intercettazioni di cui agli artt. 266 ss. c.p.p. è la giurisprudenza di legittimità a chiarirne il significato e la portata[9], per quelle preventive il cammino è assai più lungo e tortuoso. A ben guardare, infatti, nessun intervento legislativo o giurisprudenziale contribuisce a delineare un assetto generalmente condiviso, tale da evitare arbìtri interpretativi in ordine all'*an* e al *quantum* necessario per includere quest'attività nel *genus* delle captazioni *ante* o

[7] Sull'istituto delle intercettazioni processuali la dottrina è sterminata. Senza pretese di completezza, cfr. Filippi (2002a), p. 565; Marinelli (2007), p. 3.

[8] Per quanto concerne le intercettazioni preventive, Agostini (2017), pp. 141-148; Andolina (2016), pp. 568-572; Cantone e D'Angelo (2006), pp. 54-66; Filippi e Cortesi (2004), pp. 1-11; Garuti (2005), p. 1457-1461; Nocerino (2019), pp. 6-72.

[9] Come chiarito da Cass., sez un., 28 maggio 2003, n. 36747, in *Guida dir.*, 2003, p. 42, le intercettazioni consistono «nella captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere gli altri e con modalità oggettivamente idonee allo scopo, attuata da un soggetto estraneo alla stessa mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del suo carattere riservato».

praeter delictum.

Allo stato dell'arte, le intercettazioni preventive sono attività tecniche eseguite per esclusive finalità investigative ed assolutamente inutilizzabili nel procedimento penale, ovvero come «un'attività di iniziativa delle Forze di polizia [nonché dei Servizi d'*intelligence*] diretta a raccogliere informazioni utili per la prevenzione di gravi reati e non per l'acquisizione di elementi finalizzati all'accertamento della responsabilità per singoli fatti delittuosi»[10].

In sostanza, come precisa la dottrina, esse rappresentano captazioni di conversazioni o comunicazioni (telefoniche, ambientali, domiciliari o telematiche) e attività di monitoraggio sulle comunicazioni, espletabili anche in assenza di un procedimento penale, «a prescindere dall'esistenza di una *notitia criminis* e dall'obiettivo di raccogliere prove utilizzabili in giudizio»[11].

Dalla definizione fornita emerge che la dottrina – a differenza di quanto accade per le intercettazioni "tradizionali" in cui l'attenzione si è concentrata sull'oggetto e sui tratti tipici dell'attività captativa – si dedica unicamente a chiarire la finalità investigativa pre–procedimentale dell'istituto, senza soffermarsi sugli elementi caratterizzanti il peculiare strumento.

Si è detto[12] che qualunque indicazione in tal senso appare superflua in ragione del fatto che le intercettazioni preventive rappresentano solo una *species* di quelle tradizionali, differenziandosi da queste ultime solo in relazione al regime giuridico e non in ragione delle caratteristiche generali, comuni ai due istituti.

In effetti, proprio come per quelle processuali, anche per le preventive sono richieste alcune caratteristiche inequivocabili dell'atto intercettivo per poter annoverare una mera ricezione di dati e informazioni nel concetto ben più ampio e articolato di "intercettazione", in quanto non ogni forma di captazione di dialoghi o conversazioni rientra nel *genus* in esame.

Perché ciò si verifichi devono sussistere i seguenti requisiti: innanzitutto, occorre che i soggetti comunichino tra loro con il preciso intento di escludere gli altri dal contenuto della comunicazione e in modo tale da tenere quest'ultima segreta; in secondo luogo, è necessario l'uso di strumenti tecnici di percezione particolarmente invasivi e tali da superare le cautele elementari che dovrebbero garantire la libertà e la segretezza del colloquio ed a captarne i contenuti; infine, il soggetto captante deve essere assolutamente estraneo al colloquio, violando – in modo "clandestino" – la segretezza della conversazione.

Al di là delle caratteristiche comuni, quelle preventive presentano requisiti propri ed elementi peculiari che le rendono «nient'affatto assimilabili»[13] a quelle esperibili nel corso del procedimento penale.

Le intercettazioni tradizionali sono mezzi di ricerca della prova idonei ad offrire al giudice elementi indispensabili a formare il suo convincimento. Sono esperibili solo una volta iniziato il procedimento penale – ovvero dopo che la *notitia criminis* viene iscritta nell'apposito registro, durante il primo segmento dell'arco procedimentale allorquando vengono raccolti elementi probatori idonei a formulare un giudizio prognostico sulla fondatezza dell'accusa – in presenza di «un minimo *fumus commissi delicti*»[14].

La collocazione spazio-temporale delle captazioni *de quibus*, protagoniste indiscusse della fase investigativa, consente di denominarle, anche nell'ottica di un'immediata differenziazione rispetto a quelle preventive, intercettazioni "processuali" o "giudiziarie".

Viceversa, quelle preventive (o pre-procedimentali), sono mezzi di ricerca – non di una prova – ma di un indizio, o, meglio, di elementi investigativi idonei a giustificare il compimento di ulteriori attività investigative atipiche per formare la notizia di reato. Svolgendosi in una fase *pre* (o *extra*)-procedimentale, sono funzionali all'eventuale instaurazione del rito penale ma non vengono ricomprese nello stesso, vigendo il divieto di utilizzabilità dei risultati appresi in sede di profilassi nel processo vero e proprio.

In secondo luogo, il perimetro di operatività di quelle preventive è assai più variegato ri-

[10] Cantone e D'Angelo (2006), p. 54. Altri le definiscono come «le interferenze nella segretezza delle comunicazioni la cui finalità non è quella di costituire un mezzo di ricerca della prova nell'ambito di un procedimento penale, ma di agevolare l'attività di prevenzione dei reati». Così Di Bitonto (2012), p. 1196.

[11] Si esprime così Illuminati (1983), p. 171.

[12] Cercola (2016), p. 460, parla di «regime "differenziato" delle intercettazioni preventive».

[13] La necessità di tracciare una netta linea di demarcazione tra i due istituti è avvertita anche dalla Consulta. Cfr. C. cost., 29 dicembre 2004, n. 443, in *Giur. cost*., 2004, p. 4659, secondo cui non è possibile alcun confronto tra la disciplina delle intercettazioni con quella relativa alle intercettazioni preventive, le quali non tendono ad accertare ipotesi criminose ma a prevenire la commissione di reati, caratterizzandosi per una disciplina distinta e da un livello di garanzie complessivamente inferiore rispetto a quelle ordinarie.

[14] Si esprime così Marandola (2001), p. 113.

spetto a quello delle captazioni giudiziarie.

A differenza di queste ultime, il cui fine è solo limitato all'apprensione di flussi di conversazioni e comunicazioni espletabile attraverso le differenti tipologie di intercettazioni telefoniche, ambientali (e domiciliari) e telematiche, quelle preventive contemplano svariate attività che non rientrano nel concetto di intercettazione *stricto senso* intesa, ma in quello più generale di "controllo": non è, infatti, un caso che la rubrica dell'art. 226 disp. att. c.p.p. contempli sia le intercettazioni che i controlli preventivi sulle comunicazioni.

Le "altre" operazioni esperibili sono previste dal comma 4 dell'art. 226 disp. att. c.p.p., con riferimento alle intercettazioni preventive di polizia, e dal comma 4 del neointrodotto art. 4-*bis*, d.l. 144/2005[15], per quelle d'*intelligence*, consentendo «il tracciamento delle comunicazioni telefoniche e telematiche, nonché l'acquisizione di dati esterni relativi alle comunicazioni telefoniche e telematiche intercorse e di ogni altra informazione utile in possesso degli operatori di telecomunicazioni».

Dal disposto normativo emerge che la nozione di intercettazione preventiva non è poi così aderente rispetto al ventaglio di alternative investigative esperibili attraverso questo duttile strumento: per poter correttamente definire l'istituto in esame, il baricentro deve spostarsi dal concetto di "intercettazione" a quello di "controllo".

Così facendo, le captazioni *ante delictum* finiscono per rappresentare il mezzo idoneo ad acquisire, non solo flussi di conversazioni o comunicazioni, ma dati e informazioni di qualunque genere[16].

Ancora, in relazione al regime giuridico, le due forme di captazione non sono assolutamente equiparabili: differenti risultano i "casi" di intercettazione[17], le attività esperibili[18], i presupposti per procedere all'esecuzione delle operazioni[19], l'*iter* autorizzativo[20] e i termini di durata[21].

Tutt'al più, potrebbero trovare punti di contatto con le intercettazioni disposte in relazione ai reati più gravi per cui vige il c.d. "doppio binario investigativo"[22]. Ne condividono il presupposto della necessarietà investigativa (art. 13, comma 1, l. 203/1991); il termine di durata e le relative proroghe (art. 13, comma 2, l. 203/1991), nonché le deroghe relative alle intercettazioni nel domicilio, ammissibili anche in assenza del «fondato motivo di ritenere che *ivi* si stia svolgendo un'attività criminosa» (art. 3-*bis*, l. 356/1992).

Nonostante gli elementi comuni, – lo si ribadisce – le intercettazioni "straordinarie" comunque rimangono captazioni di natura procedimentale esperibili solo e quando emergono

[15] *Ex* art. 1, comma 684, l. 197/2022. Cfr. § 3.

[16] Quasi come se la legale definizione di intercettazione preventiva fosse superflua dovendo essere ricompresa nel più ampio concetto di "controllo".

[17] Nelle intercettazioni tradizionali il catalogo di reati sembra assai ampio e variegato, potendosi esperire captazioni processuali per tutte le fattispecie di cui all'art. 266, comma 1, c.p.p. ovvero, nel caso di intercettazioni di comunicazioni informatiche o telematiche di cui all'art. 266-*bis* c.p.p., anche per i reati commessi mediante l'impiego di tecnologie informatiche o telematiche. Viceversa, le intercettazioni preventive sono ammesse solo per i reati di cui agli artt. 407, comma 2, lett. *a* e 51, commi 3-*bis* e 3-*quater*, c.p.p., rappresentando una categoria assai più "ristretta". Per quelle d'*intelligence,* ai sensi dell'art. 4, d.l. 144/2005, le captazioni sono autorizzate per l'espletamento delle attività loro demandate dagli artt. 6 e 7 della legge 3 agosto 2007, n. 124, ossia ricerca ed elaborazione delle informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica dalle minacce provenienti dall'estero nonché la sicurezza interna della Repubblica e le istituzioni democratiche.

[18] Come evidenziato, mentre le intercettazioni tradizionali consistono nella captazione di flussi di conversazioni e comunicazioni anche telematiche, quelle preventive ineriscono ad un'attività ben più ampia che si concretizza nel controllo dei soggetti sottoposti.

[19] Ai sensi dell'art. 267 c.p.p., le intercettazioni giudiziarie vengono autorizzate solo se risultano «assolutamente indispensabili ai fini della prosecuzione delle indagini», qualora sussistano «gravi indizi di reato». I requisiti si attenuano nel caso di preventive, bastando la necessità dell'attività «per l'acquisizione di notizie concernenti la prevenzione» se sussistono «elementi investigativi che giustificano l'attività di prevenzione». Per quelle d'*intelligence,* come meglio si dirà (su cui vedi *infra,* § 3), anche dopo la riforma operata con l. 197/2022, i requisiti risultano meno stringenti, potendosi autorizzare nel caso ritenute indispensabili per l'espletamento delle attività loro demandate dagli artt. 6 e 7, l. 3 agosto 2007, n. 124.

[20] Nelle intercettazioni processuali l'autorizzazione è fornita dal g.i.p., il quale decide sulla richiesta del p.m. con decreto motivato. Nei casi d'urgenza, quando «vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini», il p.m. dispone l'intercettazione con decreto motivato che va comunicato immediatamente al g.i.p. il quale, entro quarantotto ore, decide sulla convalida con decreto motivato. Al contrario, come meglio si specificherà nel prosieguo (cfr. § 2.1), nel caso di intercettazioni preventive nessun controllo viene operato dall'autorità giudiziaria, venendo disposte dal procuratore della Repubblica presso il capoluogo del distretto in cui si trova il soggetto da sottoporre a controllo ovvero, nel caso in cui non sia *a priori* determinabile, del distretto in cui sono emerse le esigenze che legittimano le captazioni, ovvero, nel caso di intercettazioni preventive d'*intelligence*, il procuratore generale presso la Corte d'appello di Roma.

[21] Ai sensi dell'art. 267, comma 3, c.p.p., la durata delle intercettazioni processuali «non può superare i quindici giorni, prorogabili per periodi successivi di quindici». La durata massima delle intercettazioni preventive (sia di polizia, a norma dell'art. 226, comma 2, disp. att. c.p.p., sia di *intelligence, ex* art. 4-*bis,* d.l. 144/2005) è, invece, commisurata in quaranta giorni, prorogabili per periodi successivi di venti.

[22] Cfr. art. 13, d.l. 13 maggio 1991, n. 152, conv. in l. 12 luglio 1991, n. 203 e successivamente modificato dall'art. 3-*bis* del d.l. 9 giugno 1992, n. 133, conv. in l. 7 agosto 1992, n. 356.

sufficienti indizi di reato.

2.1. Segue: *le tipologie di captazioni pre-procedimentali.*

Altro aspetto caratterizzante le intercettazioni preventive è la poliedricità delle tipologie di captazioni esperibili, le quali differiscono, oltre che per lo scopo cui sono preposte, anche in rapporto ai soggetti legittimati a procedere[23].

Preliminarmente, può dirsi che le tre forme di intercettazione *ante delictum* seguano un "*climax* ascendente" in ordine all'ampiezza del rispettivo perimetro operativo, quasi come se il legislatore avesse inteso ampliarne gradualmente la "portata" a fronte degli indiscussi vantaggi investigativi che derivano dalla loro esecuzione: al rigore iniziale che ne imponeva un uso limitato solo per la neutralizzazione dei più efferati reati in ragione dell'indiscussa compressione delle più basiche libertà fondamentali, si contrappone il "lassismo" del legislatore che estende l'ambito applicativo dell'istituto fino ad utilizzarlo come strumento per controllare soggetti ritenuti pericolosi.

Più in particolare, la prima *species* di captazioni *ante delictum*, è rappresentata dalle intercettazioni preventive di "polizia", di cui all'art. 226 disp. att. c.p.p., finalizzate alla prevenzione dei reati gravi di terrorismo e criminalità organizzata ed eseguibili solo allorquando emergono «elementi investigativi che giustifichino l'attività di prevenzione» e risultino «necessarie» alla neutralizzazione del *periculum* rilevato.

Accanto a queste, il legislatore del 2005 colloca una forma inedita di intercettazioni preventive con cui si legittimano i Servizi d'*intelligence* ad eseguire captazioni *ante delictum* allorquando risultino «indispensabili per l'espletamento delle attività demandate ai direttori dei servizi di informazione per la sicurezza dagli artt. 6 e 7, l. 124/2007» (art. 4, d.l. 144/2005, come sostituito dal comma 1 dell'art. 12, l. 133/2012), ossia per l'esecuzione di tutte le funzioni tipiche dell'AISE e dell'AISI dirette all'assunzione di ogni informazione utile alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica.

Da ultimo, nel 2011 la complessa normazione in tema di intercettazioni preventive viene ulteriormente implementata attraverso la previsione di una speciale forma di captazione *ante delictum*, deputata alla neutralizzazione del pericolo di reiterazione di attività o comportamenti criminosi, qualora ciò risulti «necessario al fine di controllare i soggetti nei cui confronti sia stata applicata una delle misure di prevenzione personale» (art. 78 del Codice antimafia).

Si tratta di una *species* di captazione "ibrida", per cui si riscontrano elementi comuni sia alle intercettazioni preventive che a quelle giudiziarie. Più nel dettaglio, in relazione ai "tempi" dell'esecuzione delle operazioni – eseguite *ante* o *praeter delictum* – e ai "risultati" delle informazioni apprese – non utilizzabili per fini processuali – sono riconducibili alla disciplina di cui all'art. 226 disp. att. c.p.p.; circa le modalità operative, invece, richiamano la disciplina di cui all'art. 268 c.p.p. e, conseguentemente, risultano assimilabili alle intercettazioni procedimentali[24].

Il rapido *excursus* sulle tipologie di intercettazioni preventive esistenti nel panorama giuridico vigente stimola l'interprete ad un'ulteriore riflessione. Come meglio si dirà nel prosieguo[25], il pluralismo di "fonti disciplinari" non solo genera una confusione di ruoli e funzioni in merito alla legittimazione a procedere (Forze di polizia e Servizi di *intelligence*) – acuendo, così, i pericoli generato dalla coesistenza di poteri investigativi paralleli – ma innalza anche esponenzialmente il rischio di circolazione atipica delle informazioni preventive nell'ambito del procedimento penale.

[23] Per una disamina della normativa in rapporto alle singole *species* di intercettazioni preventive, si consenta un rinvio a Nocerino (2019), p. 96.
[24] Per chiarezza espositiva, si precisa che nel prosieguo non si procederà ad analizzare in via autonoma la disciplina delle intercettazioni preventive antimafia, per cui, al di là della peculiarità legate ai destinatari delle stesse, non si riscontrano criticità proprie di questa forma intercettiva: in ragione della loro natura amorfa, si ritengono estendibili le considerazioni che verranno di seguito svolte in relazione alle intercettazioni preventive di polizia.
[25] Cfr. § 4.

3. La nuova disciplina delle intercettazioni preventive d'*intelligence*.

Conviene trattate separatamente la normativa delle intercettazioni preventive d'*intelligence* che, come noto, è stata oggetto di una recente riforma operata nell'ambito della complessa manovra finanziaria per il triennio 2023-2025[26].

Si cominci col dire che il legislatore non intende tradire l'ideologia che aveva animato la riforma del 2005[27] che, anziché puntare ad un'integrazione della disciplina prevista per le intercettazioni preventive di polizia, scelse di introdurre una nuova forma di intercettazione preventiva ad appannaggio esclusivo dei Servizi di informazione per la sicurezza della Repubblica. Di novità quella novella, rispetto alle captazioni di polizia, prevedeva solo diversi protagonisti[28] e diversi presupposti applicativi[29], mentre, per quanto concerne il *modus operandi*, faceva un mero rinvio alle previsioni contenute nei commi 2, 3, 4 e 5 dell'art. 226 disp. att. c.p.p. Intendiamo dire, insomma, che la riforma del 2005 ha provveduto a tipizzare una nuova *species* di captazione *ante delictum* solo formalmente, posto che la disciplina risulta identica a quella prevista per le intercettazioni preventive di polizia.

Con la recente modifica, il legislatore fa un passo ulteriore: superando la fallimentare tecnica del rinvio, sancisce la definitiva autonomia dell'istituto delle intercettazioni preventive d'*intelligence* che, quindi, finisce per trovare una integrale regolamentazione negli artt. 4 e 4-*bis,* d.l. 144/2005. Il che le dà una identità politica ed operativa di spessore, di cui non si può non tenere conto.

Per contro, ad una rivitalizzazione d'immagine non segue una trasformazione di contenuto. La disciplina non subisce modifiche particolarmente incisive: la riforma, in alcuni casi, si limita a riprodurre il contenuto pressoché integrale dell'art. 226 disp. att. c.p.p., in altri procede a minimi ritocchi linguistici e/o sistematici che – sì – migliorano l'istituto ma – di certo – non ne alterano la struttura.

Ciò consente di affermare, con una certa convinzione, che la nuova normativa in tema di intercettazioni preventive d'*intelligence* rimane pressoché invariata rispetto al passato, salvo alcune innovazioni formali che contribuiscono a conferire maggiore coerenza al dato normativo.

La prima novità riguarda il contenuto dell'art. 4, comma 1, d.l. 144/2005: se, in passato, la normativa operava un mero richiamo alle previsioni di cui al comma 1 dell'art. 226 disp. att. c.p.p., la novella individua la tipologia di attività rientranti nelle operazioni intercettive esperibili dai Servizi d'*intelligence:* «l'intercettazione di comunicazioni o conversazioni, anche per via telematica, nonché l'intercettazione di comunicazioni o conversazioni tra presenti, anche se queste avvengono nei luoghi indicati dall'art. 614 c.p.».

Non si è ampliato l'ambito operativo delle intercettazioni preventive, né attribuiti maggiori poteri al comparto d'*intelligence:* il richiamo analitico alle singole *species* di captazioni esperibili è solo una modifica "estetica", limitandosi a "palesare" le singole operazioni che (da sempre) possono compiere gli uomini d'*intelligence.* Dunque, nessun cambiamento significativo.

Maggiori riflessioni meritano i presupposti legittimanti il decreto autorizzativo del procuratore generale presso la Corte di appello di Roma, ossia che le intercettazioni risultino indispensabili alle attività dei Servizi (quelle di cui agli artt. 6 e 7, l. 3 agosto 2007, n. 124)[30].

Nel *Dossier* del Servizio Studi del Senato, si legge: «[N]ella disciplina vigente […], il procuratore generale adotta il decreto [autorizzativo] qualora vi siano elementi investigativi che giustifichino l'attività di prevenzione e lo ritenga necessario. […] Invece la novella prevede che – non essendoci elementi investigativi nelle operazioni dei Servizi – l'autorizzazione si basi esclusivamente sul fatto che tali intercettazioni risultino "indispensabili per l'espletamento

[26] L. 29 dicembre 2022, n. 197, recante "*Bilancio di previsione dello Stato per l'anno finanziario 2023 e bilancio pluriennale per il triennio 2023-2025*", in *Gazz. uff.*, 29 dicembre 2022, n. 303.
[27] Cfr. d.l. 144/2005.
[28] Come noto, a seguito delle modifiche operate dall'art. 12, l. 133/2012, l'art. 4, d.l. 144/2005 prevede che la legittimazione attiva alla richiesta autorizzativa spetti ai Direttori dei servizi di informazione per la sicurezza di cui all'art. 2, comma 2, l. 124/2007, ovvero i Direttori dell'AISE (Agenzia di informazione per la sicurezza esterna) e dell'AISI (Agenzia di informazione per la sicurezza interna). Inoltre, sempre per effetto della novella del 2012, la competenza viene attribuita al procuratore generale presso la Corte di appello di Roma.
[29] La legge 133/2012 elimina la previsione secondo cui l'istanza può essere presentata solo per esigenze connesse alla prevenzione di attività terroristiche o di eversione dell'ordinamento costituzionale o del crimine organizzato di stampo mafioso e dispone che le intercettazioni preventive possono essere richieste «quando siano ritenute indispensabili per l'espletamento delle attività demandate ai direttori dei Servizi di informazione per la sicurezza dagli artt. 6 e 7 della l. 124/2007» (art. 4, comma 1, d.l. 144/2005).
[30] Si tratta di attività volte alla ricerca e all'elaborazione di informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica dalle minacce provenienti dall'estero nonché la sicurezza interna della Repubblica e le istituzioni democratiche.

delle attività demandate" ai Servizi»[31].

Dal tenore del *Dossier*, sembra che la novella sia scritta al fine di assottigliare le maglie di accesso all'istituto, eliminando la previsione per la quale, ai fini dell'autorizzazione a procedere, sia necessaria la presenza di elementi "informativi" atti a giustificare la valutazione del procuratore circa l'indispensabilità delle operazioni.

A nostro avviso, così non è, nel senso che la modifica non opera alcuna restrizione quanto ai presupposti. Infatti, il requisito della sussistenza degli elementi investigativi che giustificano le attività preventive (che parrebbe essere stato tolto) è espressamente richiesto solo per le sole intercettazioni *ante delictum* di polizia; né prima né dopo la riforma, tale presupposto era ed è previsto dal dettato normativo con riferimento alle captazioni preventive d'*intelligence*. Anche se qualcuno[32], in ragione del rinvio che l'art. 4, d.l. 155/2005 operava alla disciplina di cui all'art. 226 disp. att. c.p.p., ha ritenuto applicabile tale presupposto anche alle intercettazioni preventive d'*intelligence*, non c'è alcun dubbio invece che la normativa "speciale" di riferimento di cui all'art. 4, d.l. 144/2005, non effettua in alcun modo tale richiamo[33].

Di conseguenza, si può ritenere che la novella abbia solo inteso fare chiarezza sui presupposti legittimanti l'autorizzazione a procedere, fugando ogni dubbio ravvisabile sulla ambigua formulazione linguistica previgente; di conseguenza, non può dirsi che la riforma abbia operato una modifica destinata a facilitare le condizioni di utilizzo dello strumento captativo.

L'aspetto maggiormente innovativo (almeno sotto il profilo formale) attiene all'introduzione, nel d.l. 144/2005, di un inedito art. 4-*bis*, rubricato "*Disposizioni in materia di intercettazioni preventive dei servizi di informazione per la sicurezza*", che reca la nuova disciplina sulle modalità di svolgimento delle intercettazioni.

Pur rimanendo immutati alcuni aspetti della precedente normativa (il termine di durata massima delle operazioni di intercettazione[34], la forma del provvedimento autorizzativo[35], i presupposti per la richiesta e le modalità operative relative alle attività di controllo sulle comunicazioni[36]), si segnalano elementi originali che contribuiscono a rendere maggiormente coerente il dettato normativo sotto il profilo sistematico.

Le prime novità attengono al materiale oggetto di deposito presso il procuratore generale e ai termini per procedervi.

Precisamente, la riforma prevede che, oltre al verbale sintetico delle operazioni svolte e ai supporti utilizzati, l'obbligo di consegna si estende anche ai contenuti delle captazioni[37]. Conseguentemente, la novella procede a rimodulare i termini per ottemperare a tali doveri, rendendoli più congrui rispetto al passato, anche considerando i nuovi "adempimenti" da compiere.

In particolare, la riforma estende il termine dagli attuali 5 giorni (ovvero 10 in casi particolari) a 30 giorni decorrenti dalla conclusione delle operazioni, prevedendo la possibilità del differimento del termine per un periodo non superiore a 6 mesi, previa autorizzazione del procuratore generale su richiesta motivata dei Direttori dei Servizi di informazione, comprovante particolari esigenze di natura tecnica e operativa[38].

In secondo luogo, nell'ottica di conferire maggiore coerenza alla previsione in esame, il legislatore prevede un ampliamento dei doveri di distruzione di tutto il materiale consegnato, compresi i contenuti intercettati e ogni eventuale copia, anche informatica, totale o parziale, degli stessi.

[31] *Dossier* del Servizio Studi del Senato, p. 129, disponibile su *Sistema penale,* 30 dicembre 2022.
[32] Ricostruisce i termini del dibattito, Agostini (2017), pp. 141-148
[33] Sicuramente, anche nel caso di intercettazioni preventive d'*intelligence*, è necessario un "*quantum* informativo" utile al p.m. per decidere se procedere o meno all'autorizzazione. Si tratta, in particolare, del materiale acquisito all'esito del c.d. "ciclo investigativo d'*intelligence*" e che risulta indispensabile per la valutazione circa l'indispensabilità delle captazioni dei Servizi di informazione e sicurezza. Di conseguenza, in mancanza di una previsione esplicita nel dettato di cui all'art. 4, d.l. 144/2005, si potrebbe ritenere che «la presenza degli elementi fattuali da cui possa emergere il *periculum* da scongiurare deve considerarsi presupposta, ossia sottesa all'istanza autorizzativa come condizione implicita alla richiesta stessa». Così Nocerino (2019), p. 114.
[34] Il termine di durata resta di 40 giorni prorogabile per periodi successivi di 20 giorni, *ex* art. 4-*bis*, comma 1, primo periodo, d.l. 1 44/2005.
[35] La forma del provvedimento richiesta è il decreto autorizzativo, ai sensi del comma 1, secondo periodo dell'art. 4-*bis*, d.l. 144/2005.
[36] Ci si riferisce al tracciamento delle comunicazioni telefoniche e telematiche, all'acquisizione dei dati esterni relativi alle comunicazioni telefoniche e telematiche intercorse e all'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni. I presupposti per la richiesta nonché la competenza relativa all'autorizzazione sono gli stessi previsti per le operazioni di intercettazione, secondo quanto previsto dal comma 4 dell'art. 4-*bis*, d.l. 144/2005.
[37] Ai sensi dell'art. 4-*bis,* comma 2, d.l. 144/2005.
[38] Come si legge nella Relazione tecnica di accompagnamento alla proposta di emendamento, «il termine di 5 giorni per depositare i nostri risultava particolarmente restrittivo […] in presenza di operazioni prolungate nel tempo, quando le informazioni da riversare nei supporti esterni hanno la dimensione di diversa terabyte».

Non solo, perché viene introdotto l'obbligo per il procuratore di distruggere anche la documentazione da lui stesso detenuta, con eccezione dei decreti emanati, relativa alle richieste di autorizzazione alle operazioni di intercettazione, recante contenuti, anche in forma sintetica e discorsiva, delle intercettazioni[39].

Poi, la novella incide anche sui tempi per eliminare i risultati delle attività che esulano dell'intercettazione *stricto sensu* intesa (c.d. controlli)[40]: colmando il vuoto normativo della previgente disciplina, la riforma prevede che tali dati debbano essere distrutti entro 6 mesi dalla acquisizione e che i relativi verbali debbano essere trasmessi al procuratore generale, ferma restando la possibilità per il procuratore generale di autorizzare la proroga per un periodo non superiore a 24 mesi del termine per la conservazione di tali dati[41].

Spunti di novità ineriscono anche alle eccezioni alle c.d. *exclusionary rules.*

Come è noto, ai sensi del comma 5 dell'art. 4-*bis*, gli elementi acquisiti attraverso le attività preventive non possono essere utilizzati nel corso del procedimento penale, non possono essere menzionati in atti di indagine né costituire oggetto di deposizione né essere altrimenti divulgati, ferma restando la possibilità di utilizzare quel materiale per "fini investigativi".

In questo caso – seppure l'esecutivo rimarca che «[I]l mancato riferimento a tali fini dipende peraltro dalla specificità dell'attività dei Servizi di informazione che non compiono attività investigativa»[42] –, attraverso l'eliminazione di tale clausola derogatoria la riforma supera le perplessità di quanti avevano intravisto nella clausola in esame una *fictio iuris* funzionale all'ingresso in fase procedimentale dei risultati raccolti in fase preventiva[43].

Da ultimo, si prevede che le spese relative alle attività di intercettazione e tracciamento, attualmente a carico del Ministero della Giustizia, siano imputate all'apposito programma di spesa iscritto nello stato di previsione della spesa del Ministero dell'economia e delle finanze, nell'ambito degli stanziamenti previsti a legislazione vigente.

La scelta di sottrarre la "competenza" di spesa al Ministero della Giustizia non significa solo infierire sull'amministrazione delle risorse economiche, quanto intervenire sulla gestione delle informazioni ottenute, consentendo di evitare che i dati acquisiti possano essere trasferiti e conservati da un organo esterno e, dunque, impedendo «la circolazione al di fuori del comparto di *intelligence* di documentazione […] contenente elementi di natura sensibile […] che rende riconoscibile l'attività dei Servizi di informazione, determinando un evidente *vulnus* alle esigenze di riservatezza delle suddette operazioni»[44].

4. Il regime di utilizzabilità probatoria delle captazioni *ante delictum*: la presunta impermeabilità tra sistema preventivo e repressivo.

Una volta delineato lo "spazio" entro cui confinare le captazioni preventive, occorre soffermarsi sulle disposizioni inerenti al regime di utilizzabilità probatoria dei dati acquisiti tramite le investigazioni proattive, con lo scopo di comprendere più agevolmente l'origine dell'osmosi probatoria tra *pre* e *post delictum.*

Si cominci col dire che il sistema intende mantenere distinta la fase preventiva, di ricerca e analisi dei dati da quella repressiva della giurisdizione penale, sul presupposto che le due funzioni non sono in alcun modo assimilabili[45]: quella d'*intelligence* è tesa a ricercare ed elaborare tutte le informazioni utili a difendere la sicurezza interna ed esterna dello Stato e delle sue

[39] Il procuratore procede alla distruzione decorso il termine per l'adempimento degli obblighi di comunicazione da parte del Presidente del Consiglio dei ministri al Comitato parlamentare per la sicurezza della Repubblica, ossia 30 giorni dalla conclusione delle operazioni.
[40] Ossia il tracciamento delle comunicazioni telefoniche e telematiche, l'acquisizione dei dati esterni relativi alle comunicazioni telefoniche e telematiche intercorse e l'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni.
[41] Come chiarito nel *Dossier* del Servizio Studi del Senato, cit., p. 130, «[N]ella disciplina vigente la possibilità di proroga per un periodo non superiore a 24 mesi è prevista nella disciplina generale delle intercettazioni preventive dal comma 3-*bis* dell'art. 226 disp. att. c.p.p. Tale comma non è tuttavia richiamato dall'art. 4, d.l. 144/2005, per cui la possibilità di proroga della conservazione dei dati non è applicabile alle operazioni di tracciamento dei servizi di informazione».
[42] *Dossier* del Servizio Studi del Senato, cit., p. 132.
[43] Per lungo tempo, la dottrina si è chiesta se la locuzione *de qua* debba essere riferita all'attività di prevenzione in senso stretto ovvero essere estesa anche alla successiva fase delle indagini preliminari. Per un approfondimento sui termini della questione, Filippi e Cortesi (2004), pp. 2-10.
[44] Relazione tecnica di accompagnamento alla proposta emendativa, p. 2.
[45] Sulla necessità di tenere separati i due momenti, per tutti, Curtotti (2018), pp. 442-443.

istituzioni democratiche da ogni minaccia, attività eversiva e forma di aggressione criminale o terroristica; quella di polizia (giudiziaria) è deputata all'accertamento dei fatti di reato[46]. Dunque, «[N]non il principio di collaborazione, ma piuttosto il principio di separatezza ha finora caratterizzato i rapporti tra queste due espressioni del potere statuale»[47].

Proprio in questa direzione si muove la disciplina delle intercettazioni preventive, costruita in modo da garantire – almeno formalmente – l'impermeabilità del procedimento penale ai risultati di indagine di natura proattiva.

Più in particolare, il comma 3 dell'art. 226 disp. att. c.p.p., prescrive l'onere di distruzione della documentazione attestante le modalità esecutive delle operazioni di captazione e i contenuti più rilevanti carpiti dagli operanti e, per quelle d'*intelligence,* il comma 3 dell'art. 4-*bis*, d.l. 144/2005, anche delle stesse informazioni ottenute. Inoltre, il comma 5 dell'art. 226 disp. att. c.p.p. e il comma 5 dell'art. 4-*bis*, d.l. 144/2005, prevedono che gli elementi acquisiti attraverso le attività preventive non possono essere «in ogni caso […] utilizzati nel corso del procedimento penale», rafforzando la prescrizione con il divieto di pubblicizzazione delle informazioni apprese, per cui «in ogni caso […] le notizie […] non possono essere menzionate in atti di indagine né costituire oggetto di deposizione né essere altrimenti divulgate».

Con l'introduzione della regola di esclusione probatoria e del divieto di menzione delle notizie apprese *ante delictum*, rafforzate dall'obbligo di distruzione delle informazioni così ottenute, il legislatore ha voluto tenere fede al principio della necessaria separazione tra prevenzione e repressione e, più precisamente, degli ambiti e dei compiti di *intelligence* e di polizia al fine di evitare qualunque forma di contaminazione tra *pre* e *post* procedimento.

In questo senso, l'obiettivo è quello di evitare che l'inizio del procedimento penale possa essere condizionato dalle investigazioni pre-procedimentali e, di conseguenza, che gli esiti del processo dipendano da quanto emerge in una fase che nello stesso non pare assolutamente ricompresa.

Tuttavia, alle *exclusionary rules* richiamate il legislatore oppone delle "clausole derogatorie" che consentono una qualche forma di impiego dei risultati ottenuti in fase preventiva.

Intanto, contrariamente alla previsione per cui i supporti e i verbali redatti durante l'esecuzione delle operazioni devono essere distrutti, il comma 3-*bis* dell'art. 226 disp. att. c.p.p. (e, parallelamente, nel caso di captazioni d'*intelligence,* il comma 4 dell'art. 4, d.l. 144/2005), introduce la possibilità di conservare – per un periodo non superiore a ventiquattro mesi – «i dati acquisiti, anche relativi al traffico telematico, esclusi […] i contenuti delle intercettazioni», qualora siano essenziali per la prosecuzione dell'attività di prevenzione.

Inoltre, solo con riferimento alle captazioni *ante delictum* d'*intelligence,* il divieto di utilizzo procedimentale delle informazioni apprese in fase preventiva, viene stemperato da una "clausola di salvaguardia" che ne consente un impiego ai soli «fini investigativi»[48], ossia per la prosecuzione delle investigazioni di natura preventiva e non certo come "fonti" o "elementi" di prova per il processo penale.

5. I rischi di infiltrazione processuale.

Se quella appena descritta è la condizione ideale prefigurata sul piano normativo, nella prassi si assiste ad una costante interazione tra funzione preventiva e repressiva e, di conseguenza, è sempre più frequente la trasmigrazione "indiretta" dei risultati di indagini acquisiti *ante delictum* nel procedimento penale.

Ciò per almeno tre ordini di ragioni interconnesse tra loro.

La prima è intrinseca al dettato normativo. La legittimazione della procura al rilascio dell'autorizzazione a procedere alle operazioni *de quibus* contribuisce, infatti, a indebolire la

[46] La profonda distinzione tra le funzioni di *intelligence* e di p.g. è definibile sotto un profilo di competenza. I Servizi di informazione e sicurezza sono inseriti nella struttura del potere esecutivo al fine di garantire una risposta tecnica alle necessità informative del Governo mentre le autorità requirenti (quindi la polizia giudiziaria e la magistratura) sono espressione dell'autonomo potere giudiziario volto alla prevenzione ed alla repressione dei reati. Sul punto v. Orlandi (1996), p. 583-592.

[47] Così Orlandi (1996), p. 229.

[48] Clausola inserita in sede di conversione del decreto, «perché in caso contrario le intercettazioni preventive sarebbero state del tutto inutili, non potendosi, sulla base delle stesse, avviare le necessarie investigazioni. […] Tuttavia, si è ritenuto di tutelare la corretta formazione della prova, oltre che la *privacy*, vietando che le notizie acquisite, a seguito di intercettazioni preventive, vengano a conoscenza del giudice del dibattimento». Così Relazione dell'on. Pecorella, in *Atti Camera*, XIV leg., Assemblea, seduta del 19 novembre 2001, *Resoconto stenografico*, p. 16.

pretesa impermeabilità fra il procedimento penale di prevenzione e quello di cognizione.

É evidente come il p.m., laddove partecipi – direttamente o indirettamente – alla ricerca preventiva della notizia di reato, «venga necessariamente introdotto negli spazi investigativi propri [della polizia di pubblica sicurezza], sì da condividerne anche le logiche improntate a scelte di opportunità ed a valutazioni ampiamente discrezionali proprie della polizia stessa»[49].

Come sostenuto, «non sembra del tutto coerente con questa impostazione la scelta di imporre una coincidenza fra l'organo che deve autorizzare le intercettazioni preventive e l'organo che potrebbe poi instaurare un procedimento penale su fatti appresi nell'espletamento di indagini preventive; se anche il legislatore ha inteso escludere l'utilizzabilità come *notitia criminis* dei risultati captativi così ottenuti, stabilendo che essi debbano essere immediatamente distrutti dopo che il procuratore della Repubblica abbia verificato l'irregolarità delle operazioni, quest'organo potrebbe sfruttare le conoscenze in ogni caso acquisite per procedere alla ricerca della notizia di reato, per dare quindi avvio al procedimento penale, e compiere specifici atti d'indagine all'esito dei quali determinarsi eventualmente per l'esercizio dell'azione penale»[50].

Il secondo motivo che favorisce la permeabilità del procedimento penale deriva dalla possibilità che le indagini proattive "orientino" gli operatori dell'inchiesta all'acquisizione della notizia di reato.

In particolare, dal combinato disposto degli artt. 226, comma 5, disp. att. c.p.p. e 330 c.p.p., emerge che, fermo restando il divieto di impiego procedimentale, le informazioni ottenute *ante delictum* – al pari di ogni altra fonte "spuria"[51] – possono comunque rappresentare uno stimolo investigativo "per" formare la notizia di reato, nel rispetto del potere riconosciuto al p.m. e alla p.g. di prendere notizia di reato di propria iniziativa.

In altre parole, si ritiene consentito l'uso dei dati acquisiti in sede preventiva quale «presupposto euristico suscettibile di attivare investigazioni preordinate all'individuazione della *notitia criminis*»[52].

Il dato diventa ancora più rilevante a fronte della rimarcata esigenza di coordinamento ed organicità dell'azione investigativa, sul presupposto che «le iniziative promosse dal potere esecutivo e iniziative giudiziarie vanno armonizzate, non condotte separatamente»[53].

Questa nuova cultura investigativa, seppur funzionale a migliorare e velocizzare risultati investigativi, può agevolare un ingresso indiretto delle informazioni apprese *ante delictum*, favorendo proprio quella circolazione probatoria che il sistema aveva ripudiato.

Ci si riferisce, in particolare, alla possibilità di indirizzare le indagini verso una "ricerca mirata"[54]: non è infrequente, infatti, che le investigazioni compiute "per" la formazione della notizia di reato da parte della p.g. siano "guidate" dagli uomini dell'*intelligence* che ottengono dati sospetti nell'ambito dell'attività di osservazione, informazione e vigilanza compiute durante i servizi di prevenzione, in quanto « […] nulla osta che [le notizie raccolte in sede preventiva] possano essere utilizzate in modo surrettizio quali occulti strumenti di indagine da cui poi origineranno atti investigativi *post delictum*, al contrario sicuramente utilizzabili»[55]. Si pensi, ad esempio, che sulla base delle notizie acquisite tramite intercettazioni preventive d'*intelligence*, pur non figurando negli atti di indagine, la p.g. proceda a perquisizioni di propria iniziativa e, in esito ad essa, al sequestro del corpo del reato e delle cose ad esso pertinenti o all'arresto in flagranza o al fermo di indiziato di delitto[56].

La terza – probabilmente più dirimente – ragione risiede nella denunciata sovrapposizione di ruoli e funzioni tra *intelligence* e p.g.

Come si è avuto modo di anticipare[57], l'esperienza degli ultimi vent'anni mostra un progressivo ampliamento dei momenti di contatto tra i due asettici comparti, al fine di contenere le nuove emergenti esigenze investigative legate al contrasto alla criminalità organizzata di stampo mafioso ed eversivo e al terrorismo internazionale.

In questi settori, attività d'*intelligence* e investigativa vanno sempre più condividendo concetti strutturali e modalità operative onde condurre le indagini necessarie al perseguimento dei

[49] Si esprime così Andolina (2016), p. 569.
[50] Orlandi (2015), p. 559.
[51] Così la definisce Colaiacovo (2009), p. 4321.
[52] Così Cantone (1996), p. 2988.
[53] Si esprime così Orlandi (2010), p. 229.
[54] Sul punto Di Bitonto (2006), p. 255.
[55] Filippi e Cortesi (2004), p. 9.
[56] L'esempio è riportato da Filippi (2002), p. 169.
[57] Sulle ragioni che hanno determinato tale commistione, cfr. § 1.

rispettivi obiettivi. Entrambe queste attività puntano ad acquisire informazioni su fenomeni criminosi con la caratteristica di essere spazialmente diffusi e duraturi nel tempo; entrambe agiscono prevalentemente con indagini occulte, le uniche che permettono di conoscere fenomeni delittuosi ancora in corso di svolgimento.

D'altra parte, è proprio la peculiare tipologia delle fattispecie di reato coinvolte dall'attività investigativa a carattere preventivo ad accentuare il pericoloso "gioco" di ruoli tra i due comparti. Nell'ambito di siffatti complessi contesti investigativi, infatti, la medesima attività può configurarsi come repressiva rispetto ad un reato (reato presupposto) e come preventiva rispetto ad un altro tipo di fattispecie delittuosa (reato scopo)[58], determinando la progressiva erosione della linea di confine tra le attività proprie dell'*intelligence* e quelle di polizia.

Non solo. Perché l'intrico inestricabile derivante dalla commistione funzionale tra *intelligence* e p.g. è anche favorito dalla facile fruibilità e condivisibilità degli strumenti di ultimissima generazione utilizzati nei vari ambiti di indagine[59]; strumenti nelle mani degli stessi operatori per il conseguimento di scopi differenti ma interconnessi, rispetto ai quali non è poi così facilmente possibile tracciare una netta linea di demarcazione che scinda la prevenzione dalla repressione.

Si pensi, solo a titolo esplicativo, al captatore informatico che, da strumento tipizzato in chiave procedimentale, è diventato lo strumento privilegiato con il quale gli operatori danno luogo ad intercettazioni e controlli preventivi sulle comunicazioni[60], o – ancor di più – all'*IMSI Catcher,* con il quale le Forze di polizia e i Servizi di *intelligence* possono monitorare tutti i dispositivi elettronici presenti in un certo raggio di azione, identificare i titolari delle utenze individuate e procedere alla captazione di comunicazioni e al tracciamento dei dati che transitano sulla "macchina–bersaglio"[61].

Senza contare, poi, il fatto che, non esistendo un autonomo corpo di polizia per le indagini di natura repressiva, gli stessi uomini che svolgono le investigazioni proattive si trovano a compiere anche le indagini susseguenti all'inizio del procedimento penale[62]. In questi casi, la relazione osmotica tra *pre* e *post delictum*, determinata da una frequente eterogenesi dei fini nell'ambito delle diverse vesti indossate contemporaneamente, appare inevitabile, dal momento che i protagonisti dell'inchiesta saranno chiamati a svolgere indagini per l'accertamento del fatto di reato con un approccio non più puro e scevro da condizionamenti esterni ma intriso delle informazioni incamerate in fase preventiva.

6. L'interazione tra le investigazioni d'*intelligence* e il procedimento di cognizione.

A prescindere dall'interazione tra *intelligence* e p.g. e, dunque, dal possibile uso "indiretto" delle informazioni ottenute in fase preventiva, il procedimento osmotico tra pre e *post delictum* è agevolato anche dalla possibilità di impiegare – questa volta in via "diretta" in sede procedimentale e processuale – gli elementi investigativi che giustificano il rilascio dell'autorizzazione a procedere[63].

Ci si riferisce, in particolare, alla presunta spendibilità processuale della mole di informazioni che entra nel patrimonio conoscitivo del p.m. allorquando i Servizi di informazione e sicurezza presentano formale istanza per procedere alle intercettazioni e ai controlli preventivi sulle comunicazioni, *ex* art. 4, l. 155/2005.

Come noto, all'esito del ciclo investigativo d'*intelligence* – procacciamento dei dati mediante tecniche di sorveglianza non mirata; incrocio degli stessi per l'individuazione di gruppi

[58] In questo senso Andolina (2016), p. 575.
[59] Si tratta, in particolare, di strumenti di indagine occulti a più forte carattere invasivo quali – tra gli altri – il pedinamento satellitare, sistemi di cattura elettronica dell'identità dei telefoni cellulari (c.d. *IMSI Catcher*), l'ascolto dei dialoghi o la videoripresa di immagini a distanza tramite l'inoculazione di *virus* informatici in dispositivi elettronici di uso comune. Con precipuo riferimento all'uso degli strumenti tecnologici in fase preventiva e repressiva, si consenta il rinvio a Nocerino, (2020), p. 824 ss.
[60] Sul tema, volendo, Nocerino (2021b), pp. 5-40.
[61] Cfr. Camon (2020), pp. 1-10.
[62] Non è infrequente che gli agenti di pubblica sicurezza legittimati, su delega del Ministero dell'Interno, a richiedere l'autorizzazione alle intercettazioni e ai controlli preventivi sulle comunicazioni, possono rivestire anche le funzioni di p.g.
[63] Come anticipato nel § 2.1, ai sensi del comma 2 dell'art. 226 disp. att. c.p.p., le intercettazioni vengono autorizzata sulla base di «elementi investigativi che giustifichino l'attività di prevenzione».

di relazione; esecuzione delle attività "tipiche" per individuare il sospetto –, gli appartenenti al DIS informano il p.m. dell'attività preventiva compiuta, anche attraverso la consegna del materiale idoneo a rappresentare l'informazione acquisita, al fine di permettergli di valutare l'indispensabilità delle operazioni di intercettazione preventiva.

Di qui le criticità. Ci si domanda, in sostanza, se quel "patrimonio conoscitivo" di cui entra in possesso il p.m. possa o meno trovare impiego nell'ambito del procedimento di cognizione, ovvero, al contrario, debba seguire il medesimo trattamento delle informazioni apprese durante l'esecuzione delle captazioni e dei controlli preventivi di cui all'art. 226 disp. att. c.p.p.

Al fine di trovare una risposta sono alcune considerazioni preliminari.

Intanto, la possibilità di utilizzare "prove precostituite", ossia redatte fuori dal procedimento penale ovvero prima ancora della sua instaurazione, è ormai pacifica sia in dottrina[64] che in giurisprudenza[65], in ragione del condivisibile obiettivo di non disperdere strumenti di conoscenza.

In secondo luogo, va precisato che nessuna norma – né codicistica, né contenuta in leggi speciali – vieta l'acquisizione degli atti inerenti alle indagini proattive "atipiche" degli uomini d'*intelligence*. Allo stato dell'arte, infatti, non è disciplinata la sorte risultanze delle attività prodromiche alla richiesta di cui all'art. 226 disp. att. c.p.p., ossia quelle investigazioni condotte dai Servizi di *intelligence* per procacciarsi gli elementi investigativi sui quali si fonda l'istanza e la conseguente decisione del p.m.

Al contrario, il sistema sembra ammettere una parziale apertura agli atti investigativi *de quibus.* Seppur limitatamente alle informazioni apprese attraverso strumenti di cooperazione internazionale, l'art. 6, d.lgs. 54/2015, rubricato "*Utilizzazione delle informazioni o delle analisi come prova nell'ambito di un'indagine penale*", prevede la possibilità di acquisire, previa autorizzazione dello Stato membro, i dati raccolti durante l'espletamento delle attività preventive d'*intelligence* «come prove o elementi di prova», nell'ambito del processo penale.

Alla luce di tali considerazioni, deve ritenersi – quantomeno con riguardo alle captazioni d'*intelligence* – che la previsione dell'inutilizzabilità (diretta e indiretta) del materiale acquisito in via preventiva si riferisca solo ai risultati ottenuti dalle intercettazioni e dai controlli *ante delictum*, non estendendosi, per contro, al complesso di informazioni raccolte "per" fondare la richiesta autorizzativa.

Non solo. Dall'analisi delle disposizioni codiscistiche emerge anche un ulteriore dato che sembra suffragare la tesi *de qua*. Ai sensi dell'art. 256-*bis* c.p.p., infatti, è consentita l'acquisizione, da parte del p.m., di documenti e atti presso le sedi dell'AISI o dell'AISE o presso gli uffici del DIS, «qualora gli stessi risultino strettamente indispensabili ai fini delle indagini»[66], consentendo, *de facto,* l'utilizzo processuale dei risultati delle attività di indagine preventiva dei Servizi.

Di conseguenza, anche a prescindere dal deposito formale degli elementi attestanti l'attività di *intelligence* preventiva da cui emergono gli elementi su cui fondare la richiesta di intercettazioni preventive, gli atti inerenti alle indagini proattive possono trovare precisa collocazione nel procedimento penale sulla base di una "scelta investigativa" del p.m.: quest'ultimo, infatti, è legittimato a recuperare personalmente materiale utile alle indagini che diventa, *tout court,* elemento di prova da sottoporre alla valutazione del giudice.

Se questi sono gli indici dai quali emergono spiragli per consentire un utilizzo procedimentale alle informazioni preventive d'*intelligence*, si potrebbe per contro obiettare che le stesse trovino uno sbarramento processuale, in punto di acquisizione e di utilizzo, in ragione del vincolo del segreto di Stato apposto, *ex* art. 39, comma 1, l. 124/2007, «agli atti, documenti, notizie e attività la cui diffusione potrebbe recare danno all'integrità della Repubblica».

Sotto questo profilo occorre precisare che le notizie apprese dai Servizi d'*intelligence* in ragione delle attività di informazione e sicurezza non sempre possono trovare un simile limite probatorio.

Più nel dettaglio, ai sensi del comma 11 dell'art. 39, l. 124/2007, non possono essere coperte dal segreto di Stato notizie relative a fatti eversivi dell'ordine costituzionale o concernenti il terrorismo, delitti di strage, associazione a delinquere di stampo mafioso, scambio elettorale politico-mafioso.

[64] Sul punto, senza pretese di completezza, Kalb (2000), p. 16; Maggio (1990), pp. 1-30; Zacchè (2012), pp. 1-50.
[65] Riferendosi alla giurisprudenza più recente, *ex plurimis,* Cass., sez. VI, 27 maggio 2021, n. 33751, in *CED Cass.*, n. 281981; Cass., sez. V, 5 febbraio 2021, n. 12062, *ivi,* n. 280758; Cass., sez. V, 6 ottobre 2020, n. 31831, *ivi,* n. 279776.
[66] Si esprime così Giunchedi (2008), p. 10.

A ben guardare, le ipotesi delittuose richiamate ineriscono ai "casi" per i quali la legge legittima l'esecuzione delle intercettazioni e dei controlli preventivi sulle comunicazioni, di cui all'art. 226 disp. att. c.p.p.; può, quindi, affermarsi che le informazioni apprese dai Servizi d'*intelligence* in relazione alla prevenzione dei reati di criminalità organizzata e terrorismo, non essendo vincolate dal segreto di Stato, possono trovare impiego procedimentale.

Una volta ammessa la trasmigrazione in fase processuale delle risultanze delle investigazioni proattive, pare opportuno individuarne la corretta veste giuridica al fine di inquadrare la relativa acquisizione nel *genus* dei mezzi di prova tipici.

Si ritiene che alle notizie e ai dati acquisiti dai Servizi d'*intelligence* possa essere attribuita la forma di "documento", rispettandone i crismi fondamentali[67], costituendo «una rappresentazione di conoscenza incorporata su qualsiasi base materiale, redatta da soggetti estranei al procedimento penale»[68].

In effetti, la scelta di fornire una simile qualificazione giuridica alla mole di informazioni raccolte *ante delictum*, può trovare conferme nel disposto dell'art. 220 disp. att. c.p.p.[69] che, in relazione agli atti compiuti dalle forze dell'ordine prima dell'acquisizione della *notitia criminis*, attribuisce ai dati raccolti in una fase pre-procedimentale la forma di "documenti"[70].

Conseguentemente, l'acquisizione processuale di tali dati seguirà le regole generali relative alle prove documentali[71] che, come noto, non risultano sottoposte ai termini di cui all'art. 493 c.p.p.[72].

Più in particolare, nel caso di atti non aventi contenuto dichiarativo[73], i documenti contenuti nel fascicolo del p.m. possono confluire in quello dibattimentale attraverso due differenti modalità: sia a seguito della produzione e contestuale deposito ad opera della parte che intende introdurre il documento nel corso dell'udienza, ai sensi del disposto di cui all'art. 495, comma 3, c.p.p., sia mediante acquisizione concordata, *ex* art. 493, comma 3, c.p.p., per cui risulta sanata l'inutilizzabilità di tipo fisiologico.

Nel caso di documenti aventi contenuto dichiarativo, invece, l'acquisizione può avvenire mediante la testimonianza consentita anche agli organi d'*intelligence* che possono servirsi di identità mascherate[74].

Da quanto detto emerge che l'attività tipica dei Servizi di informazione e sicurezza può fare ingresso nel procedimento penale attraverso i "tradizionali" canali di acquisizione delle prove documentali, determinando «l'ennesimo scivolamento all'indietro sino ai territori dell'*intelligence* [che] rischia di alimentare l'accertamento con dati di origine occulta, di nascondere circostanze viceversa preziose nel lumeggiare il contesto investigativo di scoperta dei fatti illeciti, si sottrarre ulteriore presa allo stesso pubblico ministero e persino alla polizia, consegnando, così, il primato nelle mani dei servizi segreti: saremmo dunque di fronte […] alla "*Vergeheimdienstlinchung*" del processo penale»[75].

[67] Il concetto di documento comprende quattro elementi fondamentali: il fatto rappresentato (fatti, persone, cose o dichiarazioni); la rappresentazione (ossia la sua riproduzione); l'incorporamento (la rappresentazione fissata su un supporto attraverso metodo analogico o digitale); la base materiale (il supporto su cui è incorporata la rappresentazione). Come precisato nella *Relazione al progetto preliminare* (p. 67) e nella *Relazione al testo definitivo* (p. 182), gli artt. 234 ss. riguardano solo «i documenti formati fuori del processo nel quale si richiede o si dispone che essi facciano ingresso».

[68] Così Tonini e Conti (2014), p. 353.

[69] L'art. 220 disp. att. c.p.p. sottolinea la differenza tra documento e documentazione, stabilendo che qualora un organo di vigilanza assuma la qualifica di p.g., dal momento in cui iniziano ad emergere degli indizi di reità, non redige più "documenti" ma "documentazione". Se il documento rappresenta un fatto o un atto differente dall'atto processuale compiuto nel procedimento nel quale il documento è acquisito, la documentazione è un atto processuale compiuto nel medesimo procedimento

[70] Secondo la giurisprudenza di legittimità, gli atti compiuti prima del sorgere degli indizi di reato devono essere considerati documenti a tutti gli effetti. Cass., sez. IV, 28 aprile 2006, n. 3554, in *Arch. giur. circ.,* 2007, 4, p. 378.

[71] Sul punto Adorno (2012), pp. 13-35; Mancuso (2017), p. 105-137.

[72] Ad avviso dei giudici di legittimità, «deve escludersi che l'art. 493 […] preveda una preclusione alla esibizione di documenti, ed all'ammissione di essi da parte del giudice, ad un momento successivo a quello fissato dalla norma suddetta, essendo tale preclusione esplicitamente limitata alle prove che devono essere indicate nelle liste di cui all'art. 468 c.p.p.», fermo restando che le altre parte hanno il diritto di esaminarli a norma dell'art. 495, comma 3, c.p.p.». Cass., sez. II, 22 novembre 1994, n. 2533, in *Cass. pen*., 1996, p. 844.

[73] Sul concetto di documenti non aventi contenuto dichiarativo, Cass., sez. I, 13 luglio 2012, n. 42130, in *CED Cass*., n. 253800; Cass., sez. III, 16 aprile 2008, n. 19968, *ivi,* 240048; Cass., sez. V, 8 ottobre 2003, n. 44868, *ivi* n. 227009; Cass., sez. III, 15 giugno 1999, n. 11116, *ivi*, 214457.

[74] Per una ricostruzione storica dell'istituto, per tutti, Curtotti (2015), pp. 427-428.

[75] Così Negri (2016), p. 51.

7. Un'anomala inversione di ruoli e funzioni: la dubbia compatibilità con i principi costituzionali che regolano il sistema processuale.

Al di là delle aporie processuali determinate dalla permeabilità tra sistema preventivo e repressivo, la normativa in materia di captazioni *ante delictum* sembra anche scontrarsi con il complesso di regole atte a garantire la protezione delle libertà fondamentali attraverso la predisposizione di rigorose condizioni che ne giustificano un'eventuale limitazione.

Si tratta, più in particolare, di un articolato di garanzie introdotto al fine di delimitare le ipotesi di ingiustificate compressioni: se è vero che le intercettazioni – e ancor di più quelle preventive[76] – determinano «un'intrusione nella vita privata e, più precisamente, al diritto di libertà e segretezza della corrispondenza»[77], è altrettanto vero che il sistema costituito ne ammette una limitazione solo in presenza di due condizioni complementari e non alternative, secondo il disposto di cui all'art. 15, comma 2, Cost.

In primis, la norma richiede la sussistenza di provvedimento giurisdizionale corredato di congrua motivazione, costituendo la stessa «il livello minimo di garanzia prefigurato dal citato precetto costituzionale per la limitazione del diritto in questione, allo scopo di assicurare un equo contemperamento fra il diritto stesso e l'interesse alla prevenzione e alla repressione dei reati, oggetto anch'esso di protezione costituzionale»[78] (riserva di giurisdizione).

In secondo luogo, è indispensabile la presenza una norma giuridica che legittimi la l'ingerenza (riserva di legge), al fine di contenere il potere discrezionale del magistrato e, al contempo, scongiurare il rischio di eventuali abusi da parte degli organi inquirenti.

Per quel che in questa sede rileva, è opportuno verificare se il *dictum* normativo di cui all'art. 226 disp. att. c.p.p. possa risultare compatibile con il disposto dell'art. 15, comma 2, Cost., ossia con le condizioni legittimanti qualsiasi forma limitativa delle prerogative individuali.

La prima *quaestio* da affrontare riguarda l'infelice scelta di attribuire la legittimazione passiva alla concessione dell'autorizzazione a procedere agli Uffici della procura.

Di qui, le perplessità, posto che la normativa sembra determinare un'intrinseca violazione della riserva di giurisdizione.

In effetti, non è pacifica la decisione di ricomprendere nel *genus* di "autorità giudiziaria", unica legittimata a limitare la libertà di comunicazione, anche il magistrato del p.m.[79] che, come detto, rappresenta l'organo deputato a concedere l'autorizzazione all'esecuzione delle intercettazioni preventive sia di polizia che d'*intelligence*.

Come giustamente sostenuto[80], la scelta di attribuire anche al p.m. la legittimazione ad emanare provvedimenti limitativi della libertà personale sembra non essere condivisibile se la si contestualizza nell'ambito della Carta fondamentale: infatti, all'art. 13, commi 1 e 2 Cost., si precisa che «[…] alcuna forma di […] restrizione della libertà personale è ammessa se non per atto motivato dell'autorità giudiziaria»[81] e la locuzione si interpreta in senso "stringente", in modo da ricomprendervi solo il giudice e non anche il p.m.

In questo senso sembra anche deporre una recente pronuncia della Corte di Giustizia dell'UE[82], la quale apre nuovi scenari in relazione agli atti di indagine del p.m. che incidono

[76] L'affermazione si giustifica col fatto che, in questi casi, il limite di tollerabilità alla menomazione dei diritti appare ancor più ristretto rispetto a quanto accade a seguito dell'instaurazione del procedimento penale, dal momento che l'interesse contrapposto all'intrusione si mostra evanescente e dai contorni poco chiari e definiti. In questo senso Grevi (1971), p. 1968.

[77] Corte EDU, Grande Camera, 6 settembre 1978, *Klass c. Germania*, § 41. Nello stesso senso, *ex pluribus*, Corte EDU, sez. IV, 18 maggio 2010, *Kennedy c. Regno Unito*, § 118-129 e 151; Corte EDU, sez. II, 10 aprile 2007, *Panarisi c. Italia*; Corte EDU, sez. II, 31 maggio 2005, *Vetter c. Francia*; Corte EDU, Grande Camera, 16 dicembre 1992, *Niemietz c. Germania*, § 32.

[78] C. cost., 30 novembre 2009, n. 320, in *www.cortecostituzionale.it*.

[79] Chi propende per una sua esclusione ritiene che la funzione di garanzia dei diritti è propria del giudice e non del rappresentante della pubblica accusa, in quanto quest'ultima è capace di operare realmente solo se è esercitata da un organo terzo ed imparziale, «per cui sarebbe stato preferibile conferire tale potere ad un organo giudicante, che è il solo ad offrire autentiche garanzie di terzietà, sicché la soluzione individuata appare opinabile, poiché si espone anche sotto tale angolo di visuale a seri dubbi di illegittimità costituzionale in relazione all'art. 15 Cost.». Si esprime così Cercola (2016), p. 461. Condividono la medesima impostazione, Filippi (2002b), p. 167; Filippi e Cortesi (2004), p. 6; Garuti (2005), p. 1458. Chi, invece, ritiene doveroso includere nella nozione di "autorità giudiziaria" anche il p.m, sostiene che «l'art. 15 Cost., al comma 2, nel porre una riserva di giurisdizione "rinforzata" dall'obbligo dell'atto motivato dell'autorità giudiziaria usa una locuzione assai ampia nella quale potrebbe rientrare anche il p.m.». In questo senso Balducci (2002), p. 45.

[80] De Caro (2000), p. 196.

[81] Così sostiene Filippi (2002b), p. 167.

[82] CGUE, 2 marzo 2021, *H.K.*, C-746/18. In questa stessa prospettiva, il legislatore nazionale - recependo le indicazioni dei giudici di Lussemburgo - sceglie la strada "garantista", predisponendo dei limiti alle acquisizioni dei tabulati telefonici e telematici. Cfr. D.l. 30 settembre

sui diritti fondamentali.

Più precisamente, i giudici di Lussemburgo ridimensionano il ruolo del procuratore quale organo deputato al rilascio dell'autorizzazione all'acquisizione dei tabulati telefonici di una persona sottoposta alle indagini: in questi casi, sul presupposto per cui i tabulati delle conversazioni telefoniche consentono di apprendere e individuare tutti i contatti con altre utenze e la loro collocazione temporale, l'incidenza rispetto alle libertà individuali è così tanto evidente da imporre di riservare tale facoltà all'autorità giudiziaria solo in seguito a vaglio o autorizzazione di un giudice terzo e imparziale.

Sotto altro aspetto, la scelta di attribuire alla procura il potere di disporre intercettazioni preventive sembra alquanto «inopportuna»[83], dal momento che determina «un ribaltamento della logica del codice di procedura penale, ove nessun potere diretto è riconosciuto all'organo dell'accusa in ordine alle decisioni in tema […] di libertà fondamentali»[84] e «uno scivolamento [dello stesso] in ambiti assolutamente sottratti al dominio della legge»[85], affidando le «scelte discrezionali di politica investigativa ad un organo che dovrebbe essere soggetto soltanto alla legge»[86], con ovvie ricadute sul principio di obbligatorietà dell'azione penale.

Invero, i punti di frizione con l'assetto costituito non sono solo limitati alla discutibile scelta di attribuire alla procura la legittimazione ad autorizzare il compimento delle captazioni preventive: il dettato codicistico, infatti, offre ulteriori spunti di riflessione in merito.

Intanto, di dubbia compatibilità costituzionale rispetto al dettato di cui al comma 2 dell'art. 15 Cost., è anche la previsione atta a delineare i presupposti applicativi delle captazioni preventive in ragione dell'imperscrutabilità circa il grado di consistenza della prognosi derivante dagli elementi raccolti. In effetti, l'impiego di formule linguistiche caratterizzate da un elevato tasso di indeterminatezza rischia di neutralizzare la portata di garanzia della procedura di autorizzazione prevista dalla norma.

Inoltre, con riguardo alla forma del provvedimento autorizzativo, l'art. 226 disp. att. c.p.p. non chiarisce l'*onus* motivazionale del magistrato autorizzante: pur attribuendogli la fisionomia del decreto motivato, mancando qualunque forma di contraddittorio in favore di chi è stato sottoposto alla misura, la norma risulta in evidente contrasto con la più recente giurisprudenza europea, per cui «l'ingerenza è legittima soltanto quando il soggetto abbia la possibilità di verifica effettiva, non solo sulla necessità dello strumento invasivo ma soprattutto sul sistema predisposto dall'ordinamento interno contro gli abusi»[87] e, dunque, solamente nell'ipotesi in cui il soggetto passivo abbia la concreta possibilità di accertare la rispondenza tra quanto autorizzato e l'attività espletata[88].

Non solo. Vigendo l'obbligo di distruzione di tutti gli atti inerenti ai risultati delle intercettazioni preventive, il soggetto monitorato non può in alcun modo venire a conoscenza dell'interferenza subita e, conseguentemente, gli risulta preclusa la possibilità di operare un controllo postumo circa la presenza di eventuali abusi o arbitri dell'atto intrusivo[89].

Poi, altrettanto dubbio pare il disposto del comma 4 dell'art. 226 disp. att. c.p.p., allorquando, tra le attività di controllo esperibili, prevede la possibilità di compiere anche la possibilità di acquisire «ogni altra informazione utile in possesso degli operatori di telecomunicazioni».

Il disposto, sempre eccessivamente vago e assai generico, determina, almeno in potenza, il rischio di legittimare qualsivoglia attività funzionale all'apprensione di notizie utili alle investigazioni *ante delictum*. Questa sorta di "norma penale in bianco", potrebbe causare una violazione del principio della riserva di legge disposto dell'art. 15 Cost., non specificando i "casi" in cui la compressione del diritto alla libertà e alla segretezza della corrispondenza può essere compresso.

Infine, in relazione alla durata delle captazioni, il legislatore appare meticoloso nel determinarne il limite massimo, commisurato in quaranta giorni, prorogabili per periodi successivi

2021, n. 132, convertito, con modificazioni, dalla l. 23 novembre 2021, n. 178. Per un commento alla normativa, per tutti, Murro (2022), pp. 2440-2455.

[83] Filippi e Cortesi (2004), p. 6.

[84] L'espressione appartiene a Balducci (2002), p. 88.

[85] Andolina (2016), p. 570.

[86] Caprioli (2011), p. 451.

[87] Corte EDU, sez. IV, 29 marzo 2005, *Matheron c. Francia*, § 40.

[88] Come sostenuto, infatti, «[…] non pare ammissibile che il controllo del rispetto dei diritti inviolabili della persona venga affidato ad un esame riservato, sottratto ad ogni possibilità di coinvolgimento del soggetto a tutela del quale esso è predisposto, ma soprattutto sottratto ad un successivo sindacato giurisdizionale necessario al fine di porre rimedio agli errori». Così Filippi e Cortesi (2004), p. 5.

[89] Corte EDU, sez. I, 27 settembre 2018, *Brazzi c. Italia*.

di venti in costanza della permanenza dei presupposti di legge, precisando che il prolungamento delle operazioni deve essere accordato con decreto del pubblico ministero, nel quale deve essere dato «chiaramente atto dei motivi che rendono necessaria la prosecuzione delle operazioni», ai sensi del comma 2 dell'art. 226 disp. att. c.p.p.

Nessun dubbio di compatibilità con la riserva di legge se il legislatore avesse predisposto, proprio come accade in ambito processuale, un termine di durata massima delle investigazioni preventive; l'assenza di una simile previsione, in aggiunta alla mancanza della fissazione di un numero massimo di proroghe concedibili, rendono concreto il periodo il periodo di una durata sine die delle captazioni *ante delictum*, con evidenti ricadute sul piano della salvaguardia delle libertà fondamentali delle persone sottoposte a simili attività.

Da quanto detto emerge che «il riscontro di legalità nel quale si rifrange la profonda connotazione di garanzia sottesa alla riserva costituzionale di giurisdizione si rivela fittizio»[90]. Nonostante ci siano stati tentativi per "salvare" la disposizione *de qua* sulla base dell'inutilizzabilità degli elementi raccolti in fase preventiva nel processo penale vero e proprio[91], si ritiene inaccettabile acconsentire alla lesione di situazioni soggettive costituzionalmente protette giustificandola con la regola (tra l'altro, sempre più cedevole) dell'esclusione probatoria: la preclusione all'utilizzazione degli esiti operante "a valle" non può far venir meno la lesione dei diritti individuali già realizzata "a monte".

Dunque, «la verità è che il rischio di incidere su diritti fondamentali dell'individuo [in assenza di precisi] confini tracciati dalla legge (costituzionale e ordinaria) è motivo sufficiente perché debbano ritenersi banditi dal processo penale gli strumenti investigativi le cui potenzialità intrusive non siano determinabili *a priori*»[92].

8. Verso il superamento dei poteri investigativi paralleli: prospettive *de jure condendo*.

Una volta affrontate le criticità derivanti dalla compartecipazione di più soggetti all'inchiesta preventiva e analizzati gli inevitabili risvolti processuali che ne derivano, possono trarsi alcune conclusioni che, prendendo le mosse dalla normazione vigente, si spingono fino ad avanzare soluzioni giuridiche inedite.

Senza dubbio la soluzione più immediata ai "mali" del sistema potrebbe essere rappresentata da un intervento normativo del legislatore; una riforma sistematica delle captazioni e dei controlli *ante delictum* sia di polizia che d'*intelligence*, volta alla regolamentazione delle altre forme di sorveglianza "anticipata" che, pur non trovando espressa regolamentazione, vengono ampiamente utilizzate in fase preventiva con inevitabili riflessi sul procedimento probatorio.

Una regolamentazione in forma chiara e compiuta delle intercettazioni e dei controlli preventivi sulle comunicazioni risulterebbe funzionale alla tutela del principio di legalità nonché a conferire certezza al diritto di difesa, in modo da permettere al controllato di avere effettiva cognizione delle modalità di ingerenza degli investigatori alla sfera di riservatezza individuale, valutando la rispondenza dell'attività compiuta rispetto ai limiti individuati dal tenore della disposizione e dal contenuto del decreto autorizzativo.

L'intervento "correttivo" del legislatore non sembra, tuttavia, rappresentare l'unica strada percorribile.

A fonte dei condizionamenti delle attività preventive sul processo penale, si ritiene non solo necessario ridefinire i ruoli tra i diversi protagonisti delle indagini proattive, ma anche propendere per l'istituzione di specifici organi, con competenze riservate alla sola fase preventiva, funzionali a garantire la legittimità dell'esecuzione della procedura esecutiva e, al contempo, evitare forme di contatto "indirette" con il processo penale "puro".

In quest'ottica, si potrebbe paventare la possibilità di attribuire al Procuratore nazionale antimafia e antiterrorismo la legittimazione passiva all'autorizzazione alle captazioni preventive, sottraendola alla procura del luogo in cui sono emerse le esigenze di prevenzione, ovvero al procuratore generale presso la Corte d'appello di Roma.

In effetti, il Procuratore nazionale, pur non godendo di poteri investigativi "puri", è de-

[90] L'espressione appartiene a Pierro (2002), p. 537-538.
[91] Cfr., per tutti, Grevi (1979), p. 104.
[92] Caprioli (2017), p. 501.

putato alla raccolta, elaborazione e gestione del patrimonio informativo relativo alle diverse forme di criminalità organizzata e terrorismo: come rilevato, se da una lato questo assetto consentirebbe allo stesso di detenere un «*background* di conoscenze non solo ai fini della valutazione prognostica sull'"indispensabilità" delle captazioni preventive, ma anche del necessario raccordo […] tra investigazioni in corso e attività di *intelligence*»[93]; dall'altro viene scongiurato il rischio di sovrapposizioni ed interferenze tra organi che sono e devono rimanere separati.

Si supererebbero in tal modo le criticità individuate da chi ritiene violato l'art. 13 Cost. dall'esecuzione di attività autorizzate non da un organo giurisdizionale ma dal p.m., nonché le difficoltà di natura più strettamente operativa, determinate dai possibili condizionamenti investigativi di un organo che, dismessi i panni di "controllore" in fase proattiva, una volta iniziato il procedimento penale dirige le indagini "tradizionali" con un *background* di informazioni che ne condizionano le scelte investigative e, quindi, gli esiti processuali.

Non solo. Al fine di garantire la regolarità della procedura esecutiva, sarebbe auspicabile l'introduzione di un organo centralizzato (una sorta di giudice delle indagini proattive), con una competenza giurisdizionale *ad hoc*, ossia limitata alla sola fase procedimentale, con il compito di verificare la conformità della procedura condotta in fase preventiva rispetto al dettato normativo, sia in relazione alla legittimità del materiale appreso, sia con riguardo alla sussistenza delle condizioni per procedere alle indagini proattive tipizzate.

Al netto delle soluzioni di carattere strettamente pragmatico – volte a sanare le disfunzioni che diramano i lori effetti sul processo penale e sul suo procedimento probatorio – sullo sfondo dei rapporti tra libertà e sicurezza possono trarsi delle conclusioni di carattere sistemico, funzionali a fornire adeguata risposta alla riflessione che ha stimolato la presente ricerca.

Come ormai noto, le intercettazioni preventive e, più in generale, le indagini proattive, sacrificano inevitabilmente le prerogative individuali e, in questi casi, il limite di tollerabilità alla menomazione dei diritti appare ancor più ristretto rispetto a quanto accade a seguito dell'instaurazione del procedimento penale, dal momento che l'interesse contrapposto all'intrusione si mostra evanescente e dai contorni poco chiari e definiti.

Lo studioso, tuttavia, è tenuto a fare i conti con la realtà contingente e deve prendere atto che, pur determinando un'ingerenza al godimento delle prerogative individuali riconosciute nella Carta fondamentale, i risultati ottenibili attraverso l'espletamento delle indagini proattive sono assai efficaci nella prevenzione delle più gravi fattispecie delittuose, per cui non è prospettabile che il sistema penale ne rimanga del tutto privo, essendo preordinate a soddisfare le esigenze di sicurezza collettiva e individuale, altrettanto meritevoli di tutela secondo l'ordinamento costituito.

Ma l'utilità delle investigazioni preventive non può e non deve giustificare ogni forma di violazione ai diritti e alle libertà fondamentali, non potendosi considerare condividibile l'assioma per cui "libertà è sicurezza" e, dunque, «non c'è autentica sicurezza se è limitata ad alcuni ambiti dell'esistenza, cioè se per garantire la propria sicurezza si è obbligati a rinunciare ad alcune libertà»[94]. Anche il diritto del singolo al godimento delle sue prerogative risulta un interesse meritevole di tutela secondo l'ordinamento giuridico e, come tale, ogni individuo deve essere protetto dalla paura di venire ingiustamente privato delle più basiche libertà fondamentali.

Se l'innegabile eterogeneità dell'istituto può comportare un affievolimento di tutela dei diritti fondamentali coinvolti, non può condurre ad uno svuotamento delle garanzie e dei principi cardine dello Stato di diritto, quali quello di legalità, tassatività e determinatezza, sussidiarietà ed *extrema ratio*; principi, questi, che «rappresentano il livello di tutela irrinunciabile al di sotto del quale l'attività di prevenzione non appare più ragionevole e, pertanto, tollerabile[95].

[93] Andolina (2016), p. 569.
[94] Minniti (2018), p. 44.
[95] Malinverni (1972), p. 210.

Bibliografia

Adorno, Rossano (2012): *L'ammissione della prova in dibattimento* (Torino, Giappichelli).

Agostini, Bianca (2017): "La disciplina delle intercettazioni preventive nel sistema antiterrorismo", *Diritto penale contemporaneo – Rivista trimestrale,* 1, pp. 141-148.

Andolina, Elena (2016): "Le intercettazioni e i controlli preventivi sulle comunicazioni nel contrasto al terrorismo internazionale tra irrisolte criticità ed esigenze di riforma", *Archivio della nuova procedura penale,* 6, pp. 568-572.

Balducci, Paola (2002): *Le garanzie nelle intercettazioni tra costituzione e legge ordinaria* (Milano, Giuffrè).

Camon, Alberto (2020): "Il cacciatore di IMSI", *Archivio penale,* 1, pp. 1-20.

Cantone, Raffaele (1996): "Denunce anonime e poteri investigativi del pubblico ministero", *Cassazione penale,* p. 2982-2990.

Cantone, Raffaele e D'Angelo, Luciano (2006): "Una nuova ipotesi di intercettazione preventiva", in Dalia, Andrea Antonio (editor), *Le nuove norme di contrasto al terrorismo* (Milano, Giuffrè), pp. 54-66.

Caprioli, Francesco (2011): "La ricerca della notizia di reato da parte dell'accusatore. Opinioni a confronto", *Criminalia*, p. 437-458.

Caprioli, Francesco (2017): "Il 'captatore informatico' come strumento di ricerca della prova in Italia", *Revista brasileira di Direito Processual Penal*, 2, pp. 483-510.

Cercola, Luca (2016): *Le intercettazioni nella dinamica del processo penale* (Torino, Giappichelli).

Colaiacovo, Guido (2009): "I limiti di operatività delle denunce anonime", *Cassazione penale*, p. 4321-4324.

Curtotti, Donatella (2018): "Procedimento penale e *intelligence* in Italia: un'osmosi inevitabile, ancora orfana di regole", *Processo penale e giustizia,* 3, pp. 438-444.

Curtotti, Donatella (2015): "Operazioni sotto copertura", in Romano, Bruno (editor): *Le associazioni di tipo mafioso* (Torino, Utet), pp. 427-452.

De Caro, Agostino (2000): *Libertà personale e sistema processuale penale* (Napoli, ESI).

Di Bitonto, Maria Lucia (2012): "Terrorismo internazionale. Procedura penale e diritti fondamentali in Italia", *Cassazione penale,* p. 1181.

Di Bitonto, Maria Lucia (2006): "Raccolta di informazioni e attività di *intelligence*", in Kostoris, Roberto E. e Orlandi, Renzo (editor): *Contrasto al terrorismo interno e internazionale* (Torino, Giappichelli), p. 253-264.

European Union Agency for Fundamental Rights (2018): "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU: Mapping Member States' legal frameworks", *www.fra.europa.eu*, pp. 1 ss.

Filippi, Leonardo (2002a): "Intercettazioni telefoniche (diritto processuale penale)", *Enciclopedia del diritto*, VI (Milano, Giuffrè), pp. 565-589.

Filippi, Leonardo (2002b): "Terrorismo internazionale: le nuove norme interne di prevenzione e repressione. Profili processuali", *Diritto penale e processo,* pp. 163-176.

Filippi, Leonardo e Cortesi, Maria Francesca (2004): "Intercettazione preventiva di comunicazioni", *Enciclopedia giuridica,* XII (Roma, Treccani), pp. 1-11.

Garuti, Giulio (2005): "Le intercettazioni preventive nella lotta al terrorismo internazionale", *Diritto penale e processo,* pp. 1457-1461.

Giunchedi, Filippo (2008): "Le attività di prevenzione e di ricerca di intelligence", in Gaito, Alfredo (editor): *La prova penale* (Torino, Utet), p. 3.

Grevi, Vittorio (1979): *La nuova disciplina delle intercettazioni telefoniche* (Milano, Giuffrè).

Grevi, Vittorio (1971): "Intercettazioni telefoniche e principi costituzionali", *Rivista italiana di diritto e procedura penale,* p. 1968-1973.

Kalb, Luigi (2000): *Il documento nel sistema probatorio* (Torino, Giappichelli).

Illuminati, Giulio (1983): *La disciplina processuale delle intercettazioni* (Milano, Giuffrè).

Luparia Donati, Luca (2009): "Computer crimes e procedimento penale", in Spangher, Giorgio (editor): *Trattato di procedura penale* (Torino, Utet) 2009, pp. 475-477.

Maggio, Paola (1990): "Prova documentale", *Enciclopedia giuridica,* XII (Roma, Treccani), pp. 1-30.

Malinverni, Alessandro (1972): *Principi del processo penale* (Torino, Giappichelli).

Mancuso, Enrico Maria (2017): *Il regime probatorio dibattimentale* (Milano, Giuffrè).

Marandola, Antonella (2001): *I registri del pubblico ministero* (Padova, Cedam).

Marinelli, Claudio (2007): *Intercettazioni processuali e nuovi mezzi di ricerca della prova* (Torino, Giappichelli).

Minniti, Marco (2018): *Sicurezza è libertà* (Milano, Rizzoli).

Murro, Ottavia (2022): "Dubbi di legittimità costituzionale e problemi di inquadramento della nuova disciplina dei tabulati", *Cassazione penale,* pp. 2440-2455.

Negri, Daniele (2016): "*La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)", Archivio penale,* 2, pp. 44-54.

Nocerino, Wanda (2021a): "Il tramonto dei mezzi di ricerca della prova nell'era 2.0", *Diritto penale e processo,* pp. 1077-1088.

Nocerino, Wanda (2021b): *Il captatore informatico nelle indagini penali interne e transfrontaliere* (Padova, Cedam).

Nocerino, Wanda (2020): "Il captatore informatico: un Giano bifronte. Prassi operative *vs* risvolti giuridici", *Cassazione penale,* p. 824-851.

Nocerino, Wanda (2019): *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio* (Padova, Cedam).

Orlandi, Renzo (2015): "Il sistema di prevenzione tra esigenze di politica criminale e principi fondamentali", *Criminalia,* pp. 557-559.

Orlandi, Renzo (2010): "Attività di *intelligence* e diritto penale della prevenzione", in Illuminati, Giulio (editor): *Nuovi profili del segreto di Stato e dell'attività di* intelligence (Torino, Giappichelli), p. 227-240.

Orlandi, Renzo (1996): "Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell'*inquisitio generalis*?", *Rivista di diritto e procedura penale,* pp. 583-592.

Pierro, Guido (2002): "Molte ombre nella riforma delle intercettazioni preventive", *Diritto penale e processo,* p. 533-547.

Tonini, Paolo e Conti, Carlotta (2014): *Il diritto delle prove penali* (Milano, Giuffrè).

Zacchè, Francesco (2012): *La prova documentale* (Milano, Giuffrè).

Le inchieste dell'agenzia nazionale per la sicurezza del volo e i limiti all'attività della polizia giudiziaria

Las investigaciones de la Agencia de Seguridad Aeronáutica y los límites a la actividad de la policía judicial

Investigations by the National Agency for Flight Safety and the Limits to the Activity of the Judicial Police

Ottavia Murro
Dottore di ricerca in Diritto e Procedura Penale, Avvocato

Indagini preliminari, Regole probatorie | Investigaciones preliminares, Reglas de la prueba | Pre-Trial Investigation, Rules of evidence

Abstracts

Il contributo analizza il ruolo investigativo dell'Agenzia Nazionale per la Sicurezza del Volo (ANSV), chiamata a svolgere le inchieste di sicurezza sugli incidenti o gravi inconvenienti che vedono coinvolti gli aeromobili dell'aviazione civile. Delineati i tratti generali dell'attività dell'Agenzia, si cercheranno di approfondire i punti di contatto – ovvero di frizione – tra il ruolo degli investigatori dell'ANSV e quello della polizia giudiziaria chiamata ad intervenire sulla scena del crimine, con un nodo finale da sciogliere: quale utilizzo processuale può avere l'attività inchiesta svolta dall'ANSV?

El artículo analiza el rol investigador de la Agencia Nacional de Seguridad Aeronáutica (ANSV, por sus siglas en italiano), encargada de llevar a cabo investigaciones de seguridad en accidentes o incidentes graves en los que se ven implicadas aeronaves civiles. Una vez esbozadas las características generales de la actividad de la Agencia, se examinarán los puntos de contacto -o más bien, de fricción- entre el papel de los investigadores de la ANSV y el de la policía judicial llamada a intervenir en el lugar del delito, con un nudo final por desentrañar: ¿qué utilidad puede tener la actividad investigadora llevada a cabo por la ANSV en el contexto de un procedimiento judicial?

The paper analyzes the investigative role of the National Flight Safety Agency (ANSV), called to carry out safety investigations on accidents or serious incidents involving civil aviation aircraft. Once the general features of the Agency's activity have been outlined, we will try to deepen the points of contact - or friction - between the role of the ANSV investigators and that of the judicial police called to intervene on the crime scene, ultimately aiming to resolve the question: what procedural implications can arise from the investigative activities carried out by ANSV?

Sommario

1. Sicurezza del volo: premessa.

È ormai noto che, con la globalizzazione, gli spostamenti delle persone abbiano assunto un ruolo fondamentale per lo sviluppo economico, culturale e sociale; sicché la velocità dei trasporti ha visto un incremento dell'utilizzo dell'aereo che, nel tempo, è diventato un mezzo di comune utilizzo.

Sicurezza e prevenzione[1] rappresentano così le condizioni fondamentali di esistenza e di sviluppo dell'aviazione civile.

Non a caso, in materia aeronautica, la locuzione "sicurezza"[2] ha un significato ampio e racchiude una duplice funzione: la *safety*, ovvero la necessità di prevenire ogni eventuale incidente colposo, abbassando il rischio ad un livello accettabile; la *security*, intesa come prevenzione da ogni atto volontario ed illecito che pone in pericolo la sicurezza dell'aviazione civile[3]. In relazione al primo profilo va rilevato come la *safety* sia sempre più caratterizzata dall'evoluzione tecnica e, dunque, informatica, meccanica ed ingegneristica, tutte caratteristiche essenziali del trasporto dei velivoli; per tale motivo l'aviazione civile è in constante aggiornamento al fine di garantire la massima sicurezza di ogni volo. Sulla *security*, invece, ha profondamente inciso l'attentato dell'11 settembre 2001 che, per la prima volta nella storia, ha visto l'aeromobile trasformato in uno strumento di guerra terroristica, determinando un incremento costante e sempre più tecnologico di ogni misura di contrasto al terrorismo.

In tale contesto, nel quale appare insito il concetto di rischio, sono stati istituiti, a livello nazionale, diverse organizzazioni preposte alla sicurezza: l'Ente Nazionale Aviazione Civile (ENAC), Autorità di regolazione tecnica, certificazione, vigilanza e controllo nel settore dell'aviazione civile italiana, che ha anche il compito di definire e coordinare le misure di sicurezza del trasporto aereo, svolgendo funzioni sia in tema di *security*, sia di *safety*[4]; l'Ente Nazionale Assistenza al Volo (ENAV), i cui compiti sono l'organizzazione e l'esercizio dei servizi del traffico aereo generale, delle telecomunicazioni ed informazioni aeronautiche, dei servizi meteorologici aeroportuali; nonché della movimentazione degli aeromobili sulle aree di manovra[5].

Sempre in ottica preventiva, al fine di migliorare le condizioni di sicurezza del volo, è stata, altresì, istituita l'Agenzia Nazionale per la Sicurezza del Voli (ANSV) che ha il compito di svolgere le inchieste di sicurezza relative agli incidenti ed agli inconvenienti gravi occorsi ad aeromobili dell'aviazione civile; di identificare le cause degli eventi, di assicurare il miglioramento della sicurezza del volo[6]. Ed è proprio tale Agenzia a destare l'attenzione del giurista, poiché le inchieste di sicurezza, se da un lato rivestono un ruolo fondamentale nella prevenzione degli incidenti, dall'altro pongono non poche problematiche in merito al delicato rapporto tra l'Agenzia e l'autorità giudiziaria.

[1] Pellegrino (2005), p. 171.

[2] Va precisato che a livello normativo non esiste una definizione di sicurezza dell'aviazione civile, sul punto, De Luca (1973), p. 31. Tuttavia, nel provare a definire il concetto di sicurezza aerea - senza alcuna pretesa di esaustività - si può ritenere che questa sia, in via generale, l'insieme di leggi, regolamenti, ordini e procedure, di natura preventiva, aventi lo scopo di contenere i rischi ad un livello accettabile.

[3] Per un approfondimento si rimanda a Comenale Pinto (2005), p. 53; Grigoli (1990), p. 211; Pellegrino (2007), pp. 53-54; Vermiglio (2008), P. 145.

[4] L'ENAC deve anche certificare e controllare le condizioni di sicurezza degli aeromobili; controllare la qualità dei servizi aeroportuali e di trasporto aereo; provvedere alla certificazione del personale di volo e di terra; provvedere al rilascio delle licenze di trasporto passeggeri e merci per le compagnie aeree; provvedere alla certificazione delle ditte di costruzione e manutenzione degli aeromobili. *Sefety* e *Security* sono, dunque, di diretta competenza dell'ENAC. L'ampio spettro di attività affidate all'Ente è strettamente connesso alla circostanza che la sicurezza viene influenzata da almeno tre fattori: uomo, macchina ed ambiente; per un approfondimento, si rimanda a *La sicurezza del volo. La* Security, in www.enac.gov.it; *La sicurezza del volo. La* Sefety, in www.enac.gov.it. Sul ruolo svolto dall'Agenzia, Mastrandrea (2000), p. 533.

[5] Sul tema, Comenale Pinto (2005), p. 107.

[6] Per un approfondimento sulle inchieste di sicurezza, Camarda (1998), pp. 106 ss.; Pozzi (2002), pp. 635 ss. In senso più ampio, Saitta (1970), p. 981.

2. L'ANSV e l'inchiesta di sicurezza: profili generali.

L'Agenzia nazionale per la sicurezza del volo, istituita con il d.lgs. 25 febbraio 1999 n. 66, (successivamente modificato dal DPR 5 ottobre 2010 n. 189) è un'autorità investigativa per la sicurezza dell'aviazione civile; è pubblica, permanente, caratterizzata da ampia autonomia[7] ed indipendenza[8], posta in posizione di terzietà rispetto al sistema dell'aviazione civile e sottoposta alla vigilanza della Presidenza del Consiglio dei Ministri[9].

Le modalità di operare dell'Agenzia sono delineate prevalentemente dall'ordinamento internazionale, ovvero dall'Allegato 13 alla Convenzione relativa all'aviazione civile internazionale[10], nonchè da quello europeo che vede nel Regolamento UE n. 996/2010 (di seguito anche Regolamento) la sua fonte principale[11].

All'ANSV sono demandati specifici compiti che possono essere suddivisi in due macro categorie: a) lo svolgimento, a fini esclusivamente di prevenzione, di inchieste di sicurezza relative agli incidenti e agli inconvenienti occorsi ad aeromobili dell'aviazione civile, emanando, se necessario, le opportune raccomandazioni di sicurezza b) lo svolgimento di attività di studio e di indagine per contribuire al miglioramento della sicurezza del volo.

Va sin da subito precisato che l'inchiesta aeronautica ha quale unico fine la prevenzione e non l'individuazione di colpe o responsabilità[12]; essendo strumentale solo alla realizzazione di un elevato livello di sicurezza. Appare dunque corretto ritenere che la *mission* dell'ANSV sia tutelare «la pubblica incolumità attraverso lo svolgimento di una efficace azione di prevenzione in campo aeronautico»[13]. L'obiettivo è dunque la c.d. *just culture*, concetto rinvenibile nelle fonti sovranazionali[14] e sintetizzabile in quella "cultura nella quale gli operatori di prima linea non vengono puniti per azioni, omissioni o decisioni da essi adottate che siano proporzionali alla loro esperienza ed addestramento, ma nella quale non sono tollerate colpe gravi, violazioni intenzionali o atti dolosi"[15]. Sicché nella logica della generalprevenzione, l'indagine mira a creare futura sicurezza, a prevenire altri errori, ad elaborare modelli di condotta (sempre perfettibili).

Delineata, seppure in via generale, la *mission* dell'Agenzia, bisogna comprendere quali inchieste essa deve o può svolgere, e su quali, invece, non ha alcuna facoltà investigativa.

Le inchieste di sicurezza sono, infatti, disciplinate dall'art. 5 del Regolamento UE n. 996/2010 e si suddividono in obbligatorie e facoltative: le prime attengono agli incidenti aerei o inconvenienti gravi[16] in cui sia coinvolto un aeromobile civile[17]; le seconde a incidenti o

[7] È lo stesso art. 1 del Decreto istitutivo dell'Agenzia che, da un lato, le conferisce "autonomia amministrativa, regolamentare, patrimoniale, contabile e finanziaria" e, dall'altro, ne riconosce l'indipendenza di giudizio e di valutazione".

[8] L'indipendenza non va tuttavia intesa «come mancata soggezione all'indirizzo politico-amministrativo dello Stato», poiché essa è da intendersi come una potestà decisionale e operativa autonoma, sganciata da altri poteri pubblici, ma non come potere di autogoverno, sul punto, Pellegrino (2005), p. 170.

[9] Diversamente da quanto accade per le altre istituzioni aeronautiche, quali ENAC ed ENAV, che invece sono sotto il controllo del Ministero dei trasporti.

[10] Meglio noto come Allegato 13 ICAO "*Air Accident and Incident Investigation*".

[11] Va precisato che l'ANSV, essendo tenuta all'osservanza della normativa internazionale e UE in materia di inchieste di sicurezza, è soggetta, periodicamente, ad attività di verifica dei propri standard e delle proprie prassi investigative, sia sotto forma di *audit*, sia sotto forma di *peer review*; sul punto *Rapporto informativo sull'attività svolta dall'ANSV e sulla sicurezza dell'aviazione civile in Italia anno 2021*, in ansv.it, p. 7.

[12] Sul punto, Franchi (2013), p. 390. Inoltre, il Regolamento UE 996/2010 dà la seguente definizione di inchiesta di sicurezza: «un insieme di operazioni svolte da un'autorità investigativa per la sicurezza ai fini della prevenzione degli incidenti ed inconvenienti che comprende la raccolta e l'analisi di dati, l'elaborazione di conclusioni, la determinazione della causa o delle cause e/o di fattori concorrenti e, ove opportuno, la formulazione di raccomandazioni in materia di sicurezza». Per un approfondimento della natura delle inchieste si rimanda a Antonini (1997), pp. 51 ss.

[13] Così, *Rapporto informativo sull'attività svolta dall'ANSV*, cit., p. 8.

[14] Il concetto di *just culture* è stato formalizzato da ICAO (*International Civil Aviation Organization*), agenzia specializzata della Nazioni Unite per il trasporto aereo, nonché successivamente recepito nel Regolamento UE n. 691/2010.

[15] Così, Dekker (2012), p. 72. L'espressione è anche ripresa da Ferro (2015), p. 58.

[16] Per le definizioni complete di "incidente", "inconveniente grave" e "inconveniente" si rimanda al Regolamento UE n. 996/2010; tuttavia, in via generale, per "incidente" (*accident*), si intende un evento nel quale una persona riporti lesioni gravi o mortali; ovvero l'aeromobile riporti un danno o un'avaria che comprometta la resistenza strutturale, le prestazioni o le caratteristiche di volo dell'aeromobile e richieda generalmente una riparazione importante o la sostituzione dell'elemento danneggiato; l'aeromobile sia scomparso o sia completamente inaccessibile. Per "inconveniente grave" (*serious incident*) si intende un evento le cui circostanze rivelino che esisteva un'alta probabilità che si verificasse un incidente. Per "inconveniente" (*incident*) si intende un evento, diverso da un incidente, che pregiudichi o possa pregiudicare la sicurezza delle operazioni. Per un'analisi approfondita si rimanda a *Rapporto informativo sull'attività svolta dall'ANSV*, cit., p. 7. A livello definitorio un'importante novità attiene all'inclusione degli aeromobili a pilotaggio remoto negli oggetti di investigazione da parte dell'Agenzia, allorquando si verifichi un incidente o inconveniente grave. Sussiste così l'obbligo di inchiesta di sicurezza - in ottica di prevenzione - anche per questi mezzi e ciò in considerazione del crescente loro impiego; sul punto, Franchi (2010), pp. 1213 - 1232.

[17] In materia di obbligatorietà di svolgimento dell'inchiesta di sicurezza, l'art. 5 del Regolamento UE 2018/113914 introduce una importante

inconvenienti gravi nei quali siano coinvolti altri tipi di aeromobili, purché l'inchiesta sia utile in termini di prevenzione e per trarre insegnamenti sul piano della sicurezza. Sussiste invece l'incompetenza ad investigare relativamente ad incidenti o inconvenienti gravi occorsi ad aeromobili militari o di Stato (art. 3, comma 1, D. Lgs. 25 febbraio 1999, n. 66).

Merita di essere segnalata anche la deroga all'obbligo di investigare, introdotta per ridurre il numero di inchieste di sicurezza su eventi che, in un'ottica di prevenzione, appaiono meno significativi, al fine di consentire all'Agenzia di concentrare le risorse sugli incidenti o inconvenienti gravi la cui comprensione consenta di migliorare sensibilmente i livelli di sicurezza del volo. Più precisamente, l'agenzia può, discrezionalmente, decidere di non investigare su incidenti o inconvenienti gravi nei quali sia coinvolto, ad esempio, un aeromobile senza equipaggio; ovvero qualora nell'incidente/inconveniente grave sia coinvolto un aeromobile con equipaggio con una massa massima al decollo uguale o inferiore a 2250 kg[18].

Va comunque precisato come tutte le inchieste si devono concludere con la predisposizione di una relazione finale che deve essere resa pubblica nel più breve tempo possibile, auspicabilmente entro dodici mesi dall'accadimento dell'evento (termine ordinatorio)[19]. Nel caso il suddetto termine non possa essere rispettato, l'autorità investigativa è tenuta a pubblicare una dichiarazione almeno ad ogni anniversario dell'evento.

Delineate le caratteristiche generali dell'inchiesta di sicurezza, pare opportuno spostare l'attenzione sulle attività investigative che può svolgere l'Agenzia e sui punti di connessione con le indagini penali, al fine di volgere poi lo sguardo verso l'utilizzo dell'inchiesta di sicurezza nell'eventuale giudizio penale.

3. L'attività investigativa di sicurezza e la protezione delle prove: il ruolo dell'ANSV.

L'Agenzia, al fine di espletare al meglio le sue funzioni, ha specifiche prerogative finalizzate all'acquisizione degli elementi di prova necessari alla sua inchiesta; non a caso il "*considerando*" n. 21 del Regolamento UE n. 996/2010 precisa che "l'inchiesta di sicurezza è efficiente solo se gli elementi di prova importanti sono adeguatamente conservati".

Nel dettaglio, l'investigatore incaricato gode di un ventaglio di poteri declinati preliminarmente dall'art. 11 del Regolamento suddetto e che spaziano dall'accesso ai luoghi e all'aeromobile senza restrizioni, né ostacoli; al rilevamento e recupero delle prove per effettuare esami ed analisi; all'accesso immediato ai registratori di volo e a qualsiasi altra registrazione pertinente; alla facoltà di chiedere l'autopsia anche quando l'autorità giudiziaria non la deve disporre[20]; all'accesso ai risultati autoptici e ad ogni altro campione prelevato; sino alla possi-

novità rispetto all'art. 4, comma 1, della Direttiva CE 94/56 ed all'art. 826 cod. nav., che prevedevano che tutti gli incidenti e tutti gli inconvenienti gravi occorsi ad aeromobili dell'aviazione civile fossero oggetto di inchiesta da parte dell'autorità investigativa per la sicurezza dell'aviazione civile.

[18] Oggi, «è venuto meno l'obbligo di svolgere un'inchiesta di sicurezza per gli incidenti e per gli inconvenienti gravi occorsi alle seguenti categorie di aeromobili: aeromobili storici non complessi progettati prima del 1 o gennaio 1955 e la cui produzione sia cessata prima del 1 o gennaio 1975 oppure aeromobili di chiaro interesse storico; aeromobili specificatamente progettati o modificati per scopi di ricerca, sperimentazione o scientifici e suscettibili di essere prodotti in un numero molto limitato; aeromobili autocostruiti per fini di uso proprio e senza obiettivi commerciali; aeromobili che siano stati in servizio presso forze armate; mezzi con una massa massima al decollo non superiore ad un determinato peso indicato espressamente nel predetto allegato II; aeromobili a pilotaggio remoto con massa operativa non superiore a 150 chilogrammi»; così Franchi (2013), pp. 391 ss.; Id. (1997), pp. 39 - 44. In ogni caso, gli incidenti o i gravi inconvenienti vanno comunicati all'Agenzia e sono obbligati alla comunicazione le persone coinvolte, nonché all'ENAC, all'autorità di pubblica sicurezza e ad ogni altra pubblica autorità. Per persona coinvolta si intende il proprietario, un membro dell'equipaggio, l'esercente dell'aeromobile coinvolti in un incidente o inconveniente grave; qualsiasi persona coinvolta nella manutenzione, nella progettazione, nella costruzione dell'aeromobile, nell'addestramento del suo equipaggio; qualsiasi persona coinvolta nelle attività di controllo del traffico aereo, nelle informazioni di volo, nei servizi aeroportuali, che abbia fornito servizi per l'aeromobile; il personale dell'autorità nazionale dell'aviazione civile; il personale dell'AESA (art. 2 Regolamento).

[19] La previgente normativa distingueva tra relazione di inchiesta (in caso di incidente) e rapporto di inchiesta (in caso di inconveniente grave), prevedendo la massima diffusione delle relazioni ed una diffusione controllata dei rapporti (artt. 7 e 8 Direttiva CE 94/56, ripresi dall'art. 12, d.lgs. n. 66/1999). Oggi, invece, vi è un'unica tipologia di atto che prescinde dall'evento oggetto di indagine.

[20] In merito all'esame autoptico è utile richiamare la nota del Ministero della Giustizia con cui si è dato un positivo riscontro alla raccomandazione di sicurezza dell'ANSV n. 18/1546-08/2/A/09, che chiedeva di sensibilizzare tutte le Procure della Repubblica sulla necessità che, in caso di piloti deceduti in incidenti aerei, la relativa sepoltura non sia eseguita prima di aver sentito l'Agenzia nazionale per la sicurezza del volo. In particolare, l'ANSV auspica che la competente autorità giudiziaria disponga l'autopsia sui corpi dei piloti deceduti tutte le volte in cui tale accertamento appare assolutamente necessario per il regolare svolgimento dell'inchiesta tecnica. Il Ministero della giustizia ha così indirizzato una nota ai Procuratori generali presso le Corti di appello, precisando che "*laddove l'autorità giudiziaria ritenga che non sussistano le condizioni*

bilità di convocare ed ascoltare i testimoni.

Si delinea così un ampio spettro di poteri investigativi dell'Agenzia, la quale gode di un immediato ed incondizionato accesso alle fonti di prova, in cui il dominio dell'autorità giudiziaria sulla scena del crimine e sugli elementi di prova pare scontrarsi - e dunque sbiadire - innanzi all'equiparazione dell'indagine di sicurezza con quella giudiziaria[21].

Più nel dettaglio, gli investigatori dell'ANSV hanno dei veri e propri poteri investigativi che - di regola - sono di appannaggio della polizia giudiziaria (accertamenti urgenti, ispezioni, perquisizioni, audizione delle persone informate). Ed appare di tutta evidenza la profonda distinzione, in merito alle garanzie, tra gli atti svolti dagli investigatori dell'Agenzia e quelli, invece, svolti dall'autorità giudiziaria. Evidenti appaiono, infatti, le ricadute sul diritto di difesa dell'indagato, quantomeno in merito alla disciplina degli avvisi, alla facoltà di nominare il difensore e al diritto al silenzio.

Nel contempo, in tema di protezione delle prove, l'art. 13 del Regolamento, al fine di stabilire un equilibrio (o meglio una gerarchia) tra i diversi corpi investigativi - dispone che nessuno, prima dell'arrivo degli investigatori, possa modificare lo stato del luogo dell'incidente, prelevare campioni, intraprendere movimenti o effettuare campionamenti dell'aeromobile, del suo contenuto o del suo relitto[22].

In questa sede, e sempre in relazione all'attività investigativa, non si può tralasciare un ulteriore profilo: trattandosi di indagini a forte caratura specialistica, gli accertamenti tecnici possano costituire una prassi, piuttosto che un'eccezione. Sicché l'art. 12 del Regolamento disciplina, in via generale, quantomeno la facoltà di svolgere esami o analisi che possono modificare, alterare o distruggere, gli elementi di prova, prevedendo - a tal fine - la necessità di un preventivo accordo con l'autorità giudiziaria per garantire la cooperazione tra tutti i soggetti chiamati ad operare (*infra* par. 4).

In tale contesto emerge, tuttavia, la criticità connessa alla necessità di corredare rilievi ed accertamenti a rigorose regole di cautela, qui del tutto assenti e non contemplate neanche negli accordi con le procure (*infra* par. 4). E', infatti, ormai noto come tali attività plasmano e condizionano i successivi accertamenti e rappresentano una fase investigativa di estrema delicatezza, in quanto assicurano le fonti di prova al futuro processo[23]; sicché l'Agenzia gode di plurimi strumenti di indagine che rappresentano, ed è inutile negarlo, la più efficace tecnica di accertamento del fatto che viene utilizzata con ampiezza di poteri, in una disinvolta discrezionalità e con evidente riduzione (*rectius* annullamento) dei diritti difensivi dell'indagato. Non stupisce, infatti, come mai nel Regolamento sia nominato il "difensore" che, nel nostro codice, risulta invece protagonista insieme all'accusa e, con l'introduzione della L. 397/2000, può difendere anche "ricercando" le prove. Per comprendere l'entità del problema, e non potendo in tale sede affrontarlo in modo approfondito, basti precisare che le indagini difensive non sono contemplate dal Regolamento, né dagli accordi con le procure, apparendo dunque negato (o reso estremamente difficile) ogni spazio all'indagine tecnica del difensore.

In tale quadro normativo, sembrano delinearsi le prime collisioni ed interferenze tra il Regolamento UE n. 966/2010 e le regole del codice di rito. In particolare, si pensi agli obblighi di informazione gravanti sul pubblico ministero ma, di converso, non previsti in caso di inchiesta di sicurezza, che prosegue senza assicurare alcuna garanzia all'indagato, con il conseguente e concreto rischio di una trasmigrazione degli atti di inchiesta, viziati in punto di garanzie, nel fascicolo per il dibattimento (*infra* par. 5).

di legge per disporre l'autopsia sul cadavere di persona deceduta in seguito ad incidente aereo, appare comunque necessario porre la salma a disposizione dell'Agenzia nazionale per la sicurezza del volo, affinché quest'ultima possa procedere in via amministrativa, in esecuzione dell'obbligo gravante sullo Stato italiano (in virtù di quanto previsto dal citato Allegato 13 alla Convenzione relativa all'aviazione civile internazionale); in ansv.it.

[21] Non a caso, e proprio a ribadire una pari dignità tra investigatori e inquirenti, l'art. 11 del Regolamento UE n. 966/2010 sottolinea l'indipendenza di chi partecipa alle inchieste di sicurezza che "non accetta istruzioni da persone diverse dall'investigatore incaricato o dal rappresentante accreditato".

[22] Le uniche manovre consentite sono strettamente connesse a ragioni di sicurezza o per assistere persone ferite; in tal caso è necessaria una previa autorizzazione esplicita delle autorità responsabili del sito e, ove possibile, in consultazione con la stessa autorità investigativa per la sicurezza. Invero, già prima dell'entrata in vigore del Regolamento UE 966/2010, il Ministero della giustizia aveva trasmesso ai Procuratori Generali presso le Corti d'Appello la nota «*m_dg.DAG.30/01/2008.0014513*» , con la quale lo stesso Ministero invitava ad evitare, nel caso di un incidente aereo e nell'immediatezza successiva all'evento, compatibilmente con le azioni di primo soccorso e salvataggio, manomissioni o alterazioni delle evidenze prima dell'arrivo degli investigatori dell'ANSV, al fine di non compromettere l'acquisizione degli elementi necessari all'accertamento delle cause; sul tema Franchi (2013), p. 392.

[23] Ampiamente sul tema, Curtotti (2013), pp. 7 e ss., L'A. evidenzia come l'atto tecnico di indagine, quale antecedente della c.d. prova tecnica, richiede anche particolari competenze tecniche-scientifiche e la necessità di esperti. Sul tema, tra i tanti, anche Conti (2013), pp. 87 ss.; Felicioni (2012), *passim*; Giunchedi (2009), *passim*; Spangher (2013), pp. 1 - 3.

Ma i segmenti in collisione appaiono plurimi, come quello tra gli accertamenti urgenti di cui all'art. 11 del Regolamento e all'art. 354 c.p.p. ove quest'ultimo prevede che le tracce e le cose pertinenti al reato siano curate dall'autorità giudiziaria. Il Regolamento, invece, riconosce medesimi diritti agli investigatori dell'ANSV, conferendo a questi un potere non solo speculare, ma anche sovraordinato, rispetto a quello che l'ordinamento giuridico italiano attribuisce al pubblico ministero e alla polizia giudiziaria.

Si tratteggia così il perimento della questione: nessun dubbio che la norma europea - in caso di incidenti o gravi inconvenienti aerei - ridimensioni il potere dell'autorità giudiziaria, la quale non può assumere alcuna decisione che vada a compromettere il corretto svolgimento delle inchieste di sicurezza[24]. Di qui, però, la necessità di comprendere come le due forze investigative si devono coordinare tra di loro nel rispetto di un giusto ed auspicabile equilibrio tra esigenze di prevenzione ed esigenze di giustizia; il tutto sotto la rigida convinzione che il Regolamento non è stato scritto pensando alle esigenze di una indagine penale, né è stato stilato per tutelare eventuali diritti dell'indagato (persona fisica o ente), ma - in un'ottica di sicurezza - viene strutturato al sol fine di agevolare tutte le attività tecniche degli investigatori dell'aeronautica civile, affinché siano individuate, nel minor tempo possibile, le cause dell'incidente o del grave inconveniente, prevenendone così la ripetizione.

4. Il coordinamento tra inchiesta ed indagine: l'art. 12 del Regolamento UE n. 966/2010.

Prima dell'entrata in vigore del Regolamento le attività delle autorità investigative per la sicurezza dell'aviazione civile risultavano inibite e compresse dall'autorità giudiziaria, essendo a queste subordinate. Le criticità del rapporto tra l'inchiesta di sicurezza e quella penale sono diventate, così, una parte essenziale del Regolamento che ha creato un nuovo equilibrio tra i diversi piani di indagine.

È emblematico come già nei "considerando" (nn. 20 e 23) si faccia un esplicito riferimento al rapporto tra le due autorità investigative, garantendo, sin da subito, all'Agenzia la possibilità di svolgere i suoi compiti nelle migliori condizioni possibili, con accesso immediato e illimitato alla scena del crimine, con conseguente messa a disposizione di tutti gli elementi necessari per soddisfare le esigenze dell'inchiesta di sicurezza, senza tuttavia compromettere gli obiettivi dell'inchiesta giudiziaria ("considerando" n. 20). Nel contempo, stante una sovrapposizione di attività di indagine, il "considerando" n. 23 definisce il punto di equilibrio tra i vari interessi contrapposti (prevenzione di incidenti futuri e buona amministrazione della giustizia), decretando senza indugi come l'interesse pubblico generale veda nella sicurezza la sua massima esplicazione.

E se la terminologia gioca un ruolo importante nel comprendere la *ratio* sottesa ad un dettato normativo, non sfugge come l'art. 11 del Regolamento, nel disciplinare i poteri degli investigatori dell'aeronautica, ripete - in relazione all'operato di questi - parole come "*immediatamente*"; "*senza restrizioni*", "*senza ostacoli*", sottolineando come ogni possibile compressione e limitazione sull'inchiesta di sicurezza può, in potenza, comprometterne l'esito, con conseguenze drammatiche per la sicurezza.

Onde evitare una collisione tra le due attività di indagine, l'art. 12 del Regolamento introduce il c.d. accordo tra investigatori per la sicurezza e autorità giudiziaria. La norma, al fine di garantire che l'indagine tecnica sia condotta con diligenza ed efficienza, prevede che l'accordo preliminare disciplini precise attività di ricerca della prova e segnatamente a) l'accesso al luogo dell'incidente; b) la conservazione delle prove e l'accesso alle stesse; c) i resoconti iniziali sullo stato di ciascuna operazione; d) gli scambi d'informazioni; e) l'utilizzo appropriato delle informazioni di sicurezza. Infine, tali accordi disciplinano anche le modalità di risoluzione dei conflitti tra i due corpi investigativi.

Due le doverose precisazioni: tali accordi non sono consequenziali all'evento, bensì già predefiniti rispetto al verificarsi di qualsiasi possibile accadimento oggetto di inchiesta di sicurezza. Essi sono di portata generale e rappresentano un preciso punto di riferimento per le condotte da seguire. Il fine di tali accordi (che, come vedremo, ha dato origine ai protocolli

[24] Sul punto, Franchi (2013), p. 393.

tra le Procure e l'Agenzia) è quello di garantire coordinamento tra investigatori e inquirenti e, nel contempo, rappresenta un punto di riferimento a cui richiamarsi in caso di problematiche concrete[25].

E se l'auspicio è la cooperazione, l'art. 12 del Regolamento non si esime dal rimarcare che il conflitto di competenze vede sempre una sovrapposizione di piani investigativi ove, tuttavia, l'Agenzia appare essere sovraordinata rispetto alla polizia giudiziaria Nello specifico, nell'ipotesi in cui si debba procedere con accertamenti tecnici non ripetibili sui registratori di volo (c.d. scatola nera) e non si sia ottenuto l'accordo preliminare entro un termine ragionevole (non superiore alle due settimane successive alla richiesta), l'investigatore incaricato può liberamente effettuare esami, analisi e quant'altro sia utile alla conservazione degli elementi probatori. Tale disposizione è l'esempio concreto della supremazia delle esigenze di sicurezza e di prevenzione su quelle di giustizia.

Emerge anche la soccombenza delle norme del codice di rito rispetto a quelle del Regolamento, fonte normativa primaria direttamente applicabile. Non a caso, proprio per l'immediata obbligatorietà e diretta applicabilità del regolamento comunitario[26], l'ANSV ha sottoscritto gli accordi preliminari[27] con tutte le Procure della Repubblica presso i Tribunali ordinari[28] e presso i Tribunali per i minorenni. Si è assistito così alla trasposizione, in specifici protocolli, delle norme contenute nel Regolamento; più nel dettaglio, gli accordi tratteggiano la cooperazione e la collaborazione tra i due poteri investigativi, indicando regole, procedure e modalità per lo svolgimento degli atti nel pieno rispetto della normativa europea.

Appare così opportuno delineare i tratti salienti degli accordi tra Procure e ANSV che ricalcano la Circolare del 7 marzo 2013 del Ministero della Giustizia[29], anch'essa ispirata al principio di massima collaborazione possibile tra Autorità Giudiziaria e incaricati dell'Agenzia e finalizzata a rendere immediatamente operativo il Regolamento.

Il primo aspetto disciplinato nei protocolli attiene alla comunicazione di apertura di inchiesta, onerando, così, sia il pubblico ministero, sia l'Agenzia di comunicare all'altro corpo investigativo l'apertura di un'indagine, ovvero di una inchiesta. Lo scambio di tale informazione consente l'inizio delle distinte attività di indagine che potremmo definire parallele, indipendenti ed autonome.

Dalla lettura dei protocolli, si evince l'importanza che si riserva alla fase di analisi della scena del crimine e all'acquisizione degli elementi di prova; non a caso si disciplinano sia l'accesso ai luoghi, sia la preservazione degli stessi, nonché gli accertamenti tecnici irripetibili, l'analisi dei registratori di volo, gli esami autoptici e la conservazione degli elementi di prova.

E dunque, nell'immediatezza dell'evento, la zona deve essere delimitata e vigilata consentendo l'ingresso ai soli mezzi di soccorso e alle sole autorità investigative. Ed è proprio in relazione a tale ultimo aspetto che bisogna sottolineare come la polizia giudiziaria, seppure può accedere ai luoghi ed effettuare i primi rilievi ed accertamenti urgenti, non può svolgere alcune attività di ricerca della prova che possa manomettere, modificare, rimuovere o alterare le evidenze, fino al momento in cui gli agenti dell'ANSV non arrivano sulla scena del crimine. Sono, infatti, quest'ultimi a coordinare le suddette operazioni.

La cooperazione tra autorità investigative sembra cedere il posto, dunque, ad una vera e propria inibizione dei poteri della polizia giudiziaria che è chiamata ad operare con un ruolo - quantomeno nella fase di preservazione dello stato dei luoghi - subordinato rispetto agli investigatori tecnici.

Sia la polizia giudiziaria (coordinata dal p.m.), sia gli investigatori dell'Agenzia, possono accedere al luogo dell'incidente, tuttavia, mentre per i primi i protocolli si limitano a garantire

[25] Nel 2014 l'ANSV e il Ministero della giustizia hanno definito lo schema di accordo preliminare *ex* art. 12, paragrafo 3, Regolamento UE n. 996/201016, finalizzato a favorire il coordinamento tra l'ANSV e l'autorità giudiziaria nel caso in cui, sul medesimo evento, siano avviate sia l'inchiesta di sicurezza, sia l'indagine penale. L'accordo in questione, dopo aver riaffermato il principio secondo cui l'indagine penale dell'autorità giudiziaria e l'inchiesta di sicurezza dell'ANSV sono autonome l'una rispetto all'altra, punta ad agevolare la cooperazione tra la stessa autorità giudiziaria e gli investigatori dell'ANSV e di consentire a questi ultimi di svolgere puntualmente ed efficacemente i propri compiti anche quando siano in corso indagini penali. Sul punto, *Rapporto informativo sull'attività svolta dall'ANSV - Anno 2020*, cit. p. 11 ss.

[26] Sui regolamenti europei e sulla diretta applicabilità, Adam e Tizzano (2010), p. 143.

[27] Va rilevato come il testo di tutti gli accordi sottoscritti dall'ANSV con l'autorità giudiziaria sia identico a quello dell'accordo preliminare tipo originariamente predisposto dall'ANSV e dal Ministero della giustizia.

[28] Originariamente le Procure della Repubblica presso i Tribunali ordinari erano 153, scese poi a 140 a seguito della soppressione di numerosi uffici giudiziari all'esito della complessa procedura di revisione delle circoscrizioni giudiziarie, attuata, da ultimo, con il decreto legislativo 19 febbraio 2014 n. 14. L'ANSV nel 2015 completava tutte le sottoscrizioni con le Procure; *Rapporto informativo sull'attività svolta dall'ANSV - Anno 2020*, cit. p. 12.

[29] Ampiamente sulla Circolare, Paciaroni (2015), p 61.

l'esercizio di tale facoltà, per i secondi si sottolinea, in armonia con le disposizioni del Regolamento, la possibilità di accesso immediato e libero alla scena del crimine. Trapela, tra le righe dei protocolli, la possibilità riservata agli investigatori dell'ANSV di procedere ai primi accertamenti senza dover neanche attendere l'arrivo o l'autorizzazione dell'autorità giudiziaria.

Nel volgere lo sguardo alla conservazione dei beni oggetto di sequestro, si rimarca come questa viene concordata dal pubblico ministero con l'ANSV in merito alle modalità e al luogo, al fine di garantire una corretta catena di custodia, permettendo agli investigatori di sicurezza di accedere al luogo di custodia per svolgere tutte le attività necessarie allo svolgimento dell'inchiesta. In tal caso, vi è la facoltà - ma non l'obbligo - per l'autorità giudiziaria di nominare un ufficiale di p.g. che possa assistere all'accesso degli investigatori al luogo di custodia.

Inutile rimarcare come la principale differenza tra i due corpi investigativi si annida nell'applicabilità delle regole e delle garanzie del codice di rito solo alla polizia giudiziaria, decretando di converso un *vulnus* di tutele nell'attività paritetica svolta dagli investigatori.

Peculiare è il sequestro del registratore di volo che, tra tutti gli elementi probatori, è sicuramente quello più importante ai fini della ricostruzione dell'incidente. Questo, infatti, viene preso in consegna non già dalla polizia giudiziaria, bensì dall'ANSV che, solo nell'ipotesi in cui deve svolgere accertamenti tecnici irripetibili, informa il pubblico ministero che procede nel rispetto delle norme del codice di rito. Ed è questo l'unico accertamento che vede operare le regole del codice di procedura penale, pena l'inutilizzabilità dei risultati nel processo.

Infatti, gli accertamenti tecnici irripetibili prevedono un accordo tra i due corpi investigativi solo in merito alle procedure tecniche da utilizzare, al fine di non alterare o disperdere materiale probatorio[30]. Nel caso in cui la persona indagata formuli richiesta di incidente probatorio, viene informato l'ANSV che ha facoltà di partecipare ed avere copia degli esiti dello stesso.

Infine, nell'ipotesi in cui non sussistano le condizioni di cui all'art. 116 disp. att. c.p.p. e il pubblico ministero non dispone l'autopsia, l'ANSV può chiedere di procedere a tale esame in via amministrativa.

Nel quadro delineato emerge come le due inchieste, seppure tra loro intersecate, siano indipendenti, ciascuna finalizzata a soddisfare le proprie esigenze e gli estesi poteri dell'Agenzia, nonostante determinano delle interferenze con alcune norme del codice di rito, risultano àncorati alla superiorità della fonte normativa (il Regolamento), linea di indirizzo alla quale l'autorità giudiziaria non può non uniformarsi. Sul piano investigativo si può, così, ritenere che le esigenze di giustizia sono state subordinate a quelle di prevenzione poiché, nel bilanciamento dei diversi interessi in gioco, risulta sempre preminente l'interesse pubblico generale.

5. La spendibilità dell'inchiesta nel giudizio: dubbi, criticità, prospettive.

L'analisi fin qui condotta sembra condurci al successivo segmento procedimentale: il dibattimento. La questione è, infatti, connessa all'uso processuale dell'inchiesta tecnica, all'efficacia probatoria dei dati acquisiti, al valore ai fini del libero convincimento del giudice, all'utilizzo ai fini decisori[31]. Questione resa ancor più spinosa a causa dalla soccombenza - sopra delineata - delle norme del codice di rito sotto il peso del Regolamento, con la conseguente assenza (anche nei protocolli) di una disciplina finalizzata a garantire l'osservanza delle norme codicistiche ogniqualvolta sia prevedibile che da un determinato accertamento possa profilarsi l'esistenza di un reato[32].

Preliminarmente, va segnalata l'assenza di rimandi alla disciplina degli artt. 220 e 223 norme cord. c.p.p., *vulnus* che segna una netta distinzione tra gli atti degli investigatori di sicurezza e quelli di investigazione penale, circostanza che determina l'impossibilità di assoggettare gli atti dell'inchiesta di sicurezza alle norme del codice di rito e dunque, ad esempio, al regime delle invalidità. Né vi è una distinzione tra le attività compiute prima e quelle effettuate dopo l'individuazione degli indizi di reato, con il rischio che l'inchiesta possa divenire un *escamotage*

[30] Nel caso in cui non si raggiunga un accordo la composizione del conflitto viene disciplinata dal protocollo stipulato con la Procura di riferimento, ove di regola si prevede che la risoluzione del contrasto sia demandata ad un immediato incontro tra Procuratore della Repubblica e Presidente ANSV, *ex multis,* Protocollo ANSV e Procura di Modena del 12.05.2015.
[31] In argomenti, tra i tanti, Ubertis (2016), pp. 1192 ss.
[32] Sul punto si rimanda a *Osservazioni Governo prog. prel. norme cord. c.p.p.*, in *Doc. giust.*, 1990, p. 205.

per ottenere elementi probatori al di fuori delle garanzie difensive di regola previste.

Sorge così il problema dell'acquisizione al fascicolo per il dibattimento della relazione di sicurezza e degli atti di inchiesta, documenti extraprocessuali che - in assenza di consenso - possono confluire solo attraverso la testimonianza dell'investigatore[33]. Ma anche in relazione a tale mezzo di prova, si annida il problema dell'inapplicabilità del divieto di testimonianza indiretta all'investigatore[34] che può riferire su quanto acquisito persino dal soggetto dapprima coinvolto dell'incidente e poi imputato nel processo penale[35], il tutto in assenza di garanzie.

Inoltre, in merito all'attività svolta dagli investigatori tecnici, una domanda sorge spontanea: l'efficacia probatoria di rilievi, accertamenti tecnici, esami, analisi, svolte dagli investigatori in piena autonomia e senza assicurare alcuna garanzia non è forse - *ab origine* - viziata dalla violazione dell'art. 24 Cost.? Infatti, tutte queste attività non prevedono alcun avviso al soggetto interessato e sono svolte in assenza di ogni garanzia prevista dal codice di rito.

Sotto altro aspetto, appare difficile sostenere come i risultati dell'inchiesta di sicurezza – seppure estranei al processo penale per presupposti e finalità – debbano essere completamente trascurati nel processo penale anche quando appaiono utili per la ricostruzione dell'evento e l'individuazione di responsabilità.

Così, se prima dell'entrata in vigore del Regolamento sussisteva un problema di coordinamento ed equilibrio tra inchiesta ed indagine, oggi si dovrebbe spostare il *focus* sull'utilizzabilità o meno degli atti dell'inchiesta. Nello specifico, appare sicuramente non sostenibile decretare da un lato la netta autonomia ed indipendenza tra le due attività di indagine e, poi, dall'altro, consentire una osmosi tra atti aventi non solo diverse finalità (preventive *vs* giudiziarie), ma soprattutto una diversa disciplina in merito a garanzie e divieti di utilizzo.

E se l'ANSV non è (né può essere considerata) una sezione specializzata di polizia giudiziaria[36], la sua attività, che a monte è mantenuta rigorosamente separata da quella dell'indagine penale, andrebbe distinta anche in sede processuale, con la rigida - ma inevitabile - conseguenza di dichiarare l'inutilizzabilità di tutti gli atti svolti in violazione delle garanzie del codice di rito.

Bibliografia

Pellegrino, Francesca (2005): "La definizione di sicurezza aerea", in "Atti del convegno Aeroporti e Responsabilità, - I.S.D.I.T., Cagliari, 24-25 ottobre 2003" (Cagliari, AV), pp. 171 - 185.

Pellegrino, Francesca (2007): *Sicurezza e prevenzione degli incidenti aeronautici. Nella normativa internazionale, comunitaria e interna* (Milano, Giuffrè).

De Luca, Lamberto (1973): *Incidenti aerei e sicurezza del volo* (Roma, Tipografia Carpentieri).

Comenale Pinto, Michele (2005): "I profili di *security* e le interrelazioni con le normative di *safety*", Camarda, Guido, Cottone, Marco, Migliarotti, Monica (editor): *La sicurezza negli aeroporti, problematiche giuridiche ed interdisciplinari*, Atti del Convegno Milano, 22 aprile 2004 (Milano, Giuffrè), pp. 46 – 62.

Grigoli, Michele (1990): *Il problema della sicurezza della sfera nautica* (Milano Giuffrè).

Vermiglio, Giuseppe (2008): "Sicurezza: *safety*, *security* e sviluppo sostenibile", Tranquilli Leali, Rita e Rosafio, Elisabetta (editor): *Sicurezza, navigazione e trasporto* (Milano, Giuffrè), pp. 145 – 154.

Fanara, Elio (2000): *La nuova disciplina del trasporto aereo* (Messina, Cust).

[33] Zacchè (2012), *passim*.
[34] Ampiamente, sulla questione circa l'utilizzabilità di atti amministrativi nel processo penale, Rampioni (2019), pp. 232 ss; Orlandi (1992), *passim*.
[35] Sul tema, Clivio (2015), pp. 48 - 49.
[36] La "provocazione" è di Clivio, (2015), p. 51.

Camarda, Guido (1998): "Le inchieste sui sinistri aeronautici", in *Diritto pratico aviazione civile*, pp. 106 - 118.

Pozzi, Cristina (2002): "Incontro di studio "L'Agenzia nazionale per la sicurezza del volo: inchieste aeronautiche e inchieste penali", Roma, 21 maggio 2001, in *Diritto dei trasporti,* pp. 634 – 642.

Saitta, Nazzareno (1970): "Inchiesta amministrativa", in *Enciclopedia del diritto*, XX, pp. 981 – 989.

Franchi, Bruno (2013): "Le nuove inchieste aeronautiche", in *Responsabilità civile e prevenzione*, pp. 384 – 405.

Antonini, Alfredo (1997): "I sinistri aeronautici", in *Trasporti. Diritto, economia, politica*, pp. 51 – 70.

Dekker, Sidney (2012): *Just Culture, balacing safety and accountability* (Sidney, Ashgate).

Ferro, Giovanni Battista (2015): "*L'inchiesta di sicurezza e l'inchiesta (rectius, l'indagine) dell'Autorità Giudiziaria: una insopprimibile contradictio in adiecto*?", Franchi Bruno e Vernizzi Simone (editor): *Prevenzione degli incidenti aerei. La nuova normativa internazionale e dell'Unione Europea* (Torino, Giappichelli), pp. 53-60.

Zacche', Francesco (2012): *La prova documentale* (Milano, Giuffrè).

Franchi, Bruno (2010): "Aeromobili senza pilota (UAV): inquadramento giuridico e profili di responsabilità, in *Responsabilità civile e prevenzione*, pp. 1213-1232.

Franchi, Bruno (1997): "Gli apparecchi per il volo da diporto o sportivo: tipologia, natura giuridica e disciplina legislativa, in *Atti del Convegno "Profili normativi del volo da diporto o sportivo*, Roma 7 marzo 1997, pp. 39-47.

Curtotti, Donatella (2013): *Rilievi ed accertamenti tecnici* (Milano, Cedam).

Conti, Carlotta (2013): "La prova scientifica", Ferrua, Paolo, Marzaduri, Enrico, Spangher Giorgio (editor): *La prova penale*, Vol. 1 (Torino, Giappichelli), pp. 87-119.

Felicioni, Paola (2012): *Le ispezioni e le perquisizioni* (Milano, Giuffrè).

Giunchedi, Filippo (2009): *Gli accertamenti tecnici irripetibili (tra prassi devianti e recupero della legalità)* (Torino, Giappichelli).

Spangher, Giorgio (2013): "Diritto e scienza: un rapporto in continua evoluzione", Curtotti, Donatella e Saravo Luigi (editor), *Manuale delle investigazioni sulla scena del crimine* (Torino, Giappichelli), pp. 1-4.

Adam, Roberto e Tizzano, Antonio (2010): *Lineamenti di diritto dell'Unione Europea* (Torino, Giappichelli).

Paciaroni, Mario (2015): "Prime linee guida ai pubblici ministeri in materia di coordinamento delle inchieste in caso di incidenti aerei", Franchi, Bruno e Vernizzi, Simone (editor): *Prevenzione degli incidenti aerei.* La nuova normativa internazionale e dell'unione europea (Torino, Giappichelli), pp. 61-74.

Rampioni, Matteo (2019): "Le c.d. indagini "anfibie": linee di fondo sul controverso legame tra attività ispettive e processo penale", in *Diritto processo e giustizia*, pp. 232-248.

Orlandi, Renzo (1992): *L'efficacia probatoria di atti ed informazioni amministrative nel processo penale: contributo allo studio delle prove extracostituite* (Milano, Giuffrè).

Clivio, Nicola (2015): "Considerazioni sull'utilizzabilità in ambito penale dei risultati della inchiesta di sicurezza", in *Prevenzione degli incidenti aerei*, Franchi, Bruno e Vernizzi, Simone (editor): *Prevenzione degli incidenti aerei.* La nuova normativa internazionale e dell'unione europea (Torino, Giappichelli), pp. 45-52.

Ubertis, Giulio (2016): "Prova scientifica e giustizia penale", in *Rivista italiana di diritto e procedura penale*, pp. 1192-1203.

Securitizzazione dell'Unione europea e poteri concorrenti. Dall'investigazione, alla prevenzione, all'osservazione

Securitización y competencias concurrentes en la Unión Europea. De la investigación a la observación y prevención

Securitization and Competing Powers in the European Union. From Investigation to Observation and Prevention

Angela Procaccino
Professore associato di Diritto processuale penale - Università di Foggia
angela.procaccino@unifg.it

Diritto UE, Cooperazione giudiziaria, Procura europea | Derecho UE, Cooperación judicial, Fiscalía Europea | Judicial cooperation, European Public Prosecutor's Office

Abstracts

Nello Spazio di Libertà, Sicurezza e Giustizia è possibile rintracciare tre fenomeni: "securitizzazione", "agenzificazione" e "datificazione". L'accelerazione e l'interconnessione dei pericoli esaltano i bisogni di "sicurezza", spingono sulla "prevenzione" e trasformano l'investigazione in "osservazione preventiva". Assumono un ruolo primario il network delle Agenzie per la Giustizia e gli affari interni (JHA Network) e lo "scambio d'informazioni", anche attraverso l'interoperabilità delle banche dati. La "datificazione", dal canto suo, sta modificando talune categorie processualpenalistiche. Dopo essersi occupato di alcuni dei "poteri informativi e parainvestigativi" di Autorità solo formalmente "amministrative", l'Autore accenna anche al potenziamento di EUROPOL col Regolamento 991 del 2022 nonché alla proposta di un "Codice della cooperazione di polizia" dell'Unione europea volto a ricomporre frammentazione e concorrenza di poteri preventivi e investigativi.

En el Área de Libertad, Seguridad y Justicia de la Unión Europea es actualmente posible rastrear tres fenómenos: "securitización", "agencialización" y "datificación". La aceleración y la interconexión de los peligros empujan a la prevención y transforman la investigación en "observación preventiva". En este contexto, la red de agencias de justicia e interior (JHA Network) y el "intercambio de información" adquieren una importancia primordial. Así, tras tratar algunas de las "facultades de información y parainvestigación" de autoridades sólo formalmente "administrativas", el autor analiza el refuerzo de EUROPOL con el Reglamento 991 de 2022, así como la propuesta de un "Código de cooperación policial" de la Unión Europea encaminada a recomponer la fragmentación y competencia de las competencias preventiva e investigadora.

In the area of Freedom, Security and Justice we foresee three phenomena: "securitization", "agencyification" and "datafication". The acceleration and interconnection of dangers push prevention and transform investigation into "preventive observation". The network Justice and Home Affairs Network (JHA Network) and the "exchange of information" acquire a primary role. Thus, after dealing with some of the "information and parainvestigative powers" of only formally "administrative" Authorities, the Author will also mention the strengthening of EUROPOL with Regulation 991 of 2022, as well as the Proposal for a "Code of Police Cooperation" of the European Union aimed at recomposing the fragmentation and competition of preventive and investigative powers.

Sommario

1. Accelerazione e interconnessione dei pericoli: dal punire al prevenire, dall'investigare all'"osservare".

Non occorre dar conto dei rivolgimenti scientifici, tecnologici e sociali (come pure naturali ed antropici) che hanno trasformato nei soli ultimi 20 anni l'Europa dal punto di vista politico e dunque giuridico, disgregando e redistribuendo sovranità, poteri, fonti[1]. Fatto sta che l'esito di tali trasformazioni è ora facilmente riconoscibile. Se volessimo ridurlo ad etichette potremmo giustapporre tre termini: "securitizzazione"[2], "agenzificazione"[3] e "datificazione"[4].

Sullo sfondo dei complessi rapporti tra sovranità concorrenti nell'Unione europea spicca a nostro avviso un riassetto dei poteri pubblici e privati anche nello Spazio di Libertà, Sicurezza e Giustizia[5], nel quale il baricentro scivola sempre più verso la Sicurezza[6], mescolando i piani dell'osservazione amministrativa e della procedura penale che talvolta, per così dire finisce per "uscire da sé stessa"[7]: uno degli esempi più significativi è il potere di *segnalazione* di contenuti "ai fornitori di servizi *online* interessati ai fini dell'esame volontario della compatibilità di tali contenuti con i loro termini e condizioni", introdotto dal Regolamento (UE) 991/2022 di riforma dell'EUROPOL[8], che a sua volta sembra presupporre anche un'attività di monitoraggio proattivo di EUROPOL, da svolgere, verosimilmente, mediante intelligenza artificiale[9].

Partiamo dall'inizio: la complessificazione della realtà e (in special modo) la creazione

[1] Si rinvia, tra molti, a Kostoris (2016), pp. 9 ss.

[2] Nella vastità della letteratura, per un'analisi del concetto di sicurezza interna nell'Area Giustizia e Affari Interni e, poi, nell'Area di Libertà, Sicurezza e Giustizia, si rinvia a Chiti e Mattarella (2008), pp. 305 ss.; De Capitani (2020), pp. 375 ss.; Mitsilegas, Monar, Rees (2003), pp. 6 ss. Per le interrelazioni tra sovranità statale e sicurezza, attraverso il ruolo dei mercati e dei fenomeni migratori, si veda Adler-Nissen e Gammetoft Hannsen (2008), pp. 166 ss. Per il concetto di sicurezza interna nella fase dell'allargamento dell'Europa, si veda Henderson (2005), pp. 1 ss. e 110 ss.

[3] Chamon (2016), *passim*. Per una descrizione delle Agenzie dell'Unione quali "*political enterpreneurs*" e "*technocrat-guardian*", si vedano, rispettivamente, Wood (2018), pp. 404 ss., Cassese (2012), pp. 603 ss.; e Vitiello (2020), pp. 144 ss.

[4] Cfr. Sicurella e Scalia (2013), p. 409, ove si rileva il ruolo cruciale della "datificazione" nella ricerca della sicurezza e si dà conto del peso determinante della giurisprudenza Cedu oltre che (dopo il Trattato di Lisbona e l'esplicito riconoscimento della natura vincolante della CDFUE) di quella della Corte di Giustizia dell'Unione europea, nel bilanciamento tra bisogni investigativi e securitari e diritti individuali; nonché Pagallo e Quattrocolo (2018), pp. 391 ss., anche per il riferimento alla giurisprudenza Cedu sui limiti di cui all'art. 8 della Convenzione, nell'attività di analisi e profilazione dei dati. Si veda, inoltre, Floridi (2018), pp. 689 ss.

[5] Strutturato, all'interno della Parte terza, Titolo V del TFUE, con la nota architettura nei quattro capi (oltre a quello sulle disposizioni comuni), delle politiche su frontiere, asilo e immigrazione (Capo II), della cooperazione giudiziaria civile (Capo III) e penale (Capo IV) e della cooperazione di polizia (capo V). Si rinvia a Kostoris (2022), pp. 215 ss.; Vitiello (2020), pp. 11 ss.

[6] La "natura ossimorica" dello SLSG è sottolineata da Di Stasi e L.S. Rossi (2020), p. 9.

[7] Si riprende qui l'espressione efficacemente utilizzata da Turmo (2021), pp. 473 ss.

[8] Regolamento (UE) 991/2022, entrato in vigore il 28 giugno 2022. Si veda, *infra*, nota 104.

[9] Strumento certamente supportato dalla nuova base giuridica di cui agli artt. 2, lett. v), e 4, comma 1, lett. v) e w), Regolamento (UE) 2016/794 (Regolamento EUROPOL), così come riformato dal Regolamento (UE) 991/2022. Si veda, *infra*, paragrafo 8.

dell'"infosfera"[10] hanno ingigantito i bisogni di sicurezza e *safety*[11], influendo sia sul piano sostanziale – gonfiando la categoria del pericolo astratto "penalmente rilevante" e sgretolando il principio di territorialità[12] – , sia sul piano procedurale, ingigantendo la sfera del "probatoriamente utile"[13] attribuendo alla traccia elettronica di qualsivoglia agito umano una indubitabile utilità a futura memoria, come nel caso dei dati esterni di comunicazione e dei *file* di *log*. Il peso delle "prove elettroniche"[14] e dei "*Big Data*"[15] è peraltro attestato dalla proposta di Regolamento relativo agli "ordini di produzione" che dovrebbe consentire alle autorità giudiziarie di uno Stato membro di chiedere direttamente l'accesso alle prove elettroniche conservate da un prestatore di servizi stabilito o rappresentato in un altro Stato membro[16]. Quanto sia sensibile la materia lo dice lo stallo in cui versa il pacchetto di proposte[17] e che a nostro avviso è stato parzialmente aggirato dall'autorizzazione del 5 aprile 2022 del Consiglio agli Stati membri, a ratificare nell'interesse dell'Unione il secondo Protocollo alla Convenzione di Budapest sulla Cybercriminalità, firmato il 17 novembre 2021 in seno al Consiglio d'Europa. Si tenga conto, peraltro, che già il 6 giugno 2019 il Consiglio aveva adottato un mandato che autorizzava la Commissione a negoziare a nome dell'UE un accordo con gli Stati Uniti per facilitare l'ac-

[10] Si fa riferimento alla concezione digitalizzata della realtà, costituita da insieme di informazioni, in cui il dato personale assume un ruolo non meramente descrittivo, ma anche costitutivo dell'individuo e fondativo per il funzionamento di un numero crescente di attività della vita quotidiana. Ciò è dunque strettamente collegato con quanto ora si dirà sulla "datificazione" e sulla polivalenza anche probatoria del "dato". Nella consapevolezza di non poter ridurre, banalizzando, temi di questa portata, ci si limita a rinviare a Floridi (2017), *passim*. Si vedano pure Castells (2014), p. 27; Granieri (2006), *passim*; Scubbi (2019), pp. 27 ss.

[11] Con grande approssimazione ci si riferisce alle accezioni, ormai di generale dominio, di *sicurezza* con riferimento alla protezione da eventi dannosi e avversi causati dall'intervento umano consapevole e volontario e, invece, di *safety* come protezione da eventi avversi occorsi in conseguenza di fenomeni naturali e in alcun modo voluti. Si rinvia, ad ogni modo a Goldewijk (2008), p. 24 ss. Si tenga presente come proprio nella sua pagina d'apertura, la Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025 (reperibile al *link www.eur-lex.europa.eu/legal-content*) sottolinei come dal 2020 sia emersa una particolare complessità dell'attività dei gruppi della criminalità organizzata legata all'operatività transnazionale e online e all'utilizzo di nuove tecnologie e modi operandi altamente sofisticati: ne sono esempi i casi *EncroChat* e *Sky ECC*. Il primo è relativo all'indagine congiunta francese e olandese, svolta col sostegno di EUROPOL ed EUROJUST e destinata a smantellare una rete telefonica cifrata largamente usata dalle reti criminali. Essa ha condotto a oltre 1800 arresti e a più di 1500 nuove indagini. Il secondo è relativo all'altra operazione congiunta, seguita all'introduzione abusiva in *Sky ECC*, una rete cifrata in cui si erano trasferiti molti *ex* utenti di *EncroChat* e che ha consentito di prevenire più di 70 incidenti violenti, nonché di sequestrare circa 28 tonnellate di sostanze stupefacenti e di arrestare oltre 80 persone con la contestazione di reati associativi e traffico di stupefacenti in Belgio e nei Paesi Bassi. Da esso sono poi gemmate più di 400 ulteriori indagini.

[12] Si può probabilmente affermare che – se la crisi della materialità penale si è in larga parte consumata con la "soggettivizzazione del reato" tra XIX e XX secolo (cfr., Forzati (2019), pp. 1989 ss.) – nel XXI secolo, invece, essa si ripresenta sotto aspetti peculiari in particolar modo per il consolidamento dell'infosfera. Le mutate modalità di presentazione della fattispecie nell'epoca della complessità scientifico tecnologica e di Internet, deformano i consueti concetti, sia di azione ed omissione, sia di territorialità. Accenta lo stravolgimento del principio di territorialità (causato anche dall'enorme aumento della mobilità fisica delle persone) Bernardi (2002), p. 485, che sottolinea la crisi del detto principio, a prescindere dalla commissione su o tramite la rete. Si rinvia, pure, a Barcellona (2007), pp. 89 ss.

[13] Attualmente, l'85% delle indagini penali fa ricorso ai dati digitali e in più del 50% di tutte le indagini penali si effettuano richieste transfrontaliere finalizzate all'ottenimento di prove elettroniche. Si veda il *link www.consilium.europa.eu/it/policies/e-evidence/*.

[14] Si veda Signorato (2018), pp. 236 ss. Si rinvia, per i profili teorici, a Dominioni (2005), p. 25, il quale già rilevava le mutate esigenze probatorie e la necessità di ricorrere ad "apparati conoscitivi (principi e metodologie della scienza teorica, metodiche della scienza applicata, tecnologie, procedure di indagini tecniche e di valutazioni costruite sulla scorta di esperienze pratiche specializzate, apparecchiature con cui queste risorse di conoscenza sono utilizzate" che, fuoriuscendo dal sapere comune quanto a competenza teorica o pratica, richiedono perciò il ricorso ad un esperto. Si vedano, inoltre, Cajani e Costabile (2001), p. 12.

[15] Si tenga conto che con la Direttiva (UE) 2016/680 (cosiddetta Direttiva LED) relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte della polizia e delle autorità di giustizia penale, nonché alla libera circolazione di tali dati, già si è indubitabilmente conferito alla *crime analysis* e al crime *linkage* un ruolo determinante per la prevenzione, l'accertamento e la repressione dei reati. Tuttavia, come noto, è una fonte di *soft law* che, su tutte, consente di comprendere le implicazioni della componente algoritmica nel sistema di prevenzione e tutela della sicurezza. Si fa riferimento alla *European Ethical Charter on the use of Artificial Intelligence in Judicial systems and their environment*, adottata dal Consiglio d'Europa nel dicembre 2018, e rinvenibile al *link www.rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c*. Per un primo commento alla Carta si vedano Quattrocolo (2018) e Gialuz (2019). Si veda, pure, sebbene in relazione al profilo della giustizia più che della prevenzione, Quattrocolo (2020), pp. 267 ss. Cfr., anche, *infra.* Sul vasto e complesso concetto di "*Big Data*", si rinvia all'analisi di L. Lupària (2012), pp. 96 ss., secondo il quale, già da tempo "il processo penale moderno si vede impetuosamente investito di dati statistici e valutazioni a carattere probabilistico".

[16] La risposta alla richiesta dovrebbe arrivare entro 10 giorni, o entro 6 ore in caso di emergenza. Gli ordini di conservazione, invece, dovrebbero evitare che le prove elettroniche vengano cancellate da parte del prestatore di servizi durante il trattamento dell'ordine di produzione. Gli strumenti avranno ad oggetto esclusivamente i dati conservati poiché l'intercettazione in tempo reale delle telecomunicazioni è esclusa dall'ambito di applicazione delle norme in preparazione. Si veda il documento COM (2018) 225 *final*. Accompagna la proposta di Regolamento anche una proposta di Direttiva recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali (per cui si veda il documento COM (2018) 226 *final*. Rilevante il resoconto della discussione, in seno al consiglio dell'Unione europea avvenuta il 26 agosto 2021, e contenuto nel documento CONSIL 11314/21, reperibile *online*. Le proposte normative attualmente sono in sede di commissione permanente dei rappresentanti presso il Consiglio, riunitosi in data 23 maggio 2022.

[17] Per una sintesi dei punti di disaccordo tra Consiglio e Parlamento si può vedere la "*Nota*" della Presidenza al *Permanent Representative Committee*, n. 9296/22 (reperibile al *link www.eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9296_2022_INIT&from=EN*).

cesso alle prove elettroniche ai fini della cooperazione giudiziaria in materia penale[18]. Nella medesima direzione vanno pure le notevoli innovazioni al mandato EUROPOL, in punto di prova elettronica e capacità d'analisi, di cui si dirà appresso.

Si materializza in questo modo un inarrestabile mutamento del concetto di investigazione. L'adeguamento alla velocità, ai nuovi modi e ai nuovi strumenti dell'attuale agire umano pericoloso ha imposto, cioè, un ripensamento dei rapporti tra attività di prevenzione[19] e attività di investigazione che – con categorie più solide ma forse ormai obsolete – fino a un ventennio fa si sarebbero definite "amministrative" e "penali". E, il ripensamento sta riguardando, pure, il confine con la notizia di reato nonché il concetto stesso di questa[20].

L'investigazione tende cioè sempre più ad impastarsi con (anzi ad avanzare nel)l'osservazione monitorante e questa tende sempre più ad essere svolta da una molteplicità di "Agenzie". L'innalzamento dei livelli di sicurezza e di solidità, come quello attualmente richiesto per tutte le infrastrutture critiche[21], spinge interrelazioni tra (anche nuove) Agenzie, formalmente estranee all'ambito, per l'appunto, dello SLSG[22].

E tutte le Agenzie, a loro volta, giocano quasi tutte le proprie capacità operative sull'ampiezza delle rispettive banche dati; circostanza che accelera, a sua volta, due (ulteriori) tendenze, ossia, per un verso l'incalzare dell'interoperabilità tra banche dati stesse – che efficienta la "pesca" dell'elemento di prova (come pure della notizia di reato) – e per un altro verso l'incalzare della "datificazione" delle prove".

Insomma, in un circolo di cause ed effetti, securitizzazione e trasformazione dell'investigazione hanno cementato la collaborazione tra Agenzie dell'Unione europea finendo per sfumare i confini dell'*ex* terzo pilastro oltre che forse anche delle tradizionali categorie di

[18] Gli Stati Uniti hanno un mandato a negoziare in forza del *CLOUD Act (Clarifying Lawful Overseas Use of Data)* del marzo 2018, il quale contiene (tra l'altro) parametri proprio per la the negoziazione di accordi internazionali per agevolare altri Paesi o *Partners* nell'ottenimento di dati elettronici a fini di prevenzione, ricerca, investigazione e repressione di "*serious crime*" (il *CLOUD Act*, è composto da due parti, la prima delle quali relativa all'accesso da parte degli U.S.A. ai dati ubicati al di fuori del loro territorio; e la seconda relativa all'accesso degli altri Stati ai dati detenuti dalle compagni americane, all'interno degli stessi U.S.A.). Intanto, in data 12 maggio 2022, gli Stati uniti hanno firmato il già citato Secondo Protocollo alla Convenzione di Budapest. Non potendosi trattare compiutamente il tema, si rinvia a Brière (2021), p. 493 ss.; Calavita, (2021), *passim*; Daskal (2018), p. 220 ss.; Procaccino (2022a), p. 1168.

[19] Si rinvia, fra molti, Slobogin (2018), p. 1 ss.

[20] Il fatto che anche la sola semplice iscrizione di una notizia di reato sia suscettiva di effetti negativi per l'individuo (oltre che di congestione per l'apparato) è dimostrata dal tentativo da parte della legge 134 del 2021 (cd. Riforma Cartabia), e del successivo d.lgs. 150 del 2022, di perimetrare il concetto di notizia di reato, irrobustendo la soglia per l'iscrivibilità di un fatto, accogliendo invero taluni esiti della giurisprudenza di legittimità. A ciò si affianca anche l'altra previsione con cui la Riforma Cartabia ha richiesto che l'iscrizione della notizia di reato non rechi effetti dannosi per il soggetto iscritto. In questa sede, peraltro, non ci si occuperà dei rapporti con i servizi per la sicurezza interna. Per l'analisi del concetto di notizia di reato, dei confini e possibili sovrapposizioni di attività dei servizi e attività inquirenti si rinvia a Nocerino, in questa *Rivista*.

[21] Si rinvia, sin d'ora, alle proposte di riforma strettamente interrelate e pendenti a livello "unionale" per rafforzare la resilienza dell'Unione europea in relazione alle minacce ibride (portate cioè su e tra internet o al di fuori di essa). Innanzitutto, si deve considerare la *Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities* (c.d. direttiva CER), in fase di prima lettura (per cui si consulti il *link www.data.consilium.europa.eu/doc/document/ST-12414-2022-INIT/en/pdf)*. La proposta direttiva intende coprire undici settori: energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione, spazio e cibo, mentre quella del 2008 si applicava solo all'energia e ai trasporti. Essa mira cioè a creare un quadro che fronteggi tutti i possibili rischi, supportando gli Stati membri nel garantire che le entità critiche siano in grado di prevenire, resistere, assorbire e riprendersi da gravi incidenti, indipendentemente dal fatto che siano causati da disastri naturali, incidenti, terrorismo, minacce interne o emergenze di salute pubblica, comprese le pandemie. Ad essa è collegata la proposta di Direttiva *Security of Network and Information System* (NSI2) che riformerebbe la direttiva NSI 1. Questa proposta, in modo complementare alla prima, mira a garantire una solida resilienza informatica da parte di un gran numero di "*entities*". Al fine di garantire l'allineamento tra i due strumenti, tutte le entità critiche individuate ai sensi della direttiva CER sarebbero soggette agli obblighi di resilienza informatica ai sensi della Direttiva NIS2. Il Comitato economico e sociale europeo (EESC) ha proposto di fondere le due proposte per una maggiore semplificazione ed efficacia. Si rinvia al *link www.europarl.europa.eu*. Mette conto ricordare pure che il 27 gennaio 2022 le tre Autorità europee di vigilanza (l'Autorità bancaria europea, EBA, l'Autorità di vigilanza delle assicurazioni e delle pensioni, EIOPA e l'Autorità europea degli strumenti finanziari e dei mercati, ESMA) hanno favorevolmente accolto le raccomandazioni emanate dall'*European Systemic Risk Board* (ESRB) riguardo al rischio sistematico cibernetico. Esse sollecitano a costruire gradualmente un quadro unitario per la risposta ai gravi incidenti informatici transfrontalieri dal potenziale impatto sistemico sulla situazione finanziaria dell'Unione. A tal fine, le dette Autorità dovranno coordinarsi (oltre che con gli Stati membri) con le altre autorità ed organismi, prime fra tutte l'Agenzia dell'Unione europea per la cybersicurezza (ENISA) e la BCE. Si veda, però, nota successiva. A tal fine, come sollecitate dalle raccomandazioni, che risultano in linea con quanto previsto, peraltro, dalla *Digital Operational Resilience* proposta dalla Commissione europea, le Autorità del settore finanziario dovranno coordinarsi tra loro e con le altre autorità ed organismi con i quali esse di solito potrebbero non interagire, come l'Agenzia dell'Unione europea per la cybersicurezza (ENISA), nonché sollecitare i singoli Stati membri, la BCE e le altre Autorità coinvolte a designare un punto di contatto principale.

[22] Prime fra tutte l'OLAF, l'ufficio antifrode dell'Unione europea (istituito con Decisione e l'ENISA. Le interrelazioni della prima col sistema di polizia e giudiziario hanno da tempo sollecitato interrogativi e studi (si rinvia a De Amicis (2022), p. 313 ss., anche per la bibliografia *ivi* citata; si segnala anche l'Agenzia dell'Unione europea per la cybersicurezza (ENISA), istituita dal regolamento (UE) 2019/881, relativo anche alla "certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (EU) n. 526/2013 (Regolamento sulla cybersicurezza).

"elemento di prova" e "dato"[23].

2. Il versante investigativo della cooperazione giudiziaria penale si espande e si mescola con l'"osservazione": l'esempio dell'EPPO.

Come detto, già nell'ambito della cooperazione giudiziaria, all'interno dello Spazio di Libertà, Sicurezza e Giustizia, si è assistito all'allargamento dei poteri investigativi, in larga parte in seguito al perfezionarsi della costruzione dell'ufficio della Procura europea (EPPO). L'approvazione del Regolamento EU 1939/2019 materializza in effetti uno degli assestamenti più "rumorosi" degli equilibri dello SLSG. D'altronde, che si fosse dinanzi ad una trasformazione che toccava le corde delle sovranità e delle politiche giudiziarie è testimoniato dalla lunghissima gestazione del Regolamento attraverso numerose proposte e modifiche[24]. La struttura a cui infine si è approdati vede, come noto, più livelli (quello prettamente europeo e quello nazionale) collegati, e la presenza (tra l'altro) di un organo di controllo e coordinamento collegiale. Sono tuttavia le attività investigative e, prim'ancora, quelle volte a saggiare un'eventuale "competenza" dell'ufficio europeo, ad essere preponderanti. Si tratta, in buona sostanza un meticoloso meccanismo di pesi e contrappesi che prende l'avvio da un puntuale scambio di informazioni preliminari, il quale, a sua volta, percorre a doppia via i fascicoli delle procure nazionali e dell'EPPO ed è volto ad appurare, appunto, la sussistenza del *potere investigativo* dell'ufficio europeo e i presupposti per un'eventuale avocazione dei casi. L'ingresso dell'EPPO è stato, s'è detto, il più tormentato e visibile, poiché ha portato sulla scena attori nuovi e direttamente legittimati all'investigazione[25]. Peraltro, la rilevanza delle fasi investigativa e preinvestigativa si comprende ancor meglio ove si pensi che quella di EPPO è una "competenza" elasticamente espandibile anche alle (affatto trascurabili) *ancillary offences*[26]: che la partita si giochi in larga parte già dalla fase dell'investigazione è dimostrato dal dibattito già apertosi in dottrina, al fine di puntellare poteri intrusivi e garanzie individuali[27].

Anche EPPO sta intessendo relazioni sempre più strette sia con le agenzie costituite ai sensi del Titolo V, TFUE, sia (prima fra tutte) EUROPOL[28], sia con altre entità del diritto dell'unione (e nazionali) "formalmente" estranee all'ambito di polizia, come ad esempio l'OLAF[29] e le *Financial Intelligence Unit*[30], così sfumando anch'esso, a sua volta, il confine tra investigazione e l'"osservazione monitorante".

Vediamo poi, come anticipato, anche gli altri piani d'azione, in cui l'espansione e la dislocazione dei poteri di "osservazione monitorante" si sono affiancati a quelli di investigazione penale, fino a (talvolta) con essa confondersi, riplasmando con ciò, più silenziosamente, gli equilibri politico istituzionali europei. Si è fatto riferimento, in primo luogo, alle altre Agenzie che operano (ma non solo) nello Spazio di Libertà, Sicurezza e Giustizia, anche per il tramite, lo si vedrà ora, dello *European Travel Information and Authorisation System* (ETIAS), grazie all'interoperabilità delle diverse banche dati da esso filtrate e ai nuovi poteri di EUROPOL[31], portati dalla recentissima riforma, fra cui i poteri di "collaborazione" coi privati per l'otteni-

[23] Basti leggere le già significative rubriche del Capo IV del Regolamento EUROPOL, "(T)trattamento delle informazioni" e delle disposizioni recate: la prima, ossia l'art. 17, è rubricata "(F)onti di *informazione*)", l'art. 18 poi è rubricato "(F)inalità dell'attività di trattamento delle *informazioni*)" e l'art. 18-*bis* "Trattamento dei dati personali a sostegno di un'indagine penale". Si veda, anche, quanto si dirà in merito all'ampliamento dei poteri di EUROPOL, *infra*, e in particolare, la nota 107.

[24] Si rinvia a Venegoni (2022), p. 2798.

[25] Per le riflessioni in merito alle ripercussioni sugli equilibri interni alla magistratura creati dall'Ufficio, si veda Belfiore (2021), *passim*; Lorusso (2014), pp. 33 ss.

[26] Quanto all'Italia, i dati segnalano su 102 indagini in corso, sequestri per 40 milioni di euro, un processo pendente e nessuna decisione definitiva, vi sono 34 casi di indagini su reati connessi. Il profilo è delicatissimo e molto contestato. Sia consentito rinviare a Procaccino (2022b), p. 509 ss. In senso critico sulla "flessibilità delle regole di competenza" si veda, pure, Tavassi (2022), pp. 53 ss.

[27] Da ultimo, si veda, Cassibba (2022) e la dottrina *ivi* richiamata.

[28] La riforma di EUROPOL, ad opera del Regolamento 991/2022, difatti ha reso Europol l'*hub* informativo per tutte le agenzie del titolo V, OLAF ed ENISA. Si veda l'art. 4, comma 1, lett. j), Regolamento (UE) 2016/974 (Regolamento EUROPOL) modificato dal Regolamento (UE) 991/2022. Per specifiche relazioni con EPPO, si veda l'art. 20-*bis*, Regolamento (UE) 2016/974 (Regolamento EUROPOL) modificato dal Regolamento (UE) 991/2022.

[29] Ai sensi del detto art. 4, comma 2 lett. j), (UE) 2016/974 (Regolamento EUROPOL) come aggiornato dal Regolamento 991/2022, EUROPOL farà da centro di coordinamento tra gli Stati, le Agenzie e il medesimo OLAF; inoltre, le interrelazioni con OLAF sono specificamente disciplinate dall'art. 21 del Regolamento EUROPOL.

[30] Si veda l'art. 4, comma 1, lett. z), Regolamento 991/2022, nonché, *infra*, paragrafo 7.

[31] Si veda anche, *infra,* il paragrafo 7.

mento di prove elettroniche, il quale ha, anch'esso contribuito ad aggirare il problema dello stallo del pacchetto normativo sull'ordine di produzione e conservazione delle dette prove[32].

3. Lo Spazio di Libertà, Sicurezza e Giustizia vira verso la sicurezza: il *network* delle Agenzie per la Giustizia e gli affari interni (*JHA Network*) e lo "scambio d'informazioni".

L'altra tendenza che abbiamo visto essere immediatamente riconoscibile è lo slittamento, all'interno dello SLGS, dell'asse portante dal piano della "Giustizia" a quello della "Sicurezza", con la dilatazione dell'attività che abbiamo definito di "osservazione monitorante". Essa viene esercitata da molteplici Agenzie, (poi, lo si vedrà, anche estranee allo SLSG, ma tra loro profondamente collegate). Gli strumenti materiali in grado di consentire tale interconnessione sono le banche dati delle diverse Agenzie che, come si dirà, sono a loro volta interconnesse, grazie al (recente) potenziamento della loro interoperabilità[33].

Innanzitutto, diciamo però come nell'ambito dello SLSG operino più Agenzie, costituite in una rete, ovverosia il "*Justice and Home Affairs Agencies Network*" (JHAN)[34], la cui istituzione fu voluta dal Comitato permanente sulla Sicurezza interna nell'ambito del Consiglio nel 2010[35]. Le agenzie per lo SLSG vengono indicate anche, come detto, quali "*Justice and Home Affairs Agencies*" per via del mantenimento dell'acronimo JHA (giustizia e affari interni) derivato dalla nota denominazione del terzo pilastro del Trattato di Maastricht. Esse, peraltro, hanno certamente "*less regulatory and more operational powers*" oltre che un incisivo tratto distintivo grazie al quale "*their operational activity is strongly interlinked with the national law enforcement communities*"[36].

Allo scopo di incrementare la cooperazione tra i "corpi" dell'Unione sui problemi di comune interesse nell'amministrazione della giustizia e degli affari interni, dal 2012, il network raggruppa ben nove agenzie, ovverosia EUROPOL, EUROJUST, l'*External Action Service* (EEAS o FRONTEX), che include EU SITCEN, poi la *European Agency for large-scale IT systems* (eu-LISA), la *Fundamental Rights Agency* (FRA), lo *European Police College* (CEPOL), lo *European Asylum Support Office* (EASO), lo *European Institute for Gender Equality* (EIGE), lo *European Monitoring Centre for Drugs and Drug Addiction* (EMCCDA).

Possiamo individuare due modelli di collaborazione. Uno comprende tutte le Agenzie contemporaneamente e l'altro parte sulla spinta di una di esse e procede per contatti bilaterali o trilaterali con le altre, per poi, eventualmente allargarsi[37]. Per intendere meglio lo svolgimento e l'impatto pratico negli ultimi anni di questi due modelli di cooperazione, si pensi che nel 2018, lo *European Asylum Support Office* (EASO), FRONTEX ed EUROPOL hanno avviato un'operazione di incrocio di informazioni sui movimenti secondari nell'Unione europea e negli altri Paesi Schengen, rifluita poi in due relazioni conclusive aventi ad oggetto la prote-

[32] Si veda il già citato *link www.consilium.europa.eu/it/policies/e-evidence/*.
[33] Distinto dall'ambito delle finalità preventive e investigative (di "polizia" e *latu sensu* amministrative) il sistema e-CODEX, (già parzialmente utilizzato ma) di recente normato con Regolamento (UE) 2022/850 del Parlamento e del Consiglio del 30 maggio 2022. Difatti si tratta dell'adozione di un sistema informatizzato per lo scambio elettronico transfrontaliero di dati nel settore della cooperazione giudiziaria in materia civile e penale. Nelle parole del considerando n. 7 del Regolamento, il sistema è stato "concepito per facilitare lo scambio elettronico transfrontaliero di dati ... Nel contesto di una maggiore digitalizzazione dei procedimenti in materia civile e penale, l'obiettivo del sistema e-CODEX è migliorare l'efficienza della comunicazione transfrontaliera tra autorità competenti e facilitare l'accesso alla giustizia per cittadini e imprese". I Considerando n. 9 e 10 specificano come lo scambio elettronico di dati comprenda qualsiasi contenuto trasmissibile per via elettronica mediante il sistema, "ad esempio testo o registrazioni sonore, visive o audiovisive, sotto forma di dati, file o metadati strutturati o non strutturati", e come il regolamento però non preveda l'uso obbligatorio di tale sistema per le dette trasmissioni.
[34] Per la sintesi effettuata nel 2022 delle attività relative al 2021, si consulti il *link www.eucrim.eu/news/report-on-jha-network-activities-2021/*.
[35] Si tratta, più precisamente dello *Standing Committee on Operational Cooperation on Internal Security* (COSI). Ruolo e composizione sono espressi nell'art. 71 TFUE: il Comitato deve garantire l'efficace cooperazione operativa per la sicurezza interna dell'UE, comprese le attività di contrasto, il controllo di frontiera e la cooperazione giudiziaria in materia penale. Esso assiste il Consiglio nella reazione ad attacchi terroristici o catastrofi naturali o provocate dall'uomo ed è composto da funzionari di alto livello del Ministero dell'Interno e/o della Giustizia di ciascuno Stato membro, e da rappresentanti della Commissione e del Servizio Europeo per l'Azione Esterna (SEAE). Occorre ricordare, poi, che EUROPOL, EUROJUST, FRONTEX, CEPOL e altri organismi pertinenti possono essere invitati a partecipare alla riunione in qualità di osservatori.
[36] Luchtman e Vervaele (2014) p. 132.
[37] Si veda, difatti, il *Final Report on the JHA Agencies' Network Activities* 2021, reperibile al link *www.prd.frontex.europa.eu/wp-content/uploads/final_report_on_jhaan_activities_in_2021.pdf*, pp. 31 ss.

zione internazionale, l'immigrazione irregolare e il traffico di migranti del 2019 e del 2020[38]. Prendendo spunto dalla proficuità di tale collaborazione, nel 2021 sono state adottate delle *Linee Guida* per la stesura di due relazioni annue sistematicamente prodotte sui movimenti secondari, e su altri temi sensibili individuati dalle tre Agenzie. È stabilito che il primo ciclo di analisi si focalizzi, ad esempio, sui cittadini afgani.

Seguendo l'esempio, poi, su proposta di EUROPOL, lo *Standing Committee on Operational Cooperation on Internal Security* (COSI)[39] ha individuato un gruppo comune di riferimento (*hub team*), operativo dal novembre del 2020 e costituito dai punti di contatto di tutte le Agenzie della rete JHA, unitamente alla Direzione Affari interni e al *Joint Research Center* della Commissione, al Segretariato Generale del Consiglio, e all'ufficio del Coordinatore dell'Antiterrorismo.

4. Il potenziamento della Piattaforma Europea Multidisciplinare Contro le Minacce Criminali (*European Multidisciplinary Platform Against Criminal Threats*, EMPACT) spinge sulla collaborazione anche oltre il *JHA Network* (puntando sulla "nuova" EUROPOL).

EMPACT rappresenta la programmazione su base quadriennale di un approccio operativo e integrato alla sicurezza interna[40], che presuppone e impiega strumenti che spaziano dai controlli dei confini esterni, a quelli di polizia, alla gestione e scambio di informazioni, alla prevenzione[41] e alla proiezione "esterna" della sicurezza interna dell'Unione, anche mediante partenariati pubblico-privato. Partito in sordina tra il 2012 e il 2013, questo approccio politico-operativo è poi andato a pieno regime per due cicli, quello relativo agli anni 2014-2017 e quello relativo agli anni 2018-2021, e prevede una fase di graduazione nell'individuazione delle minacce all'Unione.

Nel 2021, il Consiglio dell'Unione ha stabilito dieci aree di priorità per EMPACT 2022-2025, tutte caratterizzate come pericolo per la sicurezza interna dell'Unione. L'attuazione del piano prevede quattro passaggi. Si parte dallo "*European Union Serious and Organised Crime Threat Assessment*" (EU SOCTA), effettuato da EUROPOL, sulla cui base (e lo si è appena visto) il Consiglio dell'Unione europea definisce le priorità relative ai "*serious and organised crime*" che gioca, nelle parole del Consiglio, un "*key role*" in EMPACT. Il secondo passaggio prevede l'identificazione di un numero più limitato di priorità ad opera del Consiglio stesso, con la predisposizione di un piano generale pluriennale con obiettivi strategici orizzontali. Esso involge esplicitamente l'uso di misure preventive oltre che repressive. Il terzo passaggio comporta lo sviluppo e il monitoraggio di piani operativi da parte del citato *Standing Committee on Operational Cooperation on Internal Security* (COSI), adottati annualmente e da esso monitorati. L'ultimo passaggio consta nella valutazione indipendente dell'efficacia dell'intero piano.

Nella "*New Security Union Strategy*", presentata dalla Commissione nel luglio 2020[42] si

[38] Si potrebbe citare, poi, sempre nell'ambito delle collaborazioni bi/trilaterali, la Conferenza organizzata nel 2021 dallo *European Monitoring Centre for Drugs and Drug Addiction* (EMCDDA) e supportata da EUROPOL e FRONTEX, al fine di comprendere le implicazioni sui mercati della droga degli sviluppi politico istituzionali e dei flussi di cui s'è detto *supra*. La Conferenza ha ospitato anche l'UNODC e il Dipartimento di Stato degli Stati Uniti. Ancora, si ricorda come nel 2021 FRA and EIGE abbiano avviato un sondaggio al fine di monitorare la violenza contro le donne negli Stati membri dell'Unione, che non sono già parte della raccolta di dati circa la violenza *gender-based*, gestita da Eurostat. Il report finale del sondaggio è atteso per il 2024.

[39] Cfr. *supra*, nota 35.

[40] Difatti lo strumento in questione non ha una specifica ed autonoma base giuridica, essendo esso verosimilmente riconducibile alle generali competenze del Consiglio dell'Unione. Ad ogni modo la presentazione, la struttura e il dettaglio delle competenze contenute nel piano (cui ora si accennerà nel testo) sono contenuti nell'Allegato, denominato *Terms of References* ad una *Nota della Presidenza del Consiglio* ai Delegati del 17 giugno 2021, n. 9921/21, reperibile al sito *www.data.consilium.europa.eu*.

[41] Assai interessante notare come proprio nell'apertura dei "*Terms of Reference*", citati alla nota precedente, si affermi come uno dei punti chiave di EMPACT sia: "*(T)the intelligence-led approach based on a future-oriented and targeted approach to crime control, focusing upon the identification, analysis and "management" of persistent and developing "problems" or "risks" of crime*".

[42] Il 16 settembre 2020, il Presidente della Commissione europea ha annunciato, nella lettera di intenti che ha accompagnato la Relazione sullo "Stato dell'Unione" indirizzata al Parlamento europeo, una nuova agenda sul crimine organizzato, la quale si inserisce nella detta *New Security Union Strategy*, ovverosia una "più estesa azione" nell'area della Sicurezza.

menziona, quale azione fondamentale, l'adozione di un'agenda per fronteggiare il crimine organizzato, incluso il traffico di esseri umani. Le due strategie ("*EU Strategy to Tackle Organised Crime* 2021-2025" e la "*EU Strategy on Combating Trafficking in Human Beings* 2021-2025") sono state adottate nell'aprile 2021. Occorre far presente, a tal riguardo, in primo luogo, come sia richiamato quale riferimento essenziale proprio il SOCTA, pubblicato nell'aprile 2021 e, in secondo luogo, come sia evidenziata l'impressionante dilatazione delle attività illecite online portata dall'epidemia di Covid-19[43]. Di assoluto interesse ai nostri fini è il fatto che la Strategia, nel riportare le diverse proposte legislative da parte della Commissione, si focalizzi anche sulla possibilità di adottare un atto di diritto derivato proprio per strutturare l'EMPACT, visto come strumento faro della cooperazione operativa per la prevenzione e il contrasto del crimine organizzato.

5. Osservazione preventiva, datificazione, valore probatorio polifunzionale.

La progressiva mescolanza di osservazione e informazione a fine di controllo preventivo e repressione penale conduce anche, ad altre due tendenze legate a doppio filo: la prima riguarda una sorta di evanescenza del confine fra i concetti di "elemento probatorio" e di "dato"[44], che rischia di accompagnarsi allo sfumare della distinzione tra i concetti di "trattamento" e "utilizzo probatorio"; la seconda riguarda la possibilità che, ove le norme non siano espresse e limpide, si ingenerino dubbi sull'individuazione delle regole applicabili nella raccolta e trattamento del dato stesso.

Come noto, la disciplina delineata dal Regolamento UE 679/2016 (l'arcinoto GDPR)[45] è applicabile in tutti i casi in cui non si tratti di attività di prevenzione, indagine e perseguimento di reati o esecuzione penale, ai quali è invece dedicata la direttiva UE 680/2016, cosiddetta *Law Enforcement Directive* (LED)[46]. Completa il quadro la direttiva 2002/58/CE, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle comunicazioni elettroniche[47] che, come noto, ha già dato visto l'articolato intervento della Corte di Lussemburgo, e che peraltro sta per essere sostituita dal Regolamento sulla vita privata e le comunicazioni elettroniche, attualmente oggetto di negoziati legislativi[48]. Lo svolgimento di funzioni che sono formalmente amministrative ma sostanzialmente di prevenzione e repressione penale genera il dubbio su quale delle due discipline possa essere applicabile, solo per fare un esempio, alle *Financial Intelligence Units* (FIU)[49]. La detta tendenza all'evanescenza delle categorie nasce poi da un progressivo slittamento dalla funzione propria ed originaria

[43] Si vedano, *Letter of intent: Key New Initiatives for 2021,* del settembre 2020*; Communication on the EU Security Union Strategy, COM(2020) 605 final; Fighting organised crime – EU strategy for 2021-25*; *European Union Serious and Organised Crime Threat Assessment (EU SOCTA 2021)*; *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions on the EU Strategy to tackle Organised Crime 2021-2025, COM/2021/170 final.*

[44] Sull'espandibilità del concetto di dato, si rinvia, fra molti, a Ducato (2016), p. 151.

[45] Occorre tenere presente che il 23 febbraio 2022 è stata presentata dalla Commissione la proposta sul cosiddetto *Data Act. Si tratta* di un Regolamento dedicato all'accesso equo ai dati e il loro utilizzo. In grossa sintesi esso intende disciplinare la creazione, l'utilizzo e la condivisione dei dati anche non personali, tra impresa e consumatori, imprese e imprese, privati ed enti pubblici. Esso si rivolge anche alla "messa a disposizione" di dati generati dall'uso di un prodotto o di un servizio da parte dell'utente. Il *Data Act* intende insomma adottare garanzie contro il trasferimento illecito di dati senza notifica da parte dei fornitori di servizi *cloud*, facilitare il passaggio tra diversi servizi *cloud* e prevedere l'elaborazione di norme di interoperabilità per il riutilizzo dei dati tra i vari settori. Ma ciò che più conta in questa sede è che esso intende anche rendere utilizzabili da parte enti pubblici e istituzioni i dati detenuti dalle imprese in determinate situazioni in cui vi sia una necessità eccezionale. Si veda il *link www.eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52022PC0068&from=EN.*

[46] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio d'Europa, 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, che abroga la decisione quadro 2008/977/GAI del Consiglio (Direttiva LED). Come noto essa garantisce la protezione dei dati personali delle persone coinvolte in procedimenti penali, che siano testimoni, vittime o indiziati, armonizzando la disciplina applicabile negli Stati membri dell'Unione europea e nei paesi Schengen. Questo strumento normativo si colloca nell'ambito della riforma della protezione dei dati, insieme al GDPR e al Regolamento (UE) 2018/1725 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione.

[47] 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 come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009.

[48] La proposta di Regolamento e la relazione di accompagnamento si leggano al *link www.eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52017PC0010.*

[49] Si veda, difatti, *infra*, paragrafo 7.

della normativa sui dati ad una funzione che invece per ciò che ci riguarda, possiamo dire sia divenuta, di raccolta e conservazione di materiale (a contenuto quasi sempre probatorio). Questo elemento, in fin dei conti, di natura documentale ha, infondo, come tutti gli elementi di prova, carattere polifunzionale. Può servire cioè a molti scopi: 1) a quello di osservazione preventiva, arrivando in ipotesi a coagulare una notizia di reato; 2) successivamente a quello della prosecuzione dell'indagine penale o all'azione cautelare; infine, e sempre che non vi siano espliciti divieti di utilizzabilità; 3) alle decisioni sulla regiudicanda penale. Insomma, di fatto e quasi inavvertitamente, sembra il "dato", che preesiste al procedimento penale (purché non rappresenti informazione in transito altrimenti ricadrebbe nel concetto di intercettazione), finisca per essere incasellato nella nostra tradizionale tassonomia processualpenalistica, all'interno della categoria della "prova documentale". In virtù del *trait d'union* rappresentato dalla interoperabilità delle banche dati[50] (normativamente prevista)[51] è evidente che il problema rischia di amplificarsi, poiché l'attività di raccolta massiva e massiccia di dati (delle più disparate nature, come si vedrà) porta alla precostituzione di altrettanto massicce e massive quantità di questi elementi *anfibi*. Insomma, si potrebbe dire, "una procedura penale al di fuori della procedura penale"[52]. D'altronde, che lo scivolamento dal "dato" all'elemento di prova (alla prova, eventualmente) sia divenuta una realtà concreta è dimostrato dai rinvii pregiudiziali che hanno dato luogo alla giurisprudenza con cui la Corte di Lussemburgo ha perimetrato la discrezionalità del diritto nazionale di determinare le condizioni alle quali autorità e fornitori di servizi di comunicazione elettronica possono sfruttare i dati in loro possesso[53]. Tale perimetro è costituito in primo luogo dalla chiarezza e dalla precisione delle norme nazionali e in secondo luogo dalla presenza di un controllo terzo ed imparziale, di modo che le persone i cui dati personali siano oggetto di attenzione dispongano di garanzie sufficienti contro i rischi di

[50] Sulla gestione del Sistema di sorveglianza delle frontiere esterne dell'Unione (EUROSUR), del sistema di contrasto alla frode documentale (FADO), e del sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) da parte dell'Agenzia FRONTEX, si veda Vitiello (2022), pp. 128 ss.

[51] Le banche dati rappresentano uno degli strumenti per l'esercizio delle attività di osservazione per la sicurezza, prevenzione e contrasto. Tracciando una sintesi dell'evoluzione storica, si ricorda che in piena stagione del contrasto al terrorismo internazionale, il bisogno di condividere informazioni in possesso delle autorità di *law enforcement* portò nel 2005, ad un accordo "di avanguardia" (il Trattato di Prüm) tra Austria, Belgio, Francia, Germania, Lussemburgo, Olanda e Spagna fuori dal quadro UE. Esso conteneva previsioni per lo scambio di profili DNA, impronte e dati dei veicoli. Italia, Portogallo, Slovenia, Finlandia, Svezia e Romania espressero la volontà di unirsi al Trattato, mentre altri Paesi temettero che l'adesione avrebbe potuto minare la legislazione UE esistente così come le altre iniziative anche spontanee per la condivisione di informazioni. Beninteso, già nel 2004, il dialogo nell'ambito UE sullo scambio di dati e *intelligence* tra le autorità di *law enforcement* venne innescato da due proposte: 1) una "iniziativa svedese" per l'adozione di una Decisione quadro sulla semplificazione e lo scambio di informazioni e di *intelligence* tra dette autorità dei Paesi UE, con particolare riguardo alle "*serious offences including terrorist acts*"; 2) una Comunicazione dalla Commissione al Consiglio e al Parlamento per potenziare l'accesso alle dette informazioni da parte delle "*law enforcement agencies*" (Cfr. Nunzi (2007), p. 145 ss.). Dopo due anni di negoziazioni si arrivò alla Decisione Quadro 2006/960/JHA del 18 dicembre 2006 sulla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge. In questo contesto si sviluppò dunque il modello europeo di scambio d'informazioni (*European Information Exchange Model*, EIXM). Successivamente, il 22 novembre 2010, venne presentata la comunicazione dalla Commissione "La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura (COM(2010)673), in attuazione del programma di Stoccolma per lo Spazio di libertà, sicurezza e giustizia per il periodo 2010-2014 (seguendo pure le linee guida deliberate dal Consiglio europeo del 25-26 marzo 2010). Tra le tre aree di azione individuate dalla strategia per il contrasto alle reti criminali internazionali, in cima vi era il miglioramento della raccolta e dello scambio di informazioni. I canali per lo scambio di informazioni transfrontaliero erano dunque individuabili in ogni Stato membro, in unità nazionali che utilizzavano uno specifico strumento di comunicazione. I principali si rinvenivano: negli uffici SIRENE (*Supplementary Information Request at National Entry*); nelle unità nazionali di Europol; negli uffici centrali nazionali Interpol. Si veda, oltre alla Comunicazione della Commissione al Parlamento europeo e al Consiglio, "Rafforzare la cooperazione in materia di applicazione della legge nell'UE: il modello europeo di scambio di informazioni (EIXM)", del 7 dicembre 2012 (COM(2012) 735 *final*, anche, su tutti Gialuz (2022), p. 313 ss. Come anticipato il discrimine tra agenzie di contrasto e agenzie d'osservazione o amministrative (e rispettive banche dati) talvolta scolora, o, per meglio dire, molto spesso le seconde svolgono funzioni anfibie e sono assistite da banche dati che finiscono per fungere da strumenti di prevenzione e repressione. L'enorme importanza dell'interoperabilità è dimostrata dal tentativo (non riuscito data la frammentazione di cui si continuerà a dar conto) di costruire un vero e proprio quadro normativo a riguardo. Si pensi, al Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio; e il Regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, 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) 2019/816. Tuttavia, una possibile modifica di tale "quadro" potrebbe derivare dalla eventuale approvazione della Proposta di Codice per la cooperazione di polizia, su cui si rinvia al paragrafo 9.

[52] Si richiama Turmo (2021), pp. 473 ss.

[53] La quale, come noto, ha pure influito sulla modifica della disciplina italiana, portata col d.l. 30 settembre 2021 n. 132, che ha modificato l'articolo 132 del Codice Privacy (d.lgs. n. 196/2003), correggendo il comma 3 e introducendo i commi 3-*bis*, 3-*ter* e 3-*quater*. Si veda, *infra*, nota successiva.

abuso[54]. La normativa nazionale che disciplini l'accesso delle autorità a dati relativi al traffico e a dati relativi all'ubicazione[55], non può, così ad esempio limitarsi ad esigere che l'accesso delle autorità ai dati risponda semplicemente alla finalità perseguita da detta normativa, ma deve prevedere le condizioni sostanziali e procedurali che regolano tale utilizzo[56].

Ove vi fosse bisogno di conferma, la consapevolezza della tendenza alla "*datificazione degli elementi di prova*" a nostro avviso si può leggere anche nella detta *Riforma EUROPOL*. Assai significativa ai fini di questo discorso è difatti la distinzione ora contenuta nell'art. 2 (dedicato alle definizioni), lett. p) e q), tra *dati personali amministrativi* e *dati investigativi*: i primi sono quelli "trattati da Europol diversi dai dati personali operativi", e i secondi sono quelli che "uno Stato membro, la Procura europea ("EPPO") (…), Eurojust o un paese terzo è autorizzato a trattare nell'ambito di un'indagine penale in corso connessa a uno o più Stati membri, conformemente alle norme e garanzie procedurali applicabili ai sensi del diritto dell'Unione o nazionale, o che uno Stato membro, l'EPPO, Eurojust o un paese terzo ha fornito a Europol a sostegno di tale indagine penale in corso, e che contengono dati personali che non riguardano le categorie di interessati di cui all'allegato II". Come si vedrà, la circolarità delle attività e delle banche dati rischia di sfumare nella pratica i sia pur nobili propositi.

6. L'osservazione e lo scambio informativo. L'interoperabilità nello *European Travel Information and Authorisation System* (ETIAS) e la clausola generale della protezione della "sicurezza".

Lo *European Travel Information and Authorisation System* (ETIAS)[57] è il sistema europeo di informazione e autorizzazione ai viaggi[58]. Riguarda gli individui interessati ad entrare nei Paesi dell'Unione europea che appartengono all'area Schengen e che non godano già di un visto[59]. Il legislatore dell'Unione ha, in buona sostanza, ritenuto che le autorità di gestione delle frontiere degli Stati membri disponessero di ancora poche informazioni sui viaggiatori

[54] Si veda GGUE, 2 marzo 2021, *Prokuratuur* (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, punto 48 e giurisprudenza *ivi* citata.
[55] Adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, 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, come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009.
[56] Si veda GGUE, 2 marzo 2021, *Prokuratuur*, cit., punto 49 e giurisprudenza *ivi* citata. La Corte ha interpretato il detto art. 15 nel senso che l'accesso ai dati relativi al traffico e all'ubicazione è giustificato ove occorra contrastare la criminalità grave o prevenire gravi minacce alla sicurezza pubblica. L'interferenza con i diritti fondamentali sanciti dagli artt. 7 e 8 CDFUE è grave, indipendentemente dal periodo concesso per l'accesso ai dati o dalla quantità di dati richiesti. Il perseguimento dei reati meno gravi non può quindi giustificare tale intervento. Tuttavia, la definizione di ciò che costituisce un reato grave spetta ancora agli Stati membri. Come per il concetto di sicurezza nazionale, però, afferma la Corte, v'è il rischio che gli Stati membri lo interpretino in senso ampio. È interessante notare che le corti costituzionali che hanno esaminato questioni simili non sempre si sono soffermati sul concetto di reato grave. si veda, comunque, *infra*, paragrafo 8. Di recente, peraltro, si veda CGUE, 5 aprile 2022, C-140/2020, reperibile *online*. In questo caso il rinvio pregiudiziale, *ex* art. 267 TFUE, era sollevato dalla Suprema Corte irlandese, in merito all'interpretazione della direttiva 2002/58/CE, letto alla luce degli articoli 7, 8, 11 e 52, par. l, CDFUE. La controversia all'origine del rinvio vedeva il privato opporsi Capo della polizia nazionale irlandese, al Ministero per le Comunicazioni (dell'energia e delle risorse naturali irlandese) e all'*Attorney General* (del governo) circa la validità del Communications (*Retention of Data) Act* interno del 2011.
[57] La base giuridica del Sistema ETIAS è contenuta in due Regolamenti: il Regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio del 12 settembre 2018 relativo al Sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) che modifica i Regolamenti (UE) 1077/2011, (UE) 515/2014, 2016/399, (UE) 2016/1624 ed (UE) 2017/2226 (di seguito da noi indicato come Regolamento ETIAS) e il Regolamento (UE) 2018/1241 del Parlamento europeo e del Consiglio del 12 settembre 2018 che modifica il Regolamento (UE) 2016/794 (Regolamento EUROPOL), poi modificato dal Regolamento (UE) 2002/991). Si vedano Turmo (2021) pp. 473 ss.; Rota (2020), pp. 131 ss.
[58] Simili programmi sono presenti in altri Paesi, primi fra i quali, gli Stati Uniti, con il loro ESTA (*Electronic System for Travel Authorization,* per cui si consulti il *link www.esta.cbp.dhs.gov/*) e il Canada, con l'eTA Program (*Electronic Travel Autorisation*, per cui si consulti il *link www.canada.ca/en/immigration-refugees-citizenship/services/visit-canada/eta.html*).
[59] Il Considerando n. 40 del Regolamento ETIAS, difatti afferma: "(A)ai fini della lotta contro i reati di terrorismo e altri reati gravi e tenuto conto della globalizzazione delle reti criminali, è fondamentale che le autorità designate competenti per la prevenzione, l'accertamento e l'indagine di reati di terrorismo e altri reati gravi ("autorità designate") dispongano delle informazioni necessarie per svolgere efficacemente i loro compiti. L'accesso ai dati contenuti nel VIS per tali finalità si è già dimostrato efficace nell'aiutare gli investigatori a compiere progressi sostanziali nei casi relativi alla tratta di esseri umani, al terrorismo o al traffico di droga. *Il VIS non contiene dati sui cittadini di Paesi terzi esenti dall'obbligo di visto*" (corsivo nostro). Si consideri che attualmente i Paesi i cui cittadini non necessitano di un visto per entrare nell'Unione europea sono 60. Per una panoramica sui Paesi che necessiteranno di uno *screening* Etias, su quelli parte dello *European Free Trade Association Schengen Agreement* (EFTA), sui futuri Paesi Schengen (Bulgaria, Croazia, Cipro, Romania), sui microstati con frontiere aperte (Andorra, Monaco, San Marino, Vaticano) si consulti il link *www.etias.com/etias-countries/*. Per una mappa dei Paesi ETIAS, di quelli che necessiteranno di visto o di visto con ATV (*Airport Transit Visa*), si consulti il *link www.frontex.europa.eu/future-of-border-control/etias/*.

che entrano nell'UE e che sono esenti dall'obbligo del visto[60]. In altri termini, per attraversare una frontiera esterna Schengen, i viaggiatori esenti dal visto dovranno essere in possesso tanto di un documento di viaggio valido quanto di un'autorizzazione ETIAS[61].

Diciamo subito che l'entrata in funzione di ETIAS è stata rimandata ormai ben tre volte (una prima volta dal 2022 al gennaio 2023, una seconda al maggio 2023 e una terza a novembre 2023)[62]. Ciò che in questa sede più interessa è che l'ETIAS rappresenta uno degli esempi più vividi di compresenza di poteri e finalità di natura *latu sensu* amministrative e penali, tra loro intercomunicanti proprio per mezzo dell'interoperabilità delle banche dati costruita nel Regolamento[63]. Non c'è dubbio che il Regolamento ETIAS[64], nel puntare formalmente alla protezione delle frontiere esterne dell'Unione, miri a creare una cornice giuridica unitaria e completa, in cui sono già presenti il Regolamento EES[65], la nota Direttiva PNR[66] (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), nonché la Direttiva API[67], queste ultime due, peraltro in fase di revisione[68]. Il sistema ETIAS opererà, per dirla, in prima approssimazione, una valutazione preliminare dei viaggiatori che beneficiano dell'accesso senza visto all'area Schengen, consentendo così agli Stati membri di negare l'autorizzazione ai viaggiatori che, in seguito allo *screening* preliminare effettuato, risultino essere considerati una minaccia per la sicurezza o un rischio in relazione alla migrazione irregolare e alla salute pubblica[69].

ETIAS garantirà l'interoperabilità con altri sistemi informatici, ovverosia il SIS II, il si-

[60] La decisione relativa all'attraversamento della frontiera esterna spetta allo Stato membro dell'UE di prima destinazione.

[61] Dal punto di vista pratico i soggetti che non hanno diritto all'ETIAS o non sono in possesso di un passaporto di un Paese dell'UE avranno bisogno di un visto Schengen per entrare nell'UE. Il tempo per la valutazione ed emissione dell'ETIAS richiederà fino a 96 ore, mentre un visto Schengen può richiedere diverse settimane. La richiesta di un visto Schengen costerà molto di più di un ETIAS.

[62] Ciò vale a dire che gli individui potranno richiedere l'ETIAS tra maggio 2023 e novembre 2023, ma l'approvazione ETIAS sarà richiesta solo da novembre 2023.Varie sono le ragioni degli slittamenti: innanzitutto la necessità di enormi sforzi tecnici necessari per realizzare l'interoperabilità delle banche dati e la messa a disposizione in tutti in punti d'accesso dell'Unione. In secondo luogo le pressioni degli intermediari e dei fornitori di servizi nel settore dei viaggi, in particolare quelli che forniscono servizi di viaggi verso i Paesi dell'Unione europea, quali ad esempio, Eurostar ed Eurotunnel.

[63] Di "*Element of Global Information System*" parla Turmo (2021), p. 477.

[64] Lo si legge chiaramente anche nel suo primo articolo, i cui commi sembrano giustapporre tali due finalità e funzioni.

[65] Regolamento (UE) del Parlamento Europeo e del Consiglio del 30 novembre 2017 che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di Paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i Regolamenti (CE) n.767/2008 e (UE) n. 1067/2011.

[66] Direttiva (UE) 2016/681del Parlamento Europeo e del Consiglio del 27 aprile 2016 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.

[67] Si tratta della direttiva 2004/82/EC del 29 aprile 2004, relativa agli obblighi per i vettori di comunicare i dati relativi alle persone trasportate, cosiddetta API *Directive* ("*Advance Passenger Information*"). Essa impone ai vettori aerei l'obbligo di trasmettere, su richiesta, i dati dei passeggeri allo Stato membro di destinazione prima del decollo del volo, per i voli in arrivo da un paese terzo, per migliorare i controlli alle frontiere e combattere l'immigrazione clandestina. Consente inoltre agli Stati membri di utilizzare i dati API a fini di contrasto.

[68] I risultati preliminari delle consultazioni in corso per la riforma della Direttiva API hanno mostrato che se i dati della Direttiva possono certamente essere usati a fini di *law enforcement* ai sensi del diritto nazionale, essa non specifica tuttavia né condizioni né tutele nell'ambito di tale trattamento. Peraltro, la direttiva *Passenger Name Record* (PNR) prevede disposizioni sull'uso dei dati API a fini di contrasto e tale incrocio crea incertezze tanto per gli individui, quanto per le autorità nazionali. La direttiva non specifica, poi, per quali voli devono essere raccolti i dati, ma lascia spazio agli Stati membri, precisando che i vettori hanno l'obbligo di trasmettere i dati solo per i voli extra Schengen in entrata. Inoltre, la direttiva non tiene pienamente conto delle evoluzioni normative dell'UE in materia di sicurezza delle frontiere e protezione dei dati (codice frontiere Schengen, sistema di ingressi/uscite (EES), ETIAS, Interoperabilità, GDPR, Direttiva LED). E dunque, a titolo esemplificativo, nell'ambito dell'EES e dell'ETIAS, gli stessi dati biografici saranno utilizzati per verificare se un cittadino di un paese terzo che si reca alle frontiere esterne Schengen abbia un'autorizzazione ETIAS o di un visto valido per salire su un aereo, nave o bus. Inoltre, i risultati preliminari della revisione attualmente in corso della direttiva PNR mostrano l'utilità di combinare i dati API e PNR al fine di rafforzare l'affidabilità e l'efficacia dei dati PNR. Si ritiene, difatti, che l'uso combinato di dati API e PNR migliori la qualità dei dati, limitando il numero di falsi positivi attualmente riscontrati dalle unità di informazione sui passeggeri nell'automazione del trattamento dei dati PNR e quindi abbassi il numero di verifiche manuali da effettuare.

[69] Secondo Turmo (2021), p. 477, sebbene ETIAS sembri essere un sistema informativo unico e nuovo, a ben guardare si può affermare che esso non sia altro che un filtro aggiunto a una rete sempre più fitta, frutto dell'integrazione capillare dei diversi sistemi informativi europei.

stema di entrata-uscita (EES)[70], il VIS[71], EURODAC[72] e le banche dati EUROPOL e INTERPOL, sebbene, però, tale interoperabilità non sia definita compiutamente nell'art. 11 del Regolamento ETIAS. Il comma 2 della disposizione prevede difatti che le modifiche agli atti normativi di abilitazione dei sistemi informativi dell'UE necessarie per stabilirne l'interoperabilità con l'ETIAS, nonché l'aggiunta delle corrispondenti disposizioni del regolamento, dovranno essere oggetto di un atto giuridico separato.

Sono previsti dal Regolamento tre supporti al funzionamento di ETIAS: il portale di ricerca europeo, il *Common Identity Repository* e un rilevatore di identità multiple[73]. Ciò che è certo è che l'interoperabilità delle banche dati copre congiuntamente sia settori di cooperazione di polizia e giudiziaria in materia penale, sia i settori dell'asilo e immigrazione, sebbene queste aree siano disomogenee per trattamento giuridico ed aspetti politici.

In buona sintesi, come anticipato, la funzione di ETIAS è almeno in prima battuta preminentemente amministrativa, consistendo essa nella valutazione del rischio che l'ingresso nell'UE da parte del richiedente comporterebbe. Sono a tal fine individuati tre fattori di rischio. Accanto a quello di immigrazione irregolare e di diffusione epidemica, in cima alla lista, l'art. 1, comma 1, del Regolamento posiziona proprio il rischio "per la sicurezza". Cercando di dare una definizione di tale ultimo rischio, poi, l'art. 3, comma 1, punto 6, si riferisce ad un "un rischio di minaccia per l'ordine pubblico, la sicurezza interna o le relazioni internazionali di uno degli Stati membri".

Come si vede bene, oltre ad essere estremamente vaga[74], tale definizione reca un arretramento esponenziale di concetti che sono già di per loro anticipatori, in quanto si riferisce ad un "rischio di minaccia". I due termini sembrano cioè fare l'uno da moltiplicatore dell'altro, consentendo di arrivare ad un grado di astrazione potenzialmente illimitato[75].

7. Due esempi di poteri informativi e parainvestigativi di "autorità amministrative": le *Financial Intelligence Unit* per la "sicurezza" nell'"*Anti-Money Laundering and Financing of Terrorism*".

Il modello dello spostamento indietro dalla "giustizia" (e dall'indagine tradizionale) all'"os-

[70] Il Regolamento (UE) 2017/2226 istituisce un sistema di ingressi/uscite (EES) per la registrazione dei dati relativi ai cittadini di Paesi extra-UE che attraversano le frontiere esterne dell'Unione europea e il Regolamento (UE) 2017/2225 modifica il codice frontiere Schengen per quanto riguarda l'uso del sistema di ingressi/uscite. Il primo, crea per l'appunto un sistema di ingressi/uscite centralizzato per i cittadini di Paesi extra-UE che attraversano le frontiere esterne dell'Unione europea per un soggiorno di breve durata. L'EES è un sistema IT automatico che sostituisce il sistema di apposizione manuale del timbro sul passaporto, dispendioso in termini di tempo, non affidabile però sull'attraversamento dei valichi di frontiera e per il rintracciamento dei soggiornanti fuori termine. Il sistema si inserisce nel quadro della prevenzione del terrorismo e dei reati gravi. Il regolamento (UE) 2017/2226 modifica molte fonti dell'Unione: la Convenzione di Applicazione dell'Accordo di Schengen; i regolamenti sul Sistema di Informazione Visti (VIS) e sull'Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà sicurezza e giustizia (eu-LISA); e, come detto innanzi, modifica anche il codice frontiere Schengen, che stabilisce le condizioni, i criteri e le norme dettagliate per l'attraversamento delle frontiere esterne dell'Unione.

[71] Si tratta del Sistema di informazione visti, aggiornato più volte. Si veda il Regolamento (CE) n. 767/2008 concernente il Sistema di Informazione Visti e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (Regolamento VIS). Si veda anche la nota precedente.

[72] Cfr. Regolamento (UE) 603/2013 che istituisce l'EURODAC, la banca dati dell'Unione per il confronto delle impronte digitali dei richiedenti asilo (originariamente creato nel 2000, con regolamento (CE) n. 2725/2000 del Consiglio, ed operativo dal 2003.

[73] Il portale di ricerca europeo svolge la funzione di portale unico o "mediatore di messaggi" connesso al sistema ETIAS. Tale infrastruttura centrale includerà una interfaccia di ricerca per gli utenti autorizzati (a ciascun *database* presente) rendendola in grado di ricercare contemporaneamente più sistemi di dati (alfanumerici o biometrici) relativi a persone fisiche o ai loro documenti di viaggio. Gli utenti otterranno quindi dati grezzi combinati su un'unica schermata senza dover eseguire ricerche separatamente su ciascuna sistema pertinente. La risposta, dunque, indicherà a quale sistema d'informazione o banca dati dell'UE appartengono i dati. L'eu-LISA conserverà le registrazioni di tutte le operazioni di trattamento dei dati effettuate in questo Portale di ricerca europeo. Quanto al "*Common Identity Repository*", questo conserverà i dati biografici e biometrici di cittadini di Paesi terzi, che siano registrati nei sistemi già esistenti con l'intento di facilitare la combinazione delle ricerche (si veda il Considerando 24 del Regolamento ETIAS). Un indicatore di "*matching*" segnalerà se vi sono dati conservati in uno dei sistemi connessi, consentendo di trovare identità multiple. L'interoperabilità prevista (dal Regolamento 818/2019 citato) anche per lo *European Criminal Records Information System for Third-Country Nationals* (ECRIS-TCN) è assai interessante poiché realizzerà una base di ricerca comune con un sistema "hit/no hit" che completerà il già esistente *EU Criminal Records Database* (ECRIS) dei cittadini non UE condannati nell'Unione (così come previsto dal Regolamento 816/2019).

[74] Mitsilegas e Mouzakiti (2020), p. 129.

[75] Qui si innestano le potenzialità di valutazione del rischio tramite intelligenza artificiale e *big data*, implementabili come detto nel Sistema ETIAS. Come noto, uno dei campi in cui più valorizzato è il ricorso agli algoritmi è quello del *risk assessment*, che (la dottrina americana) intende come valutazione prognostica del rischio-recidiva di un imputato e della sua pericolosità sociale. Attualmente risultano utilizzati circa 400 *risk assessment tools.* Si veda, Zingales (2021), *passim*.

servazione monitorante" si riscontra appieno nell'ambito del controllo a fini di prevenzione del riciclaggio di danaro[76] e del finanziamento del terrorismo, costruito intorno ad un concetto cardine, quello di "operazione sospetta", la quale fa scattare trasferimenti e scambi di comunicazioni oltre che dati ad esse relativi. La normativa europea in merito, più volte (e variamente) rimpolpata[77], creava le Unità centrali nazionali (*Financial Intelligence Unit*, FIU), affidando loro i compiti di ricezione e analisi delle segnalazioni di operazioni sospette[78] e delle altre informazioni rilevanti in materia di riciclaggio, finanziamento del terrorismo e reati ad essi connessi a detti reati presupposto[79]. Diciamo subito anche che la *Riforma EUROPOL*, col nuovo art. 4, comma 1, lett. z), ha previsto lo scambio informativo e la collaborazione diretta, o tramite punto di contatto, con le FIU.

Nell'ambito del margine di apprezzamento lasciato al legislatore nazionale – con la possibilità di configurare la FIU quale autorità amministrativa, struttura specializzata delle forze di polizia o, ancora, struttura incardinata nell'ambito dell'Autorità giudiziaria – alcuni Paesi adottavano soluzioni miste[80]. L'Italia recepiva le direttive del 2005 con il d.lgs. 21 novembre 2017, n. 231 (c.d. decreto antiriciclaggio). Il suo articolo 6 (poi rinnovato, tuttavia) disciplina l'Unità di informazione finanziaria (UIF): istituita presso la Banca d'Italia, essa rappresenta un'Autorità autonoma e operativamente indipendente.

Ai sensi del comma 4 della detta disposizione, oltre a ricevere le segnalazioni di operazioni sospette ed effettuare l'analisi dei flussi finanziari (lett. a) e b)); essa può sospendere, per un massimo di cinque giorni lavorativi, operazioni sempre sospette, anche su richiesta di un'altra

[76] Concordemente, Bergström (2018), pp. 418 ss.

[77] La storia delle politiche di prevenzione e repressione dell'*Anti- Money Laundering* (AML) inizia alla soglia della nascita dell'Unione europea, già dal 1991, con la "prima direttiva AML", per essere poi seguita nel 2001, nel 2006, nel 2015 e nel 2018, rispettivamente, dalla seconda, terza, quarta e quinta direttiva AML. La quarta direttiva del 2015 regolava più specificamente il trattamento dei dati personali da parte delle *Financial Intelligence Unit* (FIU) e accresceva la capacità di cooperazione di queste, puntando a garantire un accesso tempestivo e illimitato da parte delle FIU ai dati finanziari rilevanti, al fine di consentire alle stesse di operare con urgenza. La medesima direttiva obbligava, tra l'altro, gli enti interessati a inoltrare alle FIU ogni informazione necessarie. La Direttiva prevedeva, ancora, che le FIU potessero scambiare informazioni liberamente, spontaneamente o su richiesta, con entità di Paesi terzi. Subito dopo gli attentati terroristici di Parigi e Bruxelles (e lo scandalo *Panama Papers*), si avviò il lavoro che poi condusse alla quinta direttiva, adottata nel maggio 2018. Essa mirava a rafforzare ancora la cooperazione tra autorità nazionali nonché migliorare la cooperazione transfrontaliera, così da consentire alle FIU di ottenere informazioni da qualsiasi soggetto obbligato, anche in assenza di un precedente deposito di transazioni sospette (si vedano, Bergström (2011), pp. 97 ss.; Quintel (2022), pp. 54 ss.). Nel 2018, per completare la quinta direttiva fu emessa la Direttiva 2018/1763, al fine di contrastare il riciclaggio attraverso il diritto penale, sulla base dell'articolo 83, paragrafo 1 TFUE nonché, la Direttiva (UE) 2019/1153, recante norme che facilitano l'uso di informazioni finanziarie e di altro tipo per la prevenzione, l'accertamento, l'indagine o il perseguimento di determinati reati. Oltre a fornire nuovi strumenti per l'ottenimento d'informazioni dagli enti registrati, la Direttiva cerca di estendere lo scambio di informazioni di carattere finanziario al più ampio spettro dei *serious crime* e contiene misure per facilitare l'accesso da parte delle FIU alle informazioni della sfera del *law enforcement*. Essa, difatti, ha la sua base giuridica nell'art. 87, par. 2 TFUE, e punta proprio a che le FIU degli Stati membri scambino informazioni relative al terrorismo o all'"*organised crime*" e rispondano alle richieste EUROPOL (artt. 9 e 12, Dir. 2019/1153).
Da ultimo, nel luglio 2021, la Commissione ha proposto un pacchetto legislativo per rafforzare le norme dell'UE in materia di AML e CFT, che consiste in quattro proposte riguardanti, tra l'altro, la creazione dell'AMLA (*Anti-Money Laundering Autority*), un'altra Autorità indipendente UE (per cui si veda il *link www.finance.ec.europa.eu)*. In sintesi, come accennato nel testo, l'asse della normativa in materia AML/CTF è passato dall'essere focalizzato (specie l'AML) sul mercato unico all'essere centrato prevalentemente, forse, sul diritto penale. Ovviamente questo si riverbera sulle modalità di raccolta e scambio dei dati personali, dal momento che, laddove le disposizioni AML/CTF che fanno riferimento anche alle FIU aggancino la loro base giuridica nell'articolo 87, par. 2, TFUE, si potrebbero applicare, nella attività di trattamento, le norme sulla protezione dei dati delle forze dell'ordine, vale a dire la Direttiva LED anziché il GPDR.

[78] Precisamente l'art. 1, n. 18 della direttiva del 2018 aggiungeva all'art. 32 della precedente direttiva citata il seguente comma: "9. (F)fatto salvo l'articolo 34, paragrafo 2, nell'ambito delle sue funzioni, ogni FIU deve essere in grado di richiedere, ottenere e utilizzare informazioni da qualsiasi soggetto obbligato ai fini di cui al paragrafo 1 del presente articolo, anche laddove non sia stata trasmessa una segnalazione prevista dall'articolo 33, paragrafo 1, lettera a), o 34, paragrafo 1". Si veda, attualmente l'art. 17 della Proposta di sesta direttiva antiriciclaggio (per la quale si veda il *link www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0423*). Secondo la descrizione del *Commettee of Experts on the Evaluation of anti-Money Laundering and Financing of Terrorism - MONEYVAL*, reperibile al *link www.coe.int/en/web/moneyval/implementation/fiu* "*(T)the FIUs therefore function as an intermediary between the private entities, subject to AML/CFT obligations, and law enforcement agencies*". La storia delle FIU, non limitata al contesto europeo, ma esistente a livello di organizzazioni informali già da circa 100 anni ed è sfociata poi nel cosiddetto *Egmont Group*. Si veda, Egmont Group (1995), pp. 1 ss. In dottrina, si vedano, Gilmore (1999), p. 103; Gialuz (2022), pp. 325 ss.

[79] In prospettiva, occorre tener presente che i principali compiti della UIF, ai sensi dell'art. 17 della Proposta sesta Direttiva antiriciclaggio, citata alle note precedenti, sono la prevenzione, l'individuazione e il contrasto efficace del riciclaggio di denaro e del finanziamento del terrorismo. Ai sensi dell'articolo 18, paragrafo 1, lettera c), della proposta di direttiva, le FIU, ai fini delle loro analisi operative, hanno accesso diretto o indiretto alle informazioni di contrasto. Sembrerebbe dunque che le FIU potrebbero aver accesso diretto alle banche dati a disposizione della polizia nazionale e/o delle agenzie di *intelligence* al fine di utilizzare successivamente tali dati per le loro analisi. Tale trattamento analitico delle informazioni delle forze dell'ordine, ricondurrebbe dunque all'applicazione della LED. Si veda, sui problemi dell'applicabilità del GPDR o della LED nei vari Paesi UE, a seconda dell'ambito materiale oltre che della qualificazione delle FIU quali autorità competenti di *law enforcement*, Quintel (2022) pp. 58 ss.

[80] Per un'analisi di tali architetture e per qualche esempio delle diverse opzioni in altri Paesi (nel contesto anche internazionale), come pure per una panoramica di alcuni Paesi in cui le FIU dispongono di poteri di blocco delle transazioni e congelamento dei i conti, si veda International Money Fund, World Bank (2004), pp. 9 ss.

unità di informazione, ove non ne derivi pregiudizio per il corso delle indagini (lett. c) [81]; può effettuare verifiche, "anche attraverso ispezioni", al fine di accertare il rispetto delle disposizioni in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, con riguardo alle segnalazioni di operazioni sospette e ai casi di omessa segnalazione di operazioni sospette, nonché con riguardo alle comunicazioni previste dallo stesso decreto e ai casi di omissione delle medesime, anche avvalendosi della collaborazione del Nucleo speciale di polizia valutaria della Guardia di finanza (lett. f); può poi accertare e contestare ovvero trasmettere alle autorità di vigilanza di settore, le violazioni degli obblighi del detto decreto di cui venga a conoscenza nell'esercizio delle proprie funzioni istituzionali. Sempre la detta "Unità" assicura, poi, informative alla direzione nazionale antimafia e antiterrorismo (*ex* art. 6, comma 5, decreto antiriciclaggio); inoltre, per svolgere tutte le funzioni e i compiti ad essa attribuiti dall'art. 6, commi 4 e 5 del detto decreto, è garantito ad essa l'accesso all'anagrafe tributaria, a quella immobiliare e alle apposite sezioni del registro delle imprese.

Vi sono poi delle vere e proprie osmosi tra attività "amministrativa" della stessa "Unità" e attività delle altre pubbliche amministrazioni[82], degli organismi di autoregolamentazione[83], delle autorità investigative (Direzione antimafia e antiterrorismo, Nucleo speciale di polizia valutaria della guardia di finanza, Direzione investigativa antimafia) nonché degli organismi di informazione per la sicurezza della Repubblica di cui alla legge 3 agosto 2007, n. 124.

Ovviamente ciò si trasfonde, lo ribadiamo, nell'osmosi tra "dati" trasmessi ed elementi probatori.

L'ordito si rintraccia nel combinato disposto degli artt. 8, 9, 10, 40 e 41 del decreto antiriciclaggio. Difatti, è previsto che l'"Unità" invii alla Direzione nazionale antimafia e antiterrorismo, per il tramite del Nucleo speciale di polizia valutaria della Guardia di Finanza ovvero, per quanto attinente alle segnalazioni relative alla criminalità organizzata, per il tramite della Direzione investigativa antimafia[84], i "dati attinenti alle segnalazioni sospette e relativi ai dati anagrafici dei soggetti segnalati o collegati, necessari per la verifica della loro eventuale attinenza a procedimenti giudiziari in corso" oltre alle "informazioni necessarie all'individuazione di possibili correlazioni tra flussi merceologici a rischio e flussi finanziari sospetti", ricevendo dalla Direzione nazionale (salvo il segreto investigativo), il riscontro dell'utilità di dette informazioni. Le modalità e le tempistiche di trasmissione sono rimesse però ai Protocolli stipulati tra le autorità comunicanti. Una stretta collaborazione informativa e operativa è poi prevista dall'art. 9, anche con il detto Nucleo speciale di polizia valutaria, che attua le priorità strategiche stabilite dal Ministero per l'economia e le finanze, con la DIA e con la guardia di finanza, a cui, peraltro, vengono espressamente attribuiti autonomi poteri ispezioni, controlli e approfondimenti delle segnalazioni sospette emesse dall'"Unità", ai sensi dell'art. 40 ("anche con i poteri attribuiti al Corpo dalla normativa valutaria" dice l'art. 9, comma 4, lett. a).

La natura, come detto, *anfibia* delle FIU crea il dubbio sull'applicabilità del GDRP o della LED. In effetti tanto l'assetto normativo europeo attuale quanto quello proposto dal pacchetto antiriciclaggio e antiterrorismo (AML/CTF)[85] non sono limpidi a riguardo. Le FIU sono attualmente istituite e regolamentate ai sensi della quinta direttiva antiriciclaggio, che poggia sulla base giuridica del mercato interno. L'articolo 41 della direttiva stabilisce che si applichi il GDPR, anche se si riferisce solo ai soggetti obbligati a trasferire le informazioni sulle transazioni sospette, senza menzionare le FIU[86]. Invero, non fa chiarezza neanche l'art. 18 della Direttiva 2019/1153 (recante norme per facilitare l'accesso delle autorità competenti alle informazioni finanziarie e di altro tipo), poiché si limita a prevedere che i diritti degli interessati possano essere limitati in conformità con le rispettive norme ai sensi del GDPR e del LED, non spiegando quindi, in base a quale delle due fonti normative le FIU procedano a trattare i dati personali nello svolgimento dei propri compiti. A nostro avviso, in realtà, si può propendere per l'applicabilità della LED: gli artt. 8 e 9 della Direttiva 2019/1153 fanno chiaramente

[81] Oltre che su richiesta del Nucleo speciale di polizia valutaria della Guardia di finanza, della Direzione investigativa antimafia e dell'autorità giudiziaria.
[82] Di cui all'art. 10, d.lgs. 231/2007.
[83] Si veda l'art. 11, d.lgs. 231/2007.
[84] Si veda il combinato disposto degli artt. 8 e 40 d.lgs. 231/2007.
[85] Si veda, *supra*, nota 77.
[86] Si veda il provvedimento della Banca d'Italia adottato il 24 marzo 2020, contenente *"Disposizioni per la conservazione e la messa a disposizione dei documenti, dei dati e delle informazioni per il contrasto del riciclaggio e del finanziamento del terrorismo"*, reperibile in *www.bancaditalia.it*, adottato in applicazione degli artt. 31, 32 e 34, d.lgs. 231/2007, in materia di conservazione dei documenti, dati e informazioni utili. Qui, come si vede, la disciplina articola i differenti concetti di "documento", "dato", "informazione".

riferimento ai dati che devono essere scambiati tra le FIU e le autorità competenti, nonché tra le FIU nei diversi Stati membri. E, sebbene distinguano da una parte le UIF e dall'altra le "autorità competenti", detto scambio riguarda le *informazioni per la prevenzione, l'individuazione e la lotta al riciclaggio di denaro e ai reati presupposto associati o* l'*analisi di informazioni relative al terrorismo o alla criminalità organizzata associata al terrorismo*.

Detto trattamento non può non esser definito come effettuato per finalità di contrasto[87].

Un'ulteriore conferma dell'accrescimento delle competenze preventive e investigative "concorrenti" è data dalla stipula in data 8 giugno 2022 di un Memorandum d'Intesa (*Memorandum of Understanding*, MoU), tra l'Unità italiana e l'EPPO, con l'intento di facilitare la cooperazione tra le due Autorità in relazione ad "*all suspicious financial transactions*". L'intesa, che rappresenta il primo esempio nell'Unione europea, contiene principi e regole per lo scambio di informazioni e supporto analitico, oltre che sulle sospensioni di transazioni, sulla *data protection* oltre che sulle iniziative formative.

7.1. Segue: *l'Autorità investigativa per la sicurezza dell'aviazione civile (ANSV) e l'Agenzia europea per la sicurezza aerea (AESA).*

Sin dalla creazione di un mercato unico del trasporto aereo si profilava la necessità di garantire ai passeggeri un elevato ed uniforme livello di sicurezza, ragione per la quale normative e autorità nazionali venivano affiancate via via dalla normativa europea e dall'Agenzia investigativa per la sicurezza dell'aviazione civile nonché dall'Agenzia europea per la sicurezza aerea.

In effetti, le competenze in materia di Sicurezza e *Safety* sono distribuite tra le due Autorità attraverso un complesso sistema di fonti, normative entro il quale spiccano, in primo luogo, il Regolamento 996/2010[88] e, in secondo luogo, il Regolamento 1139/2018[89], con le connesse normative di attuazione in sede nazionale.

Il primo dei regolamenti prevede poteri autonomi ed incisivi in capo alle Agenzie nazionali di riferimento (autorità investigative per la sicurezza dell'aviazione civile)[90]. I suoi art. 1 e 5 chiariscono come oggetto del Regolamento sia il miglioramento della sicurezza del settore aereo e la garanzia di un elevato livello di efficienza, tempestività e qualità delle inchieste di sicurezza dell'aviazione civile europea, specificando pure come "l'unico obiettivo" sia la prevenzione di futuri incidenti e inconvenienti e non l'attribuzione di "colpe o responsabilità"[91].

Affermato in tal modo il discrimine tra profilo punitivo e repressivo e profilo "preventivo", il Regolamento si focalizza poi nella specificazione dell'autonomia e dell'indipendenza funzionale delle autorità investigative per la sicurezza dell'aviazione civile *ex* art. 5, rispetto alle altre autorità aeronautiche e, in generale, rispetto a "qualsiasi altra parte o ente i cui interessi o finalità possano entrare in conflitto con il compito ad essa assegnato o influenzarne l'obiettività" (art. 4, comma 2). Peraltro, è pure prescritto che detta autorità non possa sollecitare né ricevere istruzioni da alcun soggetto esterno e goda di "autorità illimitata sulla condotta delle inchieste di sicurezza" (art. 4, comma 3), e che i compiti affidati all'autorità investigativa per

[87] Quintel (2022), nt. 99. Secondo l'A., ove le FIU trattino le informazioni delle forze dell'ordine, si dovrebbe applicare la LED (anche se non soddisfano la qualifica soggettiva della LED stessa) tramite la sua estensione attraverso l'ambito materiale d'azione. L'A. mette, altresì, in evidenza l'ambiguità del combinato disposto degli artt. 7 e 4 della citata direttiva 1153/2019.

[88] Regolamento (UE) 996/2010 del Parlamento europeo e del Consiglio del 20 ottobre 2010 sulle inchieste e la prevenzione di incidenti e inconvenienti nel settore dell'aviazione civile e che abroga la direttiva 94/56/CE.

[89] Citato alla nota precedente.

[90] Giustificati dal Considerando n. 36 in forza del principio di sussidiarietà di cui all'art. 5 TUE. L'art. 4, comma 1, del Regolamento prevede che ciascuno Stato membro provveda affinché le inchieste in materia di sicurezza siano condotte o vigilate, senza interferenze esterne, da un'autorità investigativa nazionale permanente per la sicurezza dell'aviazione civile o sotto il controllo di tale autorità ("autorità investigativa per la sicurezza") in grado di condurre in modo indipendente, un'inchiesta di sicurezza completa, o per conto proprio o mediante accordi con altre autorità investigative per la sicurezza.

[91] Ogni inchiesta "di sicurezza" si conclude con una relazione sul tipo e sulla gravità dell'incidente o dell'inconveniente grave e può contenere, ove opportuno, raccomandazioni di sicurezza, che consistono in una proposta formulata a fini di prevenzione. Queste non costituiscono, tuttavia, presunzioni di colpa o attribuzioni di responsabilità per un incidente, inconveniente grave o inconveniente (cfr. art. 17, comma 3, Regolamento 996/2010). Peraltro, la relazione garantisce l'anonimato di coloro che siano stati coinvolti nell'incidente o nell'inconveniente grave (cfr. art. 16, comma 2, Regolamento 996/2010). Per un esempio di relazione stilata dall'Autorità italiana, si veda il *link www.ansv.it/wp-content/uploads/2020/07/Relazione-I-CICO.pdf*.

la sicurezza[92] possano essere estesi alla raccolta e all'analisi di informazioni relative alla sicurezza aerea, in particolare a fini di prevenzione degli incidenti, nella misura in cui tali attività non compromettano la sua indipendenza e non comportino alcuna responsabilità di carattere regolamentare, amministrativo o normativo.

Tale assetto fa evidentemente sorgere interrogativi in merito alla concorrenza dei poteri rispetto a quelli dell'autorità giudiziaria. I dubbi sono incalzati peraltro, non solo dalla "obbligatorietà" dell'iniziativa prevista dalla fonte europea (art. 5, comma 1) ma, soprattutto, dalla discrezionalità a disposizione dell'Autorità indipendente. Beninteso, il comma 5 della disposizione in parola afferma che le inchieste "sono condotte indipendentemente e separatamente da eventuali procedimenti giudiziari o amministrativi finalizzati all'accertamento di colpe o responsabilità", e che esse non devono "tuttavia arrecare pregiudizio a tali procedimenti". A disciplinare la contemporaneità delle inchieste, è stato posto tuttavia l'art. 12 del Regolamento. Esso fornisce una disciplina piuttosto dettagliata, volta proprio a prevenire detto pregiudizio, avendo di mira i profili più delicati, ovverosia quelli in cui viene in questione la salvaguardia degli elementi probatori. Esso si ispira in prima battuta al principio di leale collaborazione tra le due Autorità, prevedendo al comma 3, che vengano stipulati appositi accordi di coordinamento.

Tali accordi devono rispettare, ai sensi del detto art. 12, comma 3, l'indipendenza dell'Autorità responsabile per le inchieste di sicurezza e devono consentire che l'inchiesta tecnica sia condotta con diligenza ed efficienza. Gli accordi, inoltre, devono prendere in considerazione (quanto meno) le questioni strategiche, e più sensibili, nell'interazione tra inchiesta amministrativa e giudiziaria, ovverosia: l'accesso al luogo dell'incidente; la conservazione delle prove e l'accesso alle stesse; i resoconti iniziali e relativi poi a ciascuna operazione; gli scambi d'informazioni; l'utilizzo appropriato delle informazioni di sicurezza e, infine, devono disciplinare anche le modalità di risoluzione degli eventuali conflitti. Una previsione altamente significativa, nell'ambito dell'equilibrio e nella distribuzione dei poteri nel multilivello, è poi quella per cui gli Stati membri devono comunicare tali accordi alla Commissione la quale, a sua volta, dovrà comunicarli al presidente della rete delle autorità per la sicurezza del volo, al Parlamento europeo e al Consiglio, al fine di assicurare adeguata "informazione".

Occorre poi ricordare come il detto art. 12, preveda pure che, qualora l'intesa nel singolo caso non sia raggiunta sulla base di detti accordi entro un termine ragionevole, e non superiore alle due settimane successive alla richiesta, non è impedito all'"investigatore" dell'autorità di sicurezza effettuare comunque l'esame o l'analisi. Tuttavia, ove l'autorità giudiziaria abbia il diritto di sequestrare eventuali prove, "l'investigatore" avrà accesso immediato e illimitato a tali prove e potrà utilizzarle.

Come si vede, un equilibrio retto da un filo molto sottile, la tenuta del quale dipende tuttavia nella pratica in larga misura dalla capacità di leale cooperazione tra la magistratura e l'Autorità "amministrativa".

In Italia l'Autorità incaricata ai fini del Regolamento 996/2010 è l'Autorità nazionale per la sicurezza del volo (ANSV)[93]. Proprio al fine di evitare dannose sovrapposizioni, essa aveva, già nel 2014, stipulato gli accordi di cui all'art. 12, comma 3, con il Ministero della Giustizia[94] e, alla fine del 2015, risultava aver stipulato accordi con tutte le 140 Procure della Repubblica presso i Tribunali ordinari, oltre che 6 accordi preliminari con alcune Procure della Repubblica presso i Tribunali per i minorenni[95] (sebbene il testo di tutti questi accordi sottoscritti sia identico a quello preliminare originariamente predisposto dall'ANSV e dal Ministero della giustizia). Assai interessante rilevare, in effetti, come prima della stipula dei singoli accordi, il rischio di sovrapposizioni tra ANSV e magistratura risultava di gran lunga maggiore, così

[92] Le modalità operative delle autorità investigative per la sicurezza dell'aviazione civile di cui all'art. 4 del Regolamento sono state predisposte prevalentemente nell'ordinamento internazionale (cfr., Allegato 13 alla Convenzione relativa all'aviazione civile internazionale) e poi dell'Unione europea (proprio col Regolamento UE 996/2010). Quest'ultimo ha difatti recepito molti dei principi e previsioni già inclusi nel citato Allegato 13 alla Convenzione relativa all'aviazione civile internazionale (*Annex 13* ICAO).

[93] Già istituita con d.lgs. 25 febbraio 1999, n. 66.

[94] *Rapporto informativo sull'attività svolta dall'ANSV e sulla sicurezza dell'aviazione civile in Italia* 2020, p. 13, consultabile al *link www.ansv.it/wp-content/uploads/2021/04/Rapporto-ANSV-2020.pdf*, p. 11.

[95] Si fa presente, poi, che oltre agli accordi con le autorità giudiziarie, l'Autorità ha altresì stipulato accordi, sempre in virtù di quanto previsto dall'art. 12, paragrafo 3, con il Ministero della difesa-Arma dei Carabinieri; con l'ENAC nonché con l'ENAV S.p.A.

come sembra emergere dalla Relazione per il 2020 dell'Autorità[96].

Completa il quadro dei nuovi equilibri tra poteri l'assetto di sanzioni previste per la violazione delle disposizioni del citato Regolamento. Il decreto legislativo 14 gennaio 2013 n. 18, reca l'attuazione dell'art. 23 della fonte unionale. Essa, difatti, prescrive che gli Stati membri dell'Unione europea "prevedano norme relative alle sanzioni da applicare" per la sua violazione, precisando, altresì, che le sanzioni da irrogare siano "effettive, proporzionate e dissuasive". Il soggetto preposto all'applicazione del decreto legislativo e all'irrogazione delle sanzioni ivi previste è la stessa ANSV (art. 3, comma 1). Esse non puniscono chi abbia provocato l'evento o contribuito al suo accadimento, ma sanzionano invece quei comportamenti che impediscano o mettano a repentaglio il regolare svolgimento delle inchieste di sicurezza, quale l'omessa tempestiva comunicazione, all'autorità investigativa competente (in Italia l'ANSV), del verificarsi di un incidente o di un inconveniente grave, in quanto tale omissione può costituire un grave pregiudizio al regolare avvio dell'inchiesta di sicurezza. L'art. 9 del regolamento 996/2010 (Obbligo di comunicare il verificarsi di incidenti e inconvenienti gravi) prescrive, in effetti, che "(Q)qualsiasi persona coinvolta che è a conoscenza di un incidente o di un inconveniente grave comunic*hi* immediatamente tale informazione all'autorità investigativa competente per la sicurezza". I soggetti passibili di sanzioni, ai sensi dell'art. 2, d.lgs. 18/2013, si identificano con quelli ricompresi nella definizione di persona coinvolta di cui all'art. 2 del Regolamento UE 996/2010 e il procedimento sanzionatorio è quello che (conformemente all'art. 3, d.lgs. 18/2013) è stato deliberato dal Collegio dell'ANSV ed approvato dalla Presidenza del Consiglio dei ministri, previa acquisizione dei prescritti pareri[97].

Anche il secondo dei Regolamenti citati, il n. 1139/2018, ha approntato una disciplina volta a garantire un "livello elevato ed uniforme di sicurezza dell'aviazione civile mediante l'adozione di norme comuni di sicurezza e mediante misure volte ad assicurare la conformità di ogni prodotto, e l'osservanza di ogni persona e organizzazione coinvolte nelle attività dell'aviazione civile nell'Unione riguardo a tali norme comuni"[98]. Come anticipato in apertura, detto Regolamento istituiva anche l'Agenzia europea per la sicurezza aerea, composta dalle Autorità nazionali dell'aviazione civile, dalla Commissione europea e l'Agenzia europea per la sicurezza aerea (AESA)[99]. A partire dal 2003, l'AESA è incaricata in particolare di preparare la regolamentazione del settore (che funge da base per le proposte di atti legislativi della Commissione).

Ai sensi dell'art. 83 del Regolamento 1139/2018, l'Agenzia ha propri poteri investigativi, che sono strumentali all'assolvimento dei compiti connessi alla certificazione e alla sorveglianza, e sono specificati nell'articolo 62, comma 2)[100]. L'Agenzia difatti esegue, *per proprio conto* o tramite le autorità nazionali competenti o i soggetti qualificati, "le indagini necessarie".

[96] Si veda, il Rapporto informativo sull'attività svolta dall'ANSV e sulla sicurezza dell'aviazione civile in Italia 2020, cit. p. 13, ove si afferma che "(L)la puntuale applicazione di quanto contemplato dal regolamento UE 996/2010, nonché dagli accordi preliminari conclusi dall'ANSV con la magistratura requirente, ha (…) contribuito a mitigare, rispetto al passato, i punti di attrito tra inchiesta di sicurezza e di indagine penale, evitando, così, sostanziali penalizzazioni alle inchieste di sicurezza… In particolare, anche nel 2020 non si sono presentati casi che abbiano costretto l'ANSV ad invocare l'applicazione di quanto previsto dall'art. 10 dell'accordo preliminare in questione, relativo alla composizione di eventuali conflitti sorti in sede di applicazione dell'accordo stesso".

[97] Il procedimento in questione (si veda la deliberazione n. 51/2013 adottata con decreto del 23 ottobre 2013) è disponibile nel sito *www.ansv.it*, nel contenitore "(N)notifica incidenti/inconvenienti gravi".

[98] Oltre che ad introdurre un livello elevato ed uniforme di protezione dell'ambiente riguardo a tutto ciò che concerne le attività di trasporto aereo civile.

[99] Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea (e che modifica i Regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i Regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il Regolamento (CEE) n. 3922/91 del Consiglio). Agli artt. 5, 6 e 7 del Regolamento sono previsti, rispettivamente il programma europeo per la sicurezza aerea e il piano europeo e nazionale per la sicurezza aerea. L'art. 75 contempla "(I)istituzione e funzioni dell'Agenzia".

[100] Si riporta, per maggiore intellegibilità il testo dell'art. 62, comma 2: "(P)per garantire l'ottemperanza al presente regolamento e agli atti delegati e di esecuzione adottati sulla base del medesimo, l'Agenzia e le autorità nazionali competenti: a) ricevono e valutano le domande presentate e, se del caso, rilasciano o rinnovano i certificati e ricevono le dichiarazioni ad esse rese, conformemente al capo III; b) effettuano la sorveglianza dei titolari di certificati, delle persone fisiche e giuridiche che hanno reso dichiarazioni e di prodotti, parti, equipaggiamenti, sistemi ATM/ANS e componenti ATM/ANS, dispositivi di addestramento al volo simulato nonché degli aeroporti soggetti al presente regolamento; c) eseguono indagini, ispezioni, comprese le ispezioni a terra, audit e altre attività di sorveglianza necessarie al fine di individuare eventuali violazioni, da parte di persone fisiche o giuridiche soggette al presente regolamento, dei requisiti stabiliti nel presente regolamento e negli atti delegati e di esecuzione adottati sulla base del medesimo; d) per porre fine alle violazioni riscontrate, adottano tutte le misure necessarie atte a garantire l'applicazione delle norme, tra cui la modifica, la limitazione, la sospensione o la revoca dei certificati da essi rilasciati, il fermo operativo di un aeromobile e l'imposizione di sanzioni; e) vietano, limitano o subordinano a determinate condizioni le attività di cui al capo III per motivi di sicurezza; f) garantiscono un adeguato livello di qualifica del personale impegnato nei compiti di certificazione, sorveglianza e applicazione delle norme, anche impartendo l'opportuna formazione.

Sebbene si tratti anche in questo caso di investigazioni effettuate in un contesto "amministrativo", nondimeno le modalità e gli esiti delle stesse sono non per questo poco significativi. Essa è, difatti autorizzata ad effettuare attività di portata anche incisiva, quali "chiedere alle persone fisiche o giuridiche alle quali ha rilasciato un certificato, o che le hanno reso una dichiarazione di fornire all'Agenzia tutte le informazioni necessarie"; oppure "di fornire spiegazioni orali in merito a qualsiasi fatto, documento, oggetto, procedura o altra questione rilevante per determinare se la persona ottempera al presente regolamento e agli atti delegati e di esecuzione adottati sulla base del medesimo"; può inoltre accedere ai locali, terreni e mezzi di trasporto "pertinenti" di tali persone; così come pure esaminare qualsiasi documento, registro o dato pertinente detenuto da (o accessibile a) tali persone, oltre che estrarre copie o prelevare stralci, indipendentemente dal supporto sul quale le informazioni sono archiviate.

Inoltre, ove necessario per determinare se una persona alla quale ha rilasciato un certificato o che le ha reso una dichiarazione abbia ottemperato al Regolamento (e agli atti delegati e di esecuzione adottati sulla base del medesimo), l'Agenzia è pure abilitata ad esercitare le dette indagini suddetti in relazione a qualsiasi altra persona fisica o giuridica di cui si possa ragionevolmente presumere che possieda informazioni pertinenti per tale scopo o che, comunque, possa accedervi.

A puntellare i "poteri" ora descritti, sono state poste due clausole generali di tutela: innanzitutto è detto che essi debbano essere esercitati "nel rispetto del diritto nazionale dello Stato membro o del paese terzo in cui si svolge l'indagine, tenendo in debito conto i diritti e legittimi interessi delle persone interessate e nel rispetto del principio di proporzionalità". In secondo luogo, proprio con riferimento all'attività più invasiva di quelle descritte, sempre ai sensi dell'art. 83, comma 2, Regolamento 1139/2018, è previsto che "se per accedere ai locali, terreni e mezzi di trasporto pertinenti di cui alla lettera c) è necessaria, conformemente al diritto nazionale applicabile, un'autorizzazione preventiva dell'autorità giudiziaria o amministrativa dello Stato membro o del paese terzo in questione, tali poteri sono esercitati soltanto una volta ottenuta l'autorizzazione preventiva". Ai sensi del successivo comma 3, poi, è previsto che l'Agenzia provveda affinché i membri del suo personale e, se del caso, gli altri esperti che partecipano all'indagine siano sufficientemente qualificati, ricevano istruzioni appropriate e siano debitamente autorizzati, oltre che esercitino i loro poteri su presentazione di un'autorizzazione scritta. Ai sensi del comma 4 della disposizione, infine, i funzionari delle autorità competenti dello Stato membro nel cui territorio deve essere condotta un'indagine, assistono nel compimento delle attività su richiesta dell'Agenzia, la quale "se del caso… informa in tempo utile prima dell'indagine lo Stato membro interessato".

8. Il potenziamento di EUROPOL col Regolamento 991 del 2022.

Come noto, con l'entrata in vigore del Trattato di Lisbona, la base giuridica di EUROPOL, individuabile nell'art. 88 TFUE, condusse alla sostituzione della Decisione del Consiglio 2009/371/JHA ad opera del Regolamento EUROPOL[101]. Già quel Regolamento ne esaltava il ruolo di polo informativo, riformando le modalità di scambio coi partner, rinforzando il ruolo di gestione e protezione dei dati (con la creazione di un nuovo organismo parlamentare di controllo); prevedendo sia il diritto d'accesso ai dati personali, sia meccanismi di opposizione e compensazioni per l'eventuale gestione illegittima dei dati stessi.

Abbiamo già detto di come le innovazioni normative già apportate o in cantiere all'interno dell'Unione europea siano state spinte in massima parte dalla transnazionalità dell'agire pericoloso (e penalmente rilevante) e dei dati (prim'ancora che degli elementi probatori) portati dalle rete[102]: dunque, dalla imprescindibilità della collaborazione tra autorità nazionali ed eu-

[101] Adottato l'11 maggio dal Parlamento europeo e dal Consiglio ed entrato in vigore il 1° maggio 2017 in tutti gli Stati membri ad eccezione della Danimarca, che aveva effettuato l'"*opt-out*" dalle previsioni del Trattato relative alla Giustizia e agli affari interni.
[102] Per la spiegazione del mutato contesto criminale e tecnologico si vedano i Considerando 1, 2 3 e 6 del Regolamento (UE) 991/2022 di riforma di EUROPOL. Per il "manifesto" del Regolamento e il riferimento al radicamento nell'art. 4, par. 2, TUE, ai fini della protezione della sicurezza nazionale degli Stati membri, cfr. considerando 4 e 5, anche ai fini del potenziamento delle Unità speciali d'intervento interoperative (di cui alla già presente Decisione 2008/617/GAI del Consiglio, del 23 giugno 2008, relativa al miglioramento della cooperazione tra le unità speciali d'intervento degli Stati membri dell'Unione europea in situazioni di crisi).

ropee e tra Agenzie dell'Unione[103], dalla automazione e interconnessione nella ricerca in enormi moli di dati a disposizione e dalla utilità nel reperimento di informazioni degli operatori privati (in massima parte degli *Internet Service Provider*).

Sebbene alcune di tali esigenze potessero già in qualche modo dirsi soddisfatte dal Regolamento EUROPOL 2017 e dalle intersezioni operative e normative pure recentemente approntate in sede unionale (come si è detto per FRONTEX, EU-LISA, SIS ed ETIAS), il nuovo Regolamento (UE) 991/2022[104], approvato in data 8 giugno 2022, mira proprio a rafforzare gli interventi già effettuati. La riforma probabilmente mira a dirimere una tensione interistituzionale accesasi tra EUROPOL e lo *European Data Protection Supervisor* (EDPS). Il 21 dicembre 2021 lo EDPS firmava una decisione[105]. con la quale si intimava all'EUROPOL, ai sensi dell'art. 18, paragrafo 5 del vigente Regolamento, di cancellare entro sei mesi dalla ricezione della decisione i dati da essa detenuti, che non fossero stati sottoposti alla *Data Subjects Categorisation* (DSC).

La DSC consiste nell'identificazione, all'interno di queste grandi basi di dati, di individui sospettati, contatti e possibili "associati", vittime, testimoni e fonti informative correlate ad attività criminali. Nella sua risposta all'ordine dell'EDPS, EUROPOL affermava che: "*EDPS Decision will impact Europol's ability to analyse complex and large datasets at the request of EU law enforcement. This concerns data owned by EU Member States and operational partners and provided to Europol in connection with investigations supported within its mandate. …Europol's work frequently entails a period longer than six months, as do the police investigations it supports. This is illustrated by some of Europol's most prominent cases in recent years. Europol will seek the guidance of its Management Board and will assess the EDPS Decision and its potential consequences for the Agency's remit, for ongoing investigations as well as the possible negative impact on the* security *for EU citizens*"[106].

I punti cardine dello strumento normativo consentiranno ad EUROPOL innanzitutto di operare mediante il processamento di vaste e complesse basi di dati personali senza la classificazione degli interessati (*Data Subject Categorization*, DSC) proprio a fini di *law enforcement*. Ciò vale a dire che EUROPOL sarà in grado di trattare anche i dati relativi ad individui che non abbiano relazioni con le attività oggetto di indagine, ogni qualvolta sarà necessario per il supporto all'indagine stessa[107].

[103] Si veda, infatti il considerando 8 al Regolamento (UE) 991/2022 di Riforma EUROPOL, ove si afferma che "Europol dovrebbe essere in grado di facilitare e di supportare le iniziative per la sicurezza basate sull'intelligence lanciate dagli Stati membri — come la piattaforma multidisciplinare europea di lotta alle minacce della criminalità (EMPACT) — volte a individuare, classificare in ordine di priorità e affrontare le minacce poste dalle forme gravi di criminalità. Europol dovrebbe essere in grado di prestare a tali iniziative supporto amministrativo, logistico, finanziario e operativo.

[104] Nel detto Programma d'azione del 2020, la Commissione europea annunciava l'intenzione di potenziare il mandato EUROPOL presentando la proposta nel dicembre 2020, quale parte di un pacchetto di misure antiterrorismo. In effetti tale intenzione sarebbe poi stata portata a compimento, proprio ad opera del Regolamento 919/2022. I co-legislatori hanno cominciato il dialogo interistituzionale sulla proposta EUROPOL e il primo incontro di carattere "politico" ha avuto luogo in data 27 ottobre 2021, seguito poi da altri due incontri di tal genere e 6 riunioni "tecniche". L'accordo provvisorio raggiunto il 1° febbraio 2022, è poi stato approvato dal COREPER l'11 febbraio, seguito da quello della Commissione sulle libertà civili, giustizia e affari interni (LIBE) del 16 marzo. Il Parlamento ha adottato la proposta il 4 maggio 2022, con 480 voti favorevoli, 143 contrari e 20 astensioni, seguito poi dal Consiglio il 24 maggio. Il provvedimento è dunque stato firmato in data 8 giugno ed è entrato in vigore il 28 giugno, giorno successivo alla sua pubblicazione.

[105] La "*Decision on the retention by Europol of datasets lacking Data Subject Categorisation*", assunta in forza dell'art. 43, paragrafo 3, del Regolamento EUROPOL che definisce i poteri dello EDPS, fra i quali vi è pure quello di ordinare l'eventuale cancellazione dei dati archiviati e conservati in contrasto con la normativa EUROPOL.

[106] Lo si legga al *link www.europol.europa.eu*.

[107] L'art. 18 prevede, al paragrafo 1, che "(N)nella misura in cui è necessario al raggiungimento degli obiettivi di cui all'articolo 3, Europol può trattare informazioni, inclusi dati personali". Nel paragrafo 2, poi, prevede che "(I)i dati personali possono essere trattati solo a fini di: a) controlli incrociati diretti a identificare collegamenti o altri nessi pertinenti tra informazioni concernenti: i) persone sospettate di aver commesso un reato di competenza di Europol o di avervi partecipato, o che sono state condannate per un siffatto reato; ii) persone riguardo alle quali vi siano indicazioni concrete o ragionevoli motivi per ritenere che possano commettere reati di competenza di Europol; b) analisi strategiche o tematiche; c) analisi operative; d) facilitazione dello scambio d'informazioni tra Stati membri, Europol, altri organismi dell'Unione, Paesi terzi, organizzazioni internazionali e parti private; e) progetti di innovazione e ricerca; f) sostegno agli Stati membri, su loro richiesta, nell'informare il pubblico sulle persone sospettate o condannate che sono ricercate in base a una decisione giudiziaria nazionale relativa a un reato che rientra nell'ambito degli obiettivi di Europol, e agevolazione della comunicazione di informazioni su tali persone, agli Stati membri e a Europol, da parte dei cittadini. La disciplina si comprende solo leggendo anche l'Allegato II al Regolamento. Esso opera una distinzione (indicata con le lettere "A" e "B", tra le Categorie di dati personali e categorie di interessati ai fini dei controlli incrociati di cui all'articolo 18, paragrafo 2, lettera a); e le categorie di dati personali e categorie di interessati ai fini delle analisi strategiche o tematiche, delle analisi operative o della facilitazione dello scambio di informazioni, di cui all'articolo 18, paragrafo 2, lettere b), c) e d). La lettera "A" riguardano non solo persone che, "in base al diritto nazionale dello Stato membro interessato, sono sospettate di aver commesso un reato di competenza di Europol o di avervi partecipato, o che sono state condannate per un siffatto reato, ma anche "persone riguardo alle quali vi siano indicazioni concrete o ragionevoli motivi, secondo il diritto nazionale dello Stato membro interessato, per ritenere che possano commettere reati di competenza di Europol. Invece, le persone a cui si fa riferimento nella lettera "B" sono quelle che, "a norma del diritto nazionale dello

L'aggiornamento del Regolamento concede così all'Agenzia una sorta di capacità di analisi e scrutinio retroattivi: proprio per potenziare l'efficacia del processamento dei dati senza DSC, allargando la mole di informazioni da incrociare, viene cioè data (a certe condizioni) la possibilità di conservare anche i dati raccolti negli anni precedenti, per tutto il tempo e tutte le volte in cui sia richiesto come ausilio per un'indagine[108], sebbene sia stato posto, però, un regime transitorio per le informazioni che sono state trattate da EUROPOL prima delle modifiche al Regolamento.

Di estremo impatto sarà anche la novella in tema di collaborazione coi privati per l'ottenimento di prove elettroniche[109]: l'Agenzia, difatti, sarà in grado di ricevere dati direttamente da coloro che li detengano qualora essi siano reputati rilevanti a scopi d'indagine. A tal fine sono state poste norme specifiche per la cooperazione sia per le "situazioni di crisi *online*" sia casi di diffusione online di materiale pedopornografico. Con "situazioni di crisi *online*" ci si riferisce, poi, alla "diffusione di contenuti online relativi a un fatto in corso o recente del mondo reale che ritraggono un danno alla vita o all'integrità fisica o che richiamano un danno imminente alla vita o all'integrità fisica e che hanno l'obiettivo o l'effetto di intimidire gravemente la popolazione, a condizione che vi sia un legame o un ragionevole sospetto di legame con il terrorismo o l'estremismo violento e che si preveda la moltiplicazione esponenziale e la viralità di tale contenuto tra vari servizi *online*".

Nella consapevolezza degli interessi in gioco, il Regolamento cerca di rinforzare ulteriormente la protezione individuale[110] così come il controllo del Parlamento e la responsabilità dell'Agenzia[111]. Rilevante novità è infatti la possibilità concessa ad EUROPOL di richiedere alle autorità competenti di uno Stato membro, pur in assenza della dimensione transfrontaliera del reato, in casi specifici in cui apprezzi opportuno iniziare un'indagine penale[112], di condurla o coordinarla, nel caso in cui influisca su un interesse comune dell'Unione[113]. Altri punti caratterizzanti riguardano il rinforzo della cooperazione in ambito interno, e in particolare con l'EPPO, e il rinforzo della cooperazione in ambito esterno. A tal riguardo i profili che maggiormente spiccano sono, per un verso, il potenziamento della collaborazione con Paesi terzi a fini antiterroristici e, per un altro, la spinta verso la collaborazione con i privati per l'ottenimento di *e-evidence*.

E non è affatto un caso che la proposta di riforma EUROPOL abbia viaggiato parallela alla proposta di riforma del Regolamento sul già richiamato Sistema di informazione Schen-

Stato membro interessato, sono sospettate di aver commesso un reato di competenza di Europol o di avervi partecipato, o che sono state condannate per un siffatto reato; b) persone riguardo alle quali vi siano indicazioni concrete o ragionevoli motivi, secondo il diritto nazionale dello Stato membro interessato, per ritenere che possano commettere reati di competenza di Europol; c) persone che potrebbero essere chiamate a testimoniare nel corso di indagini sui reati in causa o di procedimenti penali conseguenti; d) persone che sono state vittime di uno dei reati in esame o per le quali taluni fatti autorizzano a ritenere che potrebbero essere vittime di un siffatto reato; e) persone di contatto e di accompagnamento; e f) persone che possono fornire informazioni sui reati in esame". Si vedano pure gli artt. 27-*bis* e 29, del Regolamento EUROPOL.

[108] Questo aspetto è profondamente legato, peraltro, all'altra rilevante novità relativa all'attività di ricerca e sviluppo nell'ambito dell'intelligenza artificiale: si introduce, come anticipato, una base giuridica dedicata al trattamento dei dati personali a fini di ricerca e innovazione, accompagnata da garanzie di protezione dei dati (come la pseudonimizzazione), che saranno applicabili a tale trattamento (cfr. artt. 2, lett. v), e 4, comma 1, lett. v) e w), Regolamento 991/2022). In buona sostanza qui risiede anche la base giuridica per l'utilizzo dell'Intelligenza artificiale da parte di EUROPOL, verosimilmente impiegabile anche a fini di "polizia predittiva.

[109] La disciplina delle "Relazioni coi Partner" è contenuta nel Capo V del Regolamento, negli artt. 23 ss. In particolare, si vedano gli artt. 26, 26-*bis* e 26-*ter* per lo scambio di dati personali con "parti private". L'art. 27 disciplina le "(I)informazioni provenienti da persone private".

[110] È difatti istituito un ufficio indipendente, *il Fundamental Right Officer (FRO),* che affiancherà il responsabile della protezione dei dati (DPO) indipendente, figura già esistente nell'organizzazione di Europol. Si ricorda poi che, nonostante già dal 1° maggio 2017, il GEPD avesse competenza a vigilare sul trattamento dei dati personali da parte di Europol, la riforma del Regolamento abbia previsto un rafforzamento delle funzioni di sorveglianza dello stesso.

[111] Mette conto rilevare come le correzioni relative al rinforzo della protezione nel processo di trattamento dei dati si deve al parere dello *European Data Protection Supervisor* (EDPS) emesso in data 8 marzo 2021 nel quale si raccomandava, tra l'altro, che alcuni concetti nella proposta di Regolamento fossero meglio definiti; che fossero rinforzate le salvaguardie relative alle deroghe rispetto al processamento di *data sets* vasti; e raccomandava anche che venissero proibiti i trasferimenti massivi e strutturali con tutti i privati inclusi nell'UE. Differentemente, lo *European Economic and Social Committee* (EESC), nel suo parere del 9 giugno 2021 (consultabile al *link www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/strengthening-europols-mandate*), non esprimeva preoccupazioni per la proposta di regolamento riguardo ai punti in questione, apprezzando invece l'incremento del budget di Europol per proteggere ulteriormente i cittadini dell'Unione. Cfr., *EDPS Opinion on the Proposal for Amendment of the Europol Regulation,* consultabile al *link www.edps.europa.eu/system/files/2021-03/21-03-08_opinion_europol_reform_en.pdf*.

[112] Si tratta di vere e proprie indagini di iniziativa**.** Beninteso con alcune limitazioni: spetta cioè al direttore esecutivo di Europol proporre l'apertura di un'indagine nazionale su un reato specifico che riguarda un solo Stato membro ma lede un interesse comune coperto da una politica dell'Unione. Saranno però le autorità nazionali a valutare la proposta.

[113] Lo *European Economic and Social Committee* (EESC) nel parere citato alla nota precedente, nel valutare positivamente la proposta di Regolamento, suggeriva addirittura che fosse arrivato il momento "*to allow Europol to act on its own initiative*".

gen[114], in virtù della quale EUROPOL sarebbe in grado di inserire, nel sistema SIS, i dati relativi a sospetti coinvolgimenti di cittadini di Paesi terzi in un'attività per la quale sussista la sua competenza. Come pure anticipato, questa innovazione nei poteri di EUROPOL ha per certi versi superato l'*empasse* del pacchetto normativo sull'ordine di produzione e conservazione delle prove elettroniche di cui s'è accennato.

9. La proposta di un "Codice della cooperazione di polizia" dell'Unione europea per ricomporre frammentazione e concorrenza dei poteri preventivi e investigativi.

Il panorama sia pur tratteggiato a grandi linee dà l'idea della considerevole complessità delle attività di quella che si è definita "osservazione monitorante", oscillante tra il piano della prevenzione, quello dell'indagine e quello della repressione penale nell'Unione europea.

L'impressionante stratificazione normativa prodottasi con il "fiorire" dello Spazio di Libertà, Sicurezza e Giustizia, e la coesistenza di diversi accordi bilaterali, trilaterali e multilaterali, hanno prodotto, come si è visto, una impressionante frammentazione, la quale rischia di divenire pericolosamente disfunzionale[115].

Lo dimostra il primo e ambizioso tentativo di dar vita, nell'Unione europea, ad un "Codice della cooperazione di Polizia": nell'ambito della detta *Security Union Strategy*, la Commissione ha deciso di esplorare tale possibilità tra nell'aprile 2021. Così, il mese successivo, ha effettuato una consultazione pubblica sulla modernizzazione e il miglioramento della cooperazione transfrontaliera[116]. Del pacchetto legislativo volto a fronteggiare tale frammentazione, presentato (sempre dalla Commissione) in data 8 dicembre 2021 fanno parte sia una proposta di Raccomandazione per il Consiglio sulla cooperazione operativa di polizia, volta a fronteggiare gli ostacoli che gli operatori di polizia incontrano nell'operare negli altri Stati membri relativamente a quelle che sono definite "*cross-border hot pursuits, surveillance, joint patrols and other joint operations*", sia una proposta di Regolamento sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II") [117] che stabilisca una nuova architettura tecnica per lo scambio tra le autorità nazionali competenti in tema di profili DNA, dattiloscopici, dati relativi a veicoli, immagini facciali e altri "*record*" di polizia[118] sia, ancora, una proposta di Direttiva sullo scambio informativo tra autorità di *law enforcement* degli Stati membri, che vorrebbe abrogare "l'iniziativa svedese" (portata con la Decisione quadro 2006/960/JHA).

Il Regolamento, ove approvato, andrebbe a modificare, tra l'altro, alcuni strumenti normativi cui s'è accennato, quali il Regolamento eu-LISA (2018/1726) e i Regolamenti per l'interoperabilità tra i sistemi di informazione nel settore delle frontiere e dei visti (2019/817) e nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione (2019/818).

[114] Regolamento (UE) 2018/1862 sul Sistema di informazione Schengen, sulla cui struttura e sulle cui interrelazioni con EUROPOL, si veda, pure, Gialuz (2022), pp. 322 ss.

[115] Si vedano le Valutazioni contenute nelle premesse alla *Proposta di Regolamento del Parlamento e del Consiglio sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II"), che modifica le decisioni 2008/615/GAI e 2008/616/GAI del Consiglio e i regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818*, derivante dalla chiusura della procedura di consultazione pubblica, rinvenibile al sito *www.ec.europa.eu*. 3, p. 6.

[116] Consultabile al *link www.europa.ew/info/law/better-regulation/have-your-say/initiatives/12614-Codice-di-cooperazione-di-polizia-dellUE-lotta-alle-forme-gravi-di-criminalita-e-alla-criminalita-organizzata-transfrontaliere_it*. Si veda, anche, *infra.*

[117] Si veda, ancora, la stesura della *Proposta di Regolamento del Parlamento e del Consiglio sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II")*, cit.

[118] Come anticipato, dall'adozione delle Decisioni Prüm nel 2008 (ovvero trattato multilaterale firmato nel 2005 da Belgio, Germania, Spagna, Francia, Lussemburgo, Paesi Bassi e Austria, poi evolutesi nella citata dec. 2008/615/GAI) si sono concretizzati sviluppi e cambiamenti considerevoli nel quadro giuridico dell'UE, nelle esigenze operative e negli sviluppi tecnico-forensi. Sono stati sviluppati vari sistemi e iniziative a livello dell'UE e internazionale con l'obiettivo di facilitare lo scambio di informazioni tra autorità di contrasto. Vi sono principalmente complementarità tra le decisioni "Prüm" e altre normative UE/internazionali pertinenti, compreso il quadro di interoperabilità. Esistono complementarità anche in relazione a taluni dei sistemi centrali di informazione dell'UE che hanno finalità diverse e, tuttavia, l'attuazione delle decisioni "Prüm" è stata lenta. Infatti, a quasi dieci anni dal termine di attuazione (26 agosto 2011) non tutti gli Stati membri avevano completato la procedura di valutazione e numerosi collegamenti bilaterali non erano stati stabiliti a causa della complessità tecnica e delle rilevanti risorse finanziarie e umane necessarie. Di conseguenza in alcuni Stati membri le interrogazioni non potevano essere confrontate con i dati se non era stata stabilita la relativa connessione bilaterale. Ciò ha ostacolato la capacità di identificare i potenziali criminali e di individuare i legami transfrontalieri tra i reati. Queste le spinte alla base della proposta normativa. Si veda, difatti, la *Proposta di Regolamento del Parlamento e del Consiglio sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II"), Scheda Finanziaria-legislativa*, punto 1.5.3, p. 53 e 54.

Cercando di sintetizzare i contenuti del possibile "Codice", occorre dire innanzitutto come essi non sembrano in realtà raggiungere quella completezza e sistematicità insita, per l'appunto, nelle promesse di un Codice.

Il Capo primo della proposta reca, come di consueto, disposizioni generali, indicando l'oggetto, la finalità e l'ambito di applicazione del Regolamento. Vengono poi regolati, nel Capo 2, lo scambio e la consultazione automatizzata, e le tipologie di "domande e risposte" relative alle categorie di dati previste dal Regolamento – ovverosia i profili DNA, i dati dattiloscopici, i dati di immatricolazione dei veicoli, le immagini del volto e gli estratti del casellario giudiziale – distintamente per ciascuna categoria di dati. Sono altresì contenute in questo capo le disposizioni comuni per l'istituzione di punti di contatto nazionali e l'adozione di misure di attuazione. L'architettura e il funzionamento della nuova struttura tecnica per lo scambio di dati sono disciplinati, poi, nel Capo 3: si prevedono così, un *router* centrale, e se ne disciplina l'uso ai fini del "lancio" delle varie interrogazioni; si disciplina poi ovviamente l'interoperabilità tra il *router* e l'archivio comune di dati di identità (per l'accesso da parte delle autorità di contrasto), e si prescrive pure, a fini di garanzia, che rimanga traccia di tutti i trattamenti dei dati effettuati. È pure disciplinato l'uso dell'Indice europeo dei casellari giudiziali (EPRIS) a fini di scambio e, anche in questi casi, è prevista la registrazione di tutte le operazioni di trattamento.

Il Capo 4 poi definisce le attività, nel caso sia emersa una "corrispondenza" (*hit*). Accanto a una disposizione relativa allo scambio automatizzato di dati di base, che lo limita a quanto necessario per l'identificazione del soggetto interessato, ve n'è un'altra sullo scambio più esteso di dati, che può essere effettuato in qualsiasi ulteriore fase e per finalità ulteriori rispetto alla mera identificazione. Il Capo successivo contiene sia disposizioni sull'accesso da parte degli Stati membri ai dati biometrici conservati da EUROPOL e provenienti da Paesi terzi, sia sull'accesso da parte di EUROPOL ai dati conservati nelle banche dati degli Stati membri. Il Capo 6, nel sottoporre i dati trattati per le finalità del Regolamento alle disposizioni della direttiva (UE) 2016/680 (LED), introduce pure espressamente i divieti di trasferimento e messa a disposizione di dati in maniera automatizzata, nei confronti di Paesi terzi od organizzazioni internazionali. Sono inoltre disciplinati la vigilanza e l'audit al fine di garantire l'adeguato rispetto delle regole descritte. Il Capo 7 individua le competenze degli Stati membri, di Europol e di eu-LISA nell'attuazione dei contenuti del Regolamento. Il capo 8 riguarda le modifiche delle citate Decisioni 2008/615/GAI e 2008/616/GAI e dei Regolamenti (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818[119]. Infine, il Capo 9 prevede alcune deroghe nella disciplina, alcuni obblighi ricognitivi e informativi (tra cui la predisposizione di relazioni e statistiche), l'effettuazione di notifiche oltre che disposizioni transitorie. Esso fissa altresì le prescrizioni per l'entrata in vigore[120], oltre a prevedere l'istituzione di un comitato e l'adozione di un manuale pratico per l'attuazione del Regolamento.

Dunque, si può probabilmente affermare come allo spostamento dalla "giustizia" alla "prevenzione" corrisponda anche lo spostamento dalla ricerca di una "legalità della giustizia penale" ad una ricerca di una "legalità della sicurezza". La ricerca sul piano della giustizia penale, paradossalmente, sembra aver trovato un suo equilibrio[121]: la frammentazione di sovranità, di poteri e di fonti ha, in qualche modo, forse, anche ampliato l'ambito della "legalità". Esso è passato da un più limitato concetto di certezza e prevedibilità della "legge" al più vasto concetto di certezza come prevedibilità del "diritto (anche) giurisprudenziale"[122].

La "legalità della sicurezza" cerca ancora un equilibrio. Diciamolo subito: qui il problema della certezza e della prevedibilità è di natura prevalentemente tecnica. Certo, abbiamo già visto come le stesse fonti eurounitarie abbiano cercato puntelli alla prevedibilità – intesa come trasparenza "procedurale" – piazzando organi e meccanismi di controllo, come quelli che han-

[119] In particolare, il Regolamento intende sostituire gli articoli da 2 a 6 e il capo 2, sezioni 2 e 3, della decisione 2008/615/GAI del Consiglio e i capi da 2 a 5 e gli articoli 18, 20 e 21 della decisione 2008/616/GAI del Consiglio, che sarebbero dunque soppressi dalla data di applicazione del nuovo strumento normativo.

[120] Entro il 2023 la proposta verrà trasmessa ai co-legislatori per l'adozione, il cui iter si stima sarà ultimato nel corso del 2024. Ove si dovesse mantenere questo termine, l'inizio del periodo di sviluppo è fissato all'esordio del 2025 (= T0), che vale da punto di riferimento per conteggiare le scadenze successive. Lo sviluppo del *router* e di EPRIS dovrebbe avvenire nel 2025 e nel 2026, con un inizio delle operazioni previsto nel 2027. Si veda, *Proposta di Regolamento del Parlamento e del Consiglio sullo scambio automatizzato di dati per la cooperazione di polizia ("Prüm II")*, cit., *Scheda finanziaria-legislativa*, punto 1.4.4, p. 51.

[121] Si veda Palombella (2006), pp. 5 ss.

[122] Si rinvia a Palazzo (2016) pp. 234 ss., il quale, tuttavia, alla p. 241, dà anche conto dei possibili "influssi antilegalitari del diritto europeo sull'ordinamento interno" in relazione ai delicati rapporti tra interpretazione conforme, disapplicazione e rinvii a Corte costituzionale e Corte di Giustizia.

no dato luogo, ad esempio, alle già riferite dinamiche (ai limiti del conflitto interistituzionale) tra EUROPOL ed EDPS[123]. Tale trasparenza "procedurale", tuttavia, non riesce affatto a garantire l'altra dimensione della trasparenza, quella tecnica, che attiene alla opacità strutturale di algoritmi e intelligenze artificiali[124].

Bibliografia

Adler-Nissen, Rebecca, Gammetoft Hannsen, Thomas (2008): *Sovereignity Games. Instrumentalizing State Sovereignity in Europe and Beyond* (New York, Palgrave).

Barcellona, Pietro (2007): "Crisi della sovranità statuale, territorialità della giurisdizione e processo di globalizzazione", in Rafaraci, Tommaso (editor), *L'area di libertà, sicurezza e giustizia*: *alla ricerca di priorità repressive ed esigenze di garanzia,* Atti del Convegno svoltosi a Catania, 9-11- giugno 2005 (Milano, Giuffrè), pp. 89 ss.

Belfiore, Rosanna (2021): "I procuratori "superdistrettuali" per i reati che ledono gli interessi finanziari dell'Unione europea: un nuovo terzo binario investigativo", *Sistema penale online.*

Bergström, Maria (2011): "EU Anti-Money Laundering Regulation: Multilevel Cooperation of Public and Private Actors", in Eckes, Christina e Konstadinides, Theodor (editors), *Crime Within the Area of Freedom, Security and Justice: A European Public Order* (Cambridge, CUP), pp. 97 ss.

Bergström, Maria (2018): "The many uses of Anti-Money Laundering Regulation", *German Law Journal*, pp. 418 ss.

Bernardi, Alessandro (2002): "Il diritto penale tra globalizzazione e multiculturalismo", *Rivista italiana di diritto pubblico comunitario*, pp. 485 ss.

Brière, Chloé (2021): *EU Criminal Procedural Law onto the Global Stage: the e-Evidence Proposals and Their Interaction with International Developments*, *European Papers*, pp. 493 ss.

Burrell, Jenna (2016): "How machines think: Understanding opacity in machine-learning algorithms", *Big Data and Society*, pp. 1 ss.

[123] Si veda, *supra*, paragrafo 8, spec. nota 105.

[124] Si veda Quattrocolo (2019), p. 274, che la discute nell'ambito del problema della parità delle armi rispetto alla pubblica accusa nel processo penale. Il tema dell'opacità dei sistemi di intelligenza artificiale e delle connesse esigenze di trasparenza è molto ampio e complesso, e ci è impossibile affrontarlo in questa sede. Ci limitiamo a ricordare che la Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM/2021/206 *final*, in corso di esame da parte delle Istituzioni UE se ne occupa, tra gli altri, all'art. 13 ("Trasparenza e fornitura di informazioni agli utenti"), il quale prevede che: "1. I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente. Sono garantiti un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi dell'utente e del fornitore di cui al capo 3 del presente titolo. 2. I sistemi di IA ad alto rischio sono accompagnati da istruzioni per l'uso in un formato digitale o non digitale appropriato, che comprendono informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per gli utenti. 3. Le informazioni di cui al paragrafo 2 specificano: a) l'identità e i dati di contatto del fornitore e, ove applicabile, del suo rappresentante autorizzato; b) le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui: i) la finalità prevista; ii) il livello di accuratezza, robustezza e cibersicurezza di cui all'articolo 15 rispetto al quale il sistema di IA ad alto rischio è stato sottoposto a prova e convalidato e che ci si può attendere, e qualsiasi circostanza nota e prevedibile che possa avere un impatto sul livello atteso di accuratezza, robustezza e cibersicurezza; iii) qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di IA ad alto rischio in conformità alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali; iv) le sue prestazioni per quanto riguarda le persone o i gruppi di persone sui quali il sistema è destinato a essere utilizzato; v) ove opportuno, le specifiche per i dati di input o qualsiasi altra informazione pertinente in termini di set di dati di addestramento, convalida e prova, tenendo conto della finalità prevista del sistema di IA; c) le eventuali modifiche apportate al sistema di IA ad alto rischio e alle sue prestazioni, che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità; d) le misure di sorveglianza umana di cui all'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA da parte degli utenti; e) la durata prevista del sistema di IA ad alto rischio e tutte le misure di manutenzione e cura necessarie per garantire il corretto funzionamento di tale sistema, anche per quanto riguarda gli aggiornamenti *software*". In letteratura si vedano, *ex multis*, da ultimo, Papadouli (2022), *passim*; Tschider (2021), pp. 126 ss.; Kiseleva (2021), *passim*. Si vedano, poi, Burrell (2016), pp. 1 ss.; Danaher (2016), pp. 29 ss.; Hildebrandt (2018), pp. 1 ss.

Cajani, Francesco e Costabile, Gerardo (editors) (2011): *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea* (Forlì, Experta).

Calavita, Oscar (2021): "La proposta di regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto", *www.lalegislazionepenale.eu.*

Cassese, Sabino (2012): "New Paths for Administrative Law: A Manifesto", *International Journal of Constitutional Law*, pp. 603 ss.

Cassibba, Fabio S. (2022): "Misure investigative del pubblico ministero europeo e principio di proporzionalità", *Sistema penale online.*

Castells, Manuel (2014): *La nascita della società in rete* (Milano, Egea)

Chamon, Merijn (2016): *EU Agencies: Legal and Political Limits to the Transformation of the EU* (Oxford, OUP).

Chiti, Edoardo e Mattarella, Bernardo G. (2008): "La sicurezza europea", *Rivista trimestrale di diritto pubblico*, pp. 305 ss.

Danaher, John (2016): "Algorithmic Decision-making and the Problem of Opacity", *Computers and Law*, 8, pp. 29 ss.

Daskal, Jennifer (2018): "Unpacking the CLOUD Act", *Eucrim*, 4, pp. 220 ss.

De Amicis, Gaetano (2022): "Gli organismi centralizzati della cooperazione amministrativa e di polizia", in Kostoris, Roberto, *Manuale di procedura penale europea* (Milano, Giuffrè), pp. 313 ss.

De Capitani, Emilio (2020): "Progress and Failure in the Area of Freedom, Security, and Justice", in Bignami, Francesca (editor), *EU Law in Populist Times: Crises and Prospects* (Cambridge, CUP), pp. 375 ss.

Di Stasi, Angela e Rossi, Lucia Serena (editors) (2020): *Lo spazio di libertà, sicurezza e giustizia* (Napoli, Editoriale scientifica).

Dominioni, Oreste (2005): *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione* (Milano, Giuffrè).

Ducato, Rossana (2016): "La crisi della definizione di dato personale nell'era del *web* 3.0", in Cortese, Fulvio e Tomasi, Marta (editors), *Le definizioni nel diritto* (Napoli, Editoriale Scientifica Italiana), p. 145.

Floridi, Luciano (2017): *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* (Milano, Raffaello Cortina).

Floridi, Luciano (2018): "AI4People. An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Reccomendations", *Minds and Machinews*, pp. 689 ss.

Forzati, Francesco (2019): "Illecito personologico fra destrutturazione del *tatstrafrecht* e affermazione del *Täter-Prinzip*. Soggettivizzazione del reato e crisi della materialità penale nel XIX e XX secolo", *Rivista italiana di diritto e procedura* penale, pp. 1989 ss.

Gialuz, Mitja (2019): "Quando la giustizia penale incontra l'intelligenza artificiale: luce e ombre dei *risk assessment tools* tra Stati Uniti ed Europa", *www.penale-contemporaneo.it*.

Gialuz, Mitja (2022): "La cooperazione orizzontale", in Kostoris, Roberto (editor), *Manuale di procedura penale europea* (Milano, Giuffrè), pp. 313 ss.

Gilmore, William C. (2004): "Dirty Money: The Evolution Of Money-Laundering Counter-Measures", *Council of Europe Press*, 3rd ed.

Goldewijk, Berma Klein (2008): "Why human? The interlinkages between security, rights and development", *Security and Human Rights,* pp. 24 ss.

Granieri, Giuseppe (2006): *La società digitale* (Roma/Bari, Laterza).

Henderson, Karen (2005): *The Area of Freedom, Security and Justice in the enlarged Europe* (London, Palgrave).

Hildebrandt, Milreille (2018): "Algorithmic Regulation and the Rule of Law", *Royal Society*, pp. 1 ss.

Kiseleva, Anastasiya (2021): "Making AI's Transparency Transparent: Notes On The EU Proposal For The AI", *European Law Blog*, 2021.

Kostoris, Roberto E. (2016): "Un diritto postmoderno", in Kostoris (editor), *Percorsi giuridici della postmodernità* (Bologna, Il Mulino), pp. 9 ss.

Lorusso, Sergio (2014): "'Superprocura' e coordinamento delle indagini in materia di criminalità organizzata, tra presente, passato e futuro", *Diritto penale contemporaneo – Rivista trimestrale*, pp. 33 ss.

Luchtman Michiel e J. Vervaele, John (2014): "European Agencies for Criminal Justice and Shared Enforcement (Eurojust and the European Public Prosecutor's Office)", *Utrecht Law Review*, p. 132.

Lupària, Luca (2012): "Trial by probabilities. Qualche annotazione 'eretica'" in Cucci, Monica, Gennari, Giuseppe, Gentilomo, Andrea (editors), L'uso della prova scientifica nel processo penale (Rimini, Maggioli Editore) pp. 96 ss.

Mitsilegas, Valsamis e Mouzakiti, Foivi (2020): "Data-driven Operational Co-operation in Europe's Area of Criminal Justice", in Billet, Carole, Turmo Araceli (editors), *Coopération opérationnelle en droit pénal de l'Union européenne* (Bruxelles, Brulyant), p. 129.

Mitsilegas, Valsamis, Monar Jörg, Rees, Wyn (2003): *The European Union and Internal Security. Guardian of the People?* (New York, Palgrave).

Nunzi, Alfredo (2007): "Exchange of information and intelligence among law enforcement authorities a European Union perspective", *Revue international de droit pénal*, pp. 145 ss.

Pagallo, Ugo e Quattrocolo, Serena (2018): "The Impact of AI on criminal law, and its twofold aspects", in Barfield, Woodrow e Pagallo, Ugo (editors), *Research Handbook on the Law of Artificial Intelligence* (Cheltenam, Elgar) pp. 391 ss.

Palazzo, Francesco (2017): "Principio di legalità e giustizia penale", Kostoris (editor), *Percorsi giuridici della postmodernità* (Bologna, Il Mulino), pp. 234 ss.

Palombella, Gianluigi (2006): *Dopo la certezza. il diritto in equilibrio tra giustizia e democrazia* (Bari, Dedalo).

Papadouli, Vasiliski (2022): "Transparency in Artificial Intelligence: A Legal Perspective", *Journal of Ethics and Legal Technologies*, pp. 25 ss.

Procaccino, Angela (2022a): "Il secondo Protocollo e le indagini della Procura europea", *Diritto penale e processo*, pp. 1168 ss.

Procaccino, Angela (2022b): "*Sliding doors*: la competenza della Procura europea e la prevenzione delle duplicazioni procedimentali", *Studi sull'integrazione europea*, pp. 509 ss.

Quattrocolo, Serena (2018): "Intelligenza artificiale e giustizia: nella cornice della Carta etica europea gli spunti per un'urgente discussione tra scienza penali e informatiche", *www.lalegislazionepenale.eu*.

Quattrocolo, Serena (2020): "Equo processo penale e sfide della società algoritmica", in D'Aloia, Antonio (editor), *Intelligenza artificiale e diritto* (Milano, Franco Angeli), pp. 267 ss.

Quintel, Teresa (2022): "Data protection rules applicable to Financial Intelligence Units: still no clarity in sight", *ERA Forum*, 23, pp. 54 ss.

Rota, Chiara (2020): "Un nuovo tassello nella difesa dello spazio comune di libera circolazione", *Rivista di Polizia*, 2, pp. 131 ss.

Sgubbi, Filippo (2019): *Diritto penale totale* (Bologna, Il Mulino).

Sicurella, Rosaria e Scalia, Valeria (2013): "Data Mining and Profiling in the Area of Freedom, Security and Justice: State of Play and New Challenges in the Balance between Security and Fundamental Rights Protection", *New Journal of European Criminal Law*, pp. 409 ss.

Signorato, Silvia (2018): *Le indagini digitali*, (Torino, Giappichelli).

Slobogin, Christopher (2018): "Preventive Justice: A Paradigm in Need of Testing", *Behavioral Sciences and the Law*, 4, pp. 1 ss.

Tavassi, Ludovica (2022): "Il primo anno di EPPO: appunti per una revisione critica", *Sistema penale*, 5, pp. 53 ss.

Tschider, Charlotte A. (2021): "Legal Opacity: Artificial Intelligence's Sticky Wicket", *Iowa Law Review Online*, pp. 126 ss.

Turmo, Araceli (2021): "Criminal procedure out of itself. A case Study of the Relationship between EU Law and Criminal Procedure Using the ETIAS System", *European Papers*, 2021, pp. 473 ss.

Venegoni, Andrea (2022): "L'EPPO nel panorama della cooperazione giudiziaria europea", *Cassazione penale,* pp. 2798 ss.

Vitiello, Daniela (2022): *Le frontiere esterne dell'Unione europea* (Bari, Cacucci).

Wood, Mattew (2018): "Mapping EU Agencies as Political Entrepreneurs", *European Journal of Political Research*, pp. 404 ss.

Zingales, Diana (2021): "Risk assessment: una nuova sfida per la giustizia penale", *www.dirittopenaleuomo.org.*

Il focus su...
Focus sobre...
Focus On...

Il rinvio pregiudiziale in ambito penale e i problemi posti dalle sentenze interpretative della Corte di Giustizia*

La remisión prejudicial en materia penal y los problemas que generan las sentencias interpretativas del Tribunal de Justicia

The Preliminary Reference in Criminal Matters and the Issues Raised by Interpretative Judgments of the Court of Justice

Alessandro Bernardi
Professore Ordinario di Diritto Penale nell'Università di Ferrara
alessandro.bernardi@unife.it

Diritto UE,
Interpretazione della legge

Derecho UE,
Interpretación de la ley

EU Law,
Legal Interpretation

Abstracts

Il lavoro sottolinea innanzitutto perché il rinvio pregiudiziale d'interpretazione sia uno strumento prezioso e vieppiù utilizzato anche in ambito penale, per poi prendere in esame le sentenze interpretative della Corte di giustizia dotate di effetti penali particolarmente problematici. Al riguardo, vengono considerate tre fondamentali tipologie di sentenze interpretative: a) quelle sibilline, o vaghe, o contraddittorie, comunque destinate a suscitare dubbi in merito alle loro ricadute sia nella causa nell'ambito della quale si è innestato il rinvio pregiudiziale, sia più in generale sugli ordinamenti penali nazionali; b) le sentenze interpretative con effetti *in malam partem* sulla norma penale interna, osteggiate dai settori della dottrina più nazionalisti e garantisti; c) le sentenze interpretative che chiedono al giudice del rinvio di prendere provvedimenti in tendenziale conflitto coi supremi principi e/o coi diritti fondamentali previsti dalle Carte nazionali, e che pertanto sono votate a innescare un "dialogo" tra Corte di giustizia e Corti costituzionali che a volte assume le sembianze di un vero "duello".

En primer lugar, el artículo analiza las razones por las cuales la remisión prejudicial de interpretación es una herramienta valiosa y cada vez más utilizada en el ámbito penal. En segundo lugar, el trabajo examina diversas sentencias interpretativas del Tribunal de Justicia con efectos penales especialmente problemáticos. A este respecto, se consideran tres tipos fundamentales de sentencias interpretativas: a) las que son sibilinas, o vagas, o contradictorias, en todo caso destinadas a suscitar dudas respecto de sus repercusiones, y ello tanto en el caso concreto en que se ha planteado la cuestión prejudicial como a nivel general del ordenamiento jurídico; b) las sentencias interpretativas con efectos in malam partem sobre el Derecho penal nacional, a las que se oponen los sectores más nacionalistas y garantistas de la doctrina; c) las sentencias interpretativas que piden al órgano jurisdiccional remitente que adopte medidas que pueden entrar en conflicto con los principios supremos y/o los derechos fundamentales de las personas establecidos en la Constitución, y que terminan, por tanto, desencadenando un "diálogo" entre el Tribunal de Justicia y los Tribunales Constitucionales, intercambio que, a veces, adquiere la apariencia de un auténtico "duelo".

The work first emphasises why the preliminary reference for interpretation is a valuable and increasingly used tool also in the criminal law sector; second, it examines interpretative judgments of the Court of Justice with problematic effects in the criminal field. In this regard, three fundamental types of interpretative judgments are considered: (a) those that are vague or contradictory, or give rise to doubts as to their effects both in the single case and, more generally, on national criminal law systems; (b) the interpretative judgments with in malam partem effects on the domestic legal system law, that are frequently criticized by the traditional criminal law literature; (c) the interpretative judgments that ask the referring court to take measures possibly in conflict with the supreme principles and/or fundamental rights laid down in the national charters, and which are therefore capable of triggering a 'dialogue' - if not an actual 'duel' - between the Court of Justice and the constitutional courts .

*Testo, aggiornato e integrato di note, della relazione svolta nell'ambito del convegno "Il rinvio pregiudiziale come strumento di sviluppo degli ordinamenti" (Università di Ferrara, 13-14 ottobre 2022).

Sommario

1. Nota introduttiva.

L'argomento affidatomi – il rinvio pregiudiziale "in materia penale"[1] e le relative sentenze interpretative della Corte di giustizia – è per me sempre stato assai ostico; e tale è rimasto, nonostante il non poco tempo ad esso dedicato. Negli anni in cui coordinavo il dottorato di ricerca nel cui ambito si inscrive l'attuale convegno, proprio per la collana del dottorato ho curato tre raccolte di atti congressuali – una del 2015 sull'interpretazione conforme al diritto UE[2], una del 2017 sui controlimiti[3] e una sempre del 2017 sul caso Taricco[4]. Orbene, tutte e tre queste raccolte hanno chiaramente a che fare col grande tema del rinvio pregiudiziale in ambito penale e del relativo dialogo tra giudici nazionali e giudici europei: tema che i molteplici scritti rinvenibili in quelle raccolte – pur spesso assai approfonditi e articolati – non sono certo riusciti a esaurire, non foss'altro che per i continui colpi di scena cui ormai tale dialogo ci ha abituato.

Nello spazio di tempo concessomi per questa relazione dovrò dunque necessariamente limitarmi ad affrontare solo taluni profili del tema in oggetto, sorvolando su molti altri nient'affatto marginali e in particolare glissando sul versante processuale del rinvio pregiudiziale, che del resto so già essere stati trattati. Mi limiterò dunque a pochi aspetti e pochi esempi del succitato dialogo tratti da una casistica ormai vastissima. Esempi, a onor del vero, relativi a questioni particolarmente controverse e proprio per questo atte a rendere assai difficile il confronto tra giudici nazionali e giudici europei e a disvelare una realtà inquietante: che cioè – al di là della indubbia utilità del rinvio pregiudiziale, in ambito penale come in qualsiasi altro ambito – a volte manca ogni certezza in merito ai risultati di questo confronto; che le risposte offerte dalla Corte di giustizia nelle sue sentenze interpretative possono non essere risolutive; che gli equilibri raggiunti possono essere sofferti e precari.

Sottolineare questa realtà non significa negare che la risposta della Corte di giustizia alla richiesta di interpretazione di una data norma UE risulti il più delle volte preziosa e non problematica, così da consentire al giudice interno di sciogliere i suoi dubbi circa la conformità o meno del primo al secondo, ovvero circa il modo più corretto di interpretare la norma nazionale per porla in sintonia con il sistema giuridico dell'Unione. Significa solo prendere coscienza del fatto che in altri casi non è così e che il ponte tra diritto nazionale e diritto UE costruito dai giudici si rivela talora fragile.

Per prepararmi a questo incontro sono andato a rileggere una serie di risalenti lavori sul caso Taricco. Uno di questi, scritto da me, si chiudeva ricordando che i rapporti tra ordinamenti nazionali e ordinamento europeo assomigliano a tutto meno che a una partita di scacchi, essendo privi di regole esatte; che dunque il dialogo tra i relativi giudici dà luogo a

[1] Materia, questa, che come noto si estende ben al di là del diritto *stricto sensu* penale, in quanto capace di abbracciare tutti gli ambiti punitivi "sostanzialmente penali": cfr. per tutti, Donini, Foffani (eds.) (2018).
[2] Bernardi (editor) (2015).
[3] Bernardi (editor) (2017a).
[4] Bernardi (editor) (2017b).

'partite' ricche di componenti emotive e dagli esiti a volte imprevedibili[5]. Questa conclusione cui pervenivo cinque anni fa mi sento di ribadirla ancora adesso, dato che nell'ultimo lustro molte sentenze della Corte di giustizia innescate da un rinvio pregiudiziale hanno suscitato e continuano a suscitare polemiche di ogni tipo, confermando che le tensioni di cui il rinvio pregiudiziale è espressione solo in alcuni casi vengono risolte grazie a questo strumento e alle relative sentenze interpretative della Corte di giustizia. In altri casi, infatti, queste sentenze si limitano a sopire momentaneamente i contrasti, mentre in altri casi ancora finiscono con l'amplificarli, col comportare l'entrata in campo delle Corti costituzionali, il cui dialogo con la Corte di giustizia può anche tramutarsi in qualcosa di molto simile a un duello.

2. Tre precisazioni.

A questo punto, dopo aver anticipato e un po' semplicizzato le mie conclusioni, desidero fare tre precisazioni:

a) sempre in ragione dei limiti di ampiezza connaturati a ogni relazione congressuale, tratterò solo del rinvio pregiudiziale d'interpretazione del diritto europeo, tralasciando il rinvio pregiudiziale di validità degli atti compiuti dagli organi dell'Unione, che presenta proprie peculiarità[6];

b) in materia penale il rinvio pregiudiziale diventa particolarmente delicato per la vistosa interrelazione tra questa materia e i principi/diritti fondamentali, i quali si sono progressivamente affermati anche nel diritto UE. Tuttavia, come si sa, in questa sede essi possono finire con l'assumere contenuti almeno parzialmente diversi da quelli propri dei paralleli principi/diritti rinvenibili nelle Costituzioni dei singoli Paesi membri, così da creare conflitti al più alto livello dei relativi ordinamenti (avrò modo di portare alcuni esempi in proposito). Riguardo ai principi/diritti fondamentali UE, ricordo che nella prima fase della costruzione europea essi si limitavano a quei pochi che si rinvenivano nel Trattato CEE[7]. A questi si sono poi aggiunti i principi/diritti fondamentali c.d. "impliciti" o "di diritto non scritto", in quanto non rintracciabili all'interno delle fonti giuridiche varate a Bruxelles, ma ricavati dalla Corte di giustizia a partire dalle tradizioni costituzionali comuni e dalle convenzioni ratificate da tutti i Paesi membri[8]. A completare l'attuale panorama dei principi/diritti fondamentali UE ha poi provveduto la Carta dei diritti fondamentali dell'Unione europea (CDFUE), i cui principi/diritti hanno ora inglobato ora affiancato i primi due insiemi di principi/diritti.

c) Sebbene abbia appena affermato che i casi di cui intendo parlare concernono sentenze interpretative della Corte di giustizia che, per varie ragioni, non hanno risolto soddisfacentemente le tensioni da cui originavano i relativi rinvii pregiudiziali, voglio qui ribadire l'assoluta indispensabilità del rinvio pregiudiziale in ambito penale. Al riguardo, basti pensare che – nonostante il testo della Costituzione consti di soli 139 articoli – è già difficile per il giudice comune fornire, rispetto a una data norma penale, la sua interpretazione conforme a Costituzione, ovvero sancire la eventuale incostituzionalità della norma in oggetto: tant'è che quest'ultima delicatissima decisione è riservata alla Corte costituzionale. È agevole allora immaginare quanto possa essere problematico per il giudice comune fornire l'interpretazione conforme al diritto UE di una data norma penale ovvero stabilire la sua eventuale incompatibilità con il diritto UE, considerato che tutte le norme UE di diritto primario e derivato, essendo in posizione di primato rispetto alla norma penale interna, possono assurgere al ruolo di norme-parametro alla cui luce effettuare l'interpretazione conforme della suddetta norma penale, ovvero fondare la disapplicazione di quest'ultima[9] (o, in alternativa, sollevare questione di costituzionalità per contrasto con gli artt. 11 e 117 della nostra Costituzione)[10] nel caso in cui il testo della norma in questione renda impossibile adeguarla in via interpretativa al diritto

[5] Bernardi (2017c), p. 84-85.

[6] Basti pensare che "la Corte [di giustizia] detiene una competenza esclusiva a fornire l'interpretazione *definitiva* di detto diritto [UE], il che significa che i giudici non di ultima istanza non sono tenuti ad effettuare il rinvio alla Corte di giustizia. Viceversa, per quanto riguarda l'accertamento dell'invalidità, la Corte, ha chiarito sin dalla sentenza *Fotofrost* che tutti i giudici – e non solo quelli di ultima istanza – sono tenuti ad effettuare un rinvio pregiudiziale quando ritengano che le disposizioni di un atto dell'Unione applicabili al caso in esame presentino profili di invalidità": Rossi (2022), p. 52.

[7] Penso innanzitutto ai diritti di voto, eleggibilità, libera circolazione e stabilimento di cui agli artt. 18, 19, 43, 48 e 52 ss. Tr. CEE.

[8] Con specifico riferimento alla materia penale cfr., anche per ulteriori riferimenti bibliografici, Bernardi (1988), p. 156 ss.

[9] Nel caso in cui essa contrasti con norme UE direttamente applicabili.

[10] Nel caso in cui essa contrasti con norme UE non direttamente applicabili.

UE. In sede di valutazione della conformità o meno della norma penale interna al diritto UE, insomma, il numero delle potenziali norme-parametro può essere pressocché sterminato, così da rendere non di rado assai difficile già appurare il dato prodromico a tale valutazione: se cioè la suddetta norma penale sia o no da ritenersi "attuativa del diritto UE"[11]. Per non parlare poi della difficoltà che il giudice interno può incontrare in sede di interpretazione di norme "esterne" all'ordinamento giuridico del proprio Paese; norme la quali, peraltro, postulano uno sviluppo omogeneo in seno all'Unione, dunque uno sviluppo improntato a metodi interpretativi uniformi[12].

Proprio alla luce della difficoltà incontrate dal giudice interno in sede di valutazione dell'incidenza del diritto UE sulla norma interna, del resto, la Corte di giustizia si dimostra molto generosa nell'accogliere i rinvii pregiudiziali anche nei casi in cui la questione sollevata sia formulata in modo impreciso[13], se del caso riconfigurandola e risolvendola alla luce di norme-parametro UE diverse da quelle considerate dal giudice del rinvio.

3. Le ragioni del progressivo incremento dei rinvii pregiudiziali in materia penale.

Il lavoro di catalogazione di tutti i rinvii pregiudiziali italiani dall'entrata in vigore del trattato di Lisbona a tutto il 2021, svolto dagli attuali iscritti al Dottorato "Diritto dell'Unione europea e ordinamenti nazionali" dell'Università di Ferrara, ha confermato un dato già noto: il numero di rinvii pregiudiziali in materia penale è senz'altro inferiore a quello riscontrato in altre materie, quali innanzitutto il diritto amministrativo e il diritto civile. Anche se occorre considerare che un ricorso concernente questioni a carattere non direttamente penale può avere ricadute significative anche in questo ambito.

In ogni caso, col passare dei decenni è avvertibile un incremento nella frequenza dei rinvii pregiudiziali in materia penale, concernenti il più delle volte specifici ambiti, quali il doppio binario sanzionatorio (penale e amministrativo) e il principio *ne bis in idem*; la natura della confisca; la tutela della vittima nel processo penale; le misure afflittive prese nei confronti dei migranti; le immunità parlamentari.

Tale incremento sembrerebbe ascrivibile a diversi motivi, tre dei quali meritano qui di essere messi in vetrina:

Il primo motivo, a carattere legislativo, risiede nella vertiginosa moltiplicazione delle norme UE dotate di possibili ricadute in ambito penale.

Al riguardo, va ricordato innanzitutto che a partire dal Trattato di Maastricht del 1992 l'UE ha acquisito una competenza penale indiretta. Questa competenza era rinvenibile dapprima nel c.d. terzo pilastro UE previsto da tale Trattato, concernente la "*Cooperazione nei settori della giustizia e degli affari interni*" (GAI) in vista della costruzione di uno "*Spazio europeo di libertà, sicurezza e giustizia*" atto a contrastare la criminalità a livello sovranazionale. All'interno di tale pilastro il Titolo VI TUE in tema di "*Disposizioni sulla cooperazione di polizia e giudiziaria in materia penale*" prevedeva che fossero varate fonti normative di armonizzazione penale improntate al metodo intergovernativo, denominate prima convenzioni e azioni comuni, poi decisioni-quadro. Successivamente, col Trattato di Lisbona del 2007-2009, è venuta meno la struttura a pilastri dell'Unione europea, cosicché quest'ultima ha semplificato la sua configurazione. Nel TFUE anche la competenza penale si è dunque informata al c.d. metodo comunitario, radicandosi nel titolo V TFUE, (concernente lo "Spazio di libertà, sicurezza e giustizia") capo IV (relativo alla "Cooperazione giudiziaria in materia penale", artt. 82-86) e trovando attuazione attraverso le direttive d'armonizzazione penale[14]. Come si sa, a seguito del riconoscimento in capo all'Unione europea di questa competenza penale indiretta è stato varato un gran numero di direttive ricche di ricadute sulle norme penali nazionali.

Va peraltro sottolineato che anche moltissime delle norme di diritto derivato UE a carat-

[11] Difficoltà, questa, per altro verso ulteriormente incrementata dalle incertezze relative a quali siano i presupposti sulla cui base considerare una norma penale nazionali "attuativa" o "non attuativa" del diritto UE. In merito all'evoluzione che ha caratterizzato il concetto di "norma attuativa del diritto UE" cfr., *infra, sub* par. 3, lett. *b)*.

[12] In merito ai quali cfr., fondamentalmente, Lenaerts, Gutierrez-Fons (2020).

[13] Cfr. Iannone (2019), par. II.

[14] Va peraltro ricordato che la prima direttiva penale è stata varata nel 2008, dunque un anno prima dell'entrata in vigore del Trattato di Lisbona.

tere non penale varate a ritmo incessante nel corso degli anni possono incidere sulle norme di diritto penale interno, condizionando l'interpretazione di queste ultime, ovvero determinando la loro disapplicazione, o la loro incostituzionalità, totale o parziale nei casi in cui esse si rivelino in tutto o in parte in insanabile contrasto col diritto UE.

È dunque di tutta evidenza che questa moltiplicazione delle norme UE atte a condizionare l'interpretazione conforme o la disapplicazione/incostituzionalità di norme penali interne abbia come conseguenza una parallela moltiplicazione dei rinvii pregiudiziali[15] finalizzati ad ottenere dalla Corte di giustizia l'esatta interpretazione delle norme parametro-UE.

Il secondo motivo, di natura giurisprudenziale, risiede nella dilatazione del concetto di "norma attuativa del diritto UE", con conseguente ulteriore moltiplicazione delle norme interne considerate da questa Corte "attuative del diritto UE" e in quanto tali scrutinabili alla luce di tale diritto. Da un lato, infatti, la Corte di giustizia ricorda che il diritto UE, ivi compresa la CDFUE, incide sull'ordinamento giuridico degli Stati membri "esclusivamente nell'attuazione del diritto dell'Unione"[16]. Dall'altro lato, però, in base alla giurisprudenza evolutiva della Corte di giustizia, sono ormai da considerarsi attuative del diritto UE anche le norme interne a qualunque titolo "interferenti col diritto UE"[17]. Certo, questa giurisprudenza a carattere estensivo non riguarda solo le norme interne di natura penale, ma tutte le norme interne di qualsiasi tipo; resta però il fatto che tale effetto estensivo si manifesta con grande evidenza in ambito penale, dato che sono davvero innumerevoli le norme penali che possono appunto risultare, a vario titolo, "interferenti col diritto UE".

Il terzo motivo, di natura sia legislativa sia giurisprudenziale, consiste nella progressiva emersione e valorizzazione dei principi/diritti UE (come già accennato[18], contenuti volta a volta nei Trattati, ovvero ricavati dalla giurisprudenza della Corte di giustizia, ovvero ancora previsti dalla CDFUE) destinati a entrare in relazione con le norme penali nazionali.

Questi principi/diritti, oltretutto, sono sempre più spesso considerati dotati di effetto diretto dalla Corte di giustizia, cosicché – per quanto riguarda l'Italia – altrettanto spesso i giudici comuni non sarebbero tenuti a interpellare in prima battuta la Corte costituzionale[19]. Ad esempio, come ricordato dall'Avvocato generale Michal Bobek nelle sue *Conclusioni* presentate il 23 settembre 2021 nell'ambito della causa C-205/20, *NE*, "il diritto a una tutela giurisdizionale effettiva, il principio di non discriminazione fondata sulla religione o sulle convinzioni personali, il principio di ne bis in idem o il diritto a ferie retribuite, sono stati recentemente dichiarati direttamente efficaci"[20]. Inoltre, nella recente sentenza della Grande camera relativa alla medesima causa[21] è stato dichiarato direttamente efficace anche il principio di proporzionalità della sanzione sancito dall'art. 49.3 CDFUE, ma rinvenibile anche in numerosissimi testi normativi UE che obbligano gli Stati a prevedere, in caso di violazione delle norme in essi contenute, sanzioni non solo "efficaci" e "dissuasive" ma anche, per l'appunto, "proporzionate" e dunque non più severe dello stretto necessario[22]. Cosicché il giudice comune, per rendere tali sanzioni rispettose del principio di proporzionalità UE, sembrerebbe potere e dovere conformare in via interpretativa la sanzione applicabile all'interno del compasso edittale previsto dalla norma penale nazionale, di fatto escludendo il ricorso a sanzioni collocate nei pressi del massimo edittale, se appunto sproporzionate rispetto all'illecito commesso; ovvero sembrerebbe addirittura potere e dovere effettuare l'eventuale disapplicazione del minimo edittale, così da irrogare una sanzione anche al di sotto di quest'ultimo; ovvero ancora sembrerebbe poter decidere la disapplicazione della norma penale interna che preveda una misura punitiva per sua stessa natura (per esempio una misura detentiva anziché pecuniaria, oppure una misura penale anziché amministrativa) intrinsecamente sproporzionata, senza necessariamente

[15] Effettuati essenzialmente dai giudici comuni, ma ormai sempre più di frequente anche dalle Corti costituzionali. Al riguardo cfr. già Passaglia (editor) (2010). Cfr. altresì, per tutti, Mengozzi (2015), p. 707 ss.

[16] Con specifico riferimento alla CDFUE cfr., testualmente, Corte di giustizia (2019), punto 10.

[17] In merito al processo di progressiva dilatazione del concetto di "attuazione del diritto dell'Unione" di cui all'art. 51.1 CDFUE – processo che ha portato a considerare espressiva di tale "attuazione" ogni normativa nazionale volta anche semplicemente a incidere su ambiti regolati dalle suddette fonti UE – cfr., anche per i relativi riferimenti giurisprudenziali e dottrinali, Bernardi (2016), p. 59 ss.

[18] Cfr. *supra, sub* par. 2.

[19] Cfr., ad esempio, Ruggeri (2022). In argomento cfr. altresì, per tutti e con varietà di accenti, Barbareschi (2022); Parodi (2022), p. 128 ss.; Ruggeri (2021), p. 211 ss.

[20] *Ivi,* punto 48, con puntuali riferimenti alle sentenze della Corte di giustizia che hanno riconosciuto l'efficacia diretta dei suddetti principi.

[21] Sent. Corte di giustizia, Grande Sezione, 8 marzo 2022, Causa C-205/20, *NE.*

[22] In merito all'art. 49.3 CDFUE cfr., per tutti, Gambardella (2021), p. 26 ss.; Sotis (2012), con ulteriori riferimenti bibliografici; *amplius* N. Recchia (2020), *passim*; nonché, da ultimo, Bobek (2021), punto 37.

rimettere il caso alla Corte costituzionale[23].

4. Rinvio pregiudiziale e sentenze interpretative problematiche.

Già si è accennato al fatto che il rinvio pregiudiziale debba ritenersi uno strumento indispensabile e prezioso[24], tanto più prezioso quanto più, con la vertiginosa moltiplicazione delle fonti UE, risulti per i giudici nazionali vieppiù difficile valutare il loro impatto sul diritto interno. Resta il fatto che il rinvio pregiudiziale a volte non innesca, quantomeno nell'immediato, un percorso capace di risolvere i problemi che gravano sulle spalle del giudice nazionale, così da consentire l'adeguamento per via interpretativa della norma penale (o penal-amministrativa) interna al diritto UE, ovvero da permettere la disapplicazione di tale norma, ovvero ancora da porre la Corte costituzionale in condizione di sancirne l'incostituzionalità[25]. Ciò accade, in estrema sintesi, in relazione a tre diverse ipotesi di risposta della Corte di giustizia. La prima ipotesi si verifica quando la Corte di giustizia offre al giudice *a quo* una risposta che non risulta chiarificatrice, ma che al contrario si rivela, sibillina, vaga o contraddittoria (par. 4.1). La seconda ipotesi si registra quando la Corte di giustizia dà un responso che conferisce alla norma UE interpretata un significato produttivo di effetti sfavorevoli: vale a dire un significato tale da suggerire al giudice interno di interpretare estensivamente un elemento costitutivo della norma penale per conformarlo alle esigenze del diritto UE; ovvero un significato tale da suggerire a questo giudice di disapplicare norme di favore restrittive della punibilità, con conseguente dilatazione, anche in questo caso, dell'ambito applicativo della fattispecie penale (par. 4.2 s.). La terza ipotesi si riscontra quando la risposta della Corte di giustizia postula in capo al giudice interno "obblighi di conformazione" del diritto punitivo interno al diritto UE che risultano in contrasto più o meno evidente coi supremi principi e/o coi diritti fondamentali iscritti nelle Costituzioni nazionali (par. 4.3 ss.).

4.1. *Sentenze interpretative sibilline, vaghe, contraddittorie.*

Veniamo dunque alla prima ipotesi, concernente i casi in cui la Corte di giustizia dà risposte *sibilline, vaghe* o *contraddittorie*. Al riguardo, va ricordato che la tale Corte non deve né fornire l'interpretazione comunitariamente conforme della norma nazionale, né valutare essa stessa la sussistenza o meno di un contrasto tra tale norma e il diritto UE[26] (anche se spesso fa capire benissimo il suo punto di vista al riguardo)[27]. Deve solo limitarsi a fornire chiarificazioni in merito all'esatto significato delle fonti UE in rapporto di sospetta tensione con la norma nazionale *sub iudice*, in modo da facilitare la decisione del giudice interno circa la sussistenza o meno di tale stato di tensione e, se del caso, circa il possibile superamento di quest'ultimo per via interpretativa.

Ancora, va ricordato che nelle sue sentenze la Corte di giustizia si sforza di regola di essere comprensibile a operatori del diritto appartenenti a culture giuridiche e a ceppi linguistici alquanto differenti, e a tal fine evita processi argomentativi particolarmente elaborati privilegiando testi assertivi scarni ed essenziali, privi di orpelli eccessivamente dogmatici e delle forme di dialettica interna propria delle sentenze che accolgono le *dissenting opinions*[28].

Malgrado ciò, i fraintendimenti sono sempre dietro l'angolo, stante la difficoltà per la Corte di giustizia di sintonizzarsi con le diverse forme di sensibilità giuridica proprie dei Paesi

[23] Cfr., ancora, A. Ruggeri (2022).
[24] Cfr. *supra, sub* par. 2, *in fine*.
[25] Come noto, il rifiuto della Corte costituzionale di considerarsi "giudice nazionale" legittimato a effettuare il rinvio pregiudiziale alla Corte di Giustizia è venuto meno con l'ordinanza n. 103 del 2008 per quanto riguarda i giudizi di costituzionalità in via principale, e con l'ordinanza n. 207 del 2013 per quanto riguarda i giudizi di costituzionalità in via incidentale.
[26] L'incompetenza della Corte di giustizia a pronunciarsi sulla compatibilità della normativa nazionale con quella UE è infatti pacifica.
[27] In effetti, la Corte di giustizia ha presto dimostrato di voler frequentemente fornire al giudice *a quo* risposte così articolate da evidenziare il proprio convincimento in merito alla questione che tale giudice è chiamato a risolvere, e pertanto da limitare grandemente il potere discrezionale di quest'ultimo. Ad esempio, cfr. già Corte di giustizia, sent. 29 giugno 1978, causa 154/77, *Deckman*; sent. 12 ottobre 1978, causa 13/78, *Eggers*.
[28] Ricorda che la questione dell'introduzione delle opinioni dissenzienti nelle sentenze della Corte di giustizia fu da quest'ultima rigettata innanzitutto per "la necessità di garantire l'uniforme applicazione del diritto comunitario da parte degli stati membri e dei giudici nazionali" Vespaziani (2017),

membri[29]. In ogni caso, va tenuto presente che a volte i giudici di Lussemburgo non riescono ad offrire al giudice nazionale una chiara interpretazione della normativa europea pertinente al caso in esame, così da consentirgli di effettuare con sufficiente consapevolezza la suddetta valutazione[30].

a) Esempi più o meno risalenti di sentenze interpretative della Corte di giustizia *sibilline* o comunque tali da risultare di difficile comprensione per il giudice interno si rinvengono, ad esempio, nel campo del diritto penale agro-alimentare. Emblematiche, al riguardo, le sentenze relative ai casi *Tasca*[31], *Smanor*[32] e *Pontini*[33] nelle quali il giudizio sulla legittimità o meno della normativa sanzionatoria interna rispetto al diritto UE è stato fatto dipendere dalla sussistenza di elementi fattuali di assai difficile valutazione, ovvero è stato incentrato su criteri oltremodo elastici, se non addirittura inafferrabili; con il risultato di lasciare il giudice nazionale in una condizione di persistente dubbio sul da farsi. Ma la dottrina non ha mancato di segnalare anche ulteriori e più recenti sentenze interpretative della Corte di giustizia caratterizzate da un forte coefficiente di ambiguità[34] sulle quali è qui impossibile soffermarsi adeguatamente.

b) Quanto poi alle sentenze interpretative *vaghe*, esse si riscontrano soprattutto quando l'attività chiarificatrice della Corte di giustizia ha ad oggetto norme connotate da un intrinseco livello di elasticità che tale Corte non sempre riesce/vuole/può ridurre significativamente per via ermeneutica[35]. Un esempio in tal senso ci è offerto dalla sentenza del 2 marzo 2021, causa C-746/18, *H.K.*, concernente l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58/CE *relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche*; concernente, cioè, l'interpretazione di una norma in base alla quale gli Stati membri possano limitare i diritti dei cittadini qualora tale limitazione costituisca, all'interno di una società democratica, una misura necessaria, opportuna e proporzionata per la salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica, e per la prevenzione, ricerca, accertamento e perseguimento dei reati ovvero dell'uso non autorizzato del sistema di comunicazione elettronica[36]. A seguito di un rinvio pregiudiziale della Corte Suprema dell'Estonia effettuato al fine di sapere sino a che punto possano giustificarsi, rispetto al diritto UE, limitazioni di fonte interna ai citati diritti in vista della "prevenzione, ricerca, accertamento e perseguimento dei reati"[37] , la Corte di giustizia afferma che la norma in questione, letta "alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della

[29] Cfr., al riguardo, gli interessanti spunti di Schönberger (2015), p. 508 ss.

[30] In merito al problema della certezza sollevato da talune sentenze interpretative della Corte di giustizia in ambito penale cfr. già Grasso (1989), p. 276 ss., e bibliografia ivi riportata.

[31] Sent. 26 febbraio 1976, causa 65/75, *Tasca.* In questa sentenza la Corte di giustizia evidenzia appunto l'incompatibilità col diritto CEE della normativa sanzionatoria italiana in tema di zuccheri "*qualora [detta normativa] metta in pericolo gli obiettivi ed il funzionamento di tale organizzazione* [vale a dire della "*organizzazione comune dei mercati nel settore dello zucchero"], ed in ispecie del suo regime di prezzi*" (corsivo non testuale). La legittimità della normativa in questione viene dunque fatta dipendere da valutazioni macroeconomiche che tendono a esulare dalla competenza del giudice del rinvio.

[32] Sent. 14 luglio 1988, causa 298/87, *Smanor*, punto 25: "La prima parte della questione pregiudiziale sollevata dal tribunal de commerce di l'Aigle va quindi risolta nel senso che l'art. 30 del trattato osta a che uno Stato membro applichi ai prodotti importati da un altro Stato membro, ove essi sono legalmente prodotti e messi in commercio, una normativa nazionale che riserva il diritto di usare la denominazione "yogurt" solo allo yogurt fresco e non allo yogurt surgelato, *qualora le caratteristiche di quest' ultimo prodotto non siano sostanzialmente diverse da quelle del prodotto fresco e un'adeguata etichettatura, con l'indicazione della data limite per la vendita o per il consumo, basti a garantire al consumatore una corretta informazione*" (corsivo non testuale). In dottrina cfr. Capelli (1988), p. 391 ss.

[33] Corte di giustizia, sent. 24 giugno 2010, causa C-375/08, *Pontini e a.*, nel cui dispositivo si afferma: "La normativa comunitaria, ed in particolare il regolamento (CE) del Consiglio 17 maggio 1999, n. 1254, relativo all'organizzazione comune dei mercati nel settore delle carni bovine, non subordina l'ammissibilità di una domanda di premi speciali ai bovini maschi e di pagamento per l'estensivizzazione alla produzione di un titolo giuridico valido che giustifichi il diritto del richiedente di utilizzare le superfici foraggere oggetto di tale domanda di aiuti. *Tuttavia, la normativa comunitaria non osta a che gli Stati membri impongano nella loro normativa nazionale l'obbligo di produrre un titolo siffatto, a condizione che siano rispettati gli obiettivi perseguiti dalla normativa comunitaria e i principi generali del diritto comunitario, in particolare il principio di proporzionalità*" (corsivo non testuale)". In argomento cfr. Viscardini Donà (2013), p. 345 ss.

[34] Cfr., ad esempio Gardini (2015), in particolare p. 320 ss.

[35] Salvo sostituirsi di fatto al giudice del rinvio nel valutare la conformità al diritto UE della normativa nazionale *sub iudice.*

[36] Più specificamente, n base a tale norma "1. Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 ["Riservatezza delle comunicazioni"] e 6 ["dati sul traffico"], all´articolo 8, paragrafi da 1 a 4 ["Presentazione e restrizione dell´identificazione della linea chiamante e collegata"], e all´articolo 9 ["Dati relativi all'ubicazione diversi dai dati relativi al traffico"] della presente direttiva, qualora tale restrizione costituisca, ai sensi dell´articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all´interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell´uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l´altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all´articolo 6, paragrafi 1 e 2, del trattato sull´Unione europea".

[37] Cfr. Sent. *H.K.*, cit., punto 26.

Carta dei diritti fondamentali dell'Unione europea[38], deve essere interpretat[a] nel senso che ess[a] osta ad una normativa nazionale, la quale consenta l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi all'ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro *le forme gravi di criminalità* o la prevenzione *di gravi minacce alla sicurezza pubblica (…)*"[39].

Ora, se da un lato risulta indubbia la carente determinatezza delle due formule or ora riportate in corsivo, dall'altro lato appare discutibile che la Corte di giustizia potesse offrire al giudice del rinvio una risposta più circostanziata e vincolante di quella sopra testualmente riportata senza invadere gli spazi di discrezionalità valutativa in linea di principio a lui riservati. Resta il fatto che questa carente determinatezza sembra fatta apposta per supportare le ben note resistenze a conformare in via interpretativa le fonti nazionali a quelle UE[40]. E infatti, chiamata a prendere posizione sulle ricadute nel nostro ordinamento della sentenza in esame[41], la Corte di cassazione[42] non ha mancato di affermare: "non pare che la decisione della Corte di giustizia del 2 marzo 2021 sia idonea ad escludere la sussistenza di residui profili di incertezza interpretativa e discrezionalità applicativa in capo alla normativa interna; in sostanza la richiamata pronuncia europea sembra incapace di produrre effetti applicativi immediati e diretti a causa dell'indeterminatezza delle espressioni ivi utilizzate al fine di legittimare l'ingerenza dell'autorità pubblica nella vita privata dei cittadini[43]. Nell'impossibilità di dibattere in questa sede i profili di criticità di questa presa di posizione della nostra Suprema Corte[44], resta l'amarezza nel constatare le persistenti difficoltà che caratterizzano il dialogo tra i giudici nazionali ed europei.

Un esempio abbastanza recente di sentenza interpretativa *contraddittoria* che merita di essere ricordata – anche se innescata dal rinvio pregiudiziale di un giudice non italiano – si rinviene nella sentenza *Link Logistic*[45]. Come puntualmente segnalato dalla dottrina, questa sentenza da un lato "esclude l'effetto diretto di una direttiva che imponeva allo Stato membro di stabilire sanzioni 'proporzionate', oltre che efficaci e dissuasive, nel caso di violazioni della disciplina sancita dalla stessa direttiva"[46], ma dall'altro lato afferma che "Il giudice nazionale, in virtù del proprio obbligo di adottare tutte le misure appropriate, di carattere generale o particolare, per garantire il rispetto di tale disposizione, deve interpretare il diritto nazionale conformemente alla disposizione medesima, o, qualora tale interpretazione conforme non risulti possibile, disapplicare ogni disposizione nazionale laddove, nelle circostanze del caso di specie, l'applicazione di tale disposizione conduca ad un risultato contrario al diritto dell'Unione"[47]. Ora – come noto e come ribadito dalla Corte di Giustizia nella sentenza *Poplawski II*[48] – solo rispetto alle norme UE dotate di effetto diretto sussiste in capo al giudice interno

[38] Articoli, questi, concernenti: il *rispetto della vita privata e della vita familiare*; la *protezione dei dati di carattere personale*; la *libertà di espressione e d'informazione*; la *portata e interpretazione dei diritti e dei principi.*

[39] Corsivo non testuale.

[40] Resistenze in merito alle quali cfr., per tutti. E. Lamarque (2015), p. 91 ss.

[41] Come noto, infatti, le sentenze interpretative della Corte non rilevano solo in relazione al caso pendente davanti al giudice del rinvio, ma spiegano i loro effetti rispetto ad ogni caso analogo riscontrabile in qualsivoglia Paese UE. Cfr., per tutti, Calzolaio (2009), p. 41 ss.; nonché, più recentemente e anche per ulteriori amplissimi riferimenti dottrinali e giurisprudenziali, Postiglione, (2019).

[42] Sez. 2, sent. 22 luglio 2021, n. 28532.

[43] La stessa sentenza si cura di precisare che "infatti, il riferimento alle 'forme gravi di criminalità' ed alla funzione di 'prevenzione di gravi minacce alla sicurezza pubblica', sembra necessariamente implicare un intervento legislativo volto ad individuare, sulla base di 'criteri oggettivi', così come richiesto dalla stessa pronuncia della Corte europea, le categorie di reati per i quali possa ritenersi legittima l'acquisizione dei dati di traffico telefonico o telematico". In una sua successiva pronuncia (sent. 7 settembre 2021 n. 33116) sempre la Sez. II della Cassazione ha ribadito quanto da lei precedentemente affermato in merito alla genericità della sentenza *H.K.* rispetto ai casi in cui "i dati di traffico telematico e telefonico possono essere acquisiti"; cosicché, in barba all'efficacia erga omnes degli arresti della Corte di Lussemburgo, tale sentenza "non può trovare diretta applicazione in Italia fino a quando non interverrà il legislatore italiano ed europeo.

[44] In merito ai quali cfr. Petroni (2021), par. 5. L'a. ipotizza "la sollecitazione di un intervento della Corte costituzionale, al fine di valutare la compatibilità tra l'articolo 132 del d.lgs. 196/2003 e la direttiva in questione, quale normativa interposta dall'articolo 117 Cost", peraltro esposto alle perplessità che tendono ad accompagnare gli interventi additivi del giudice delle leggi. Per una energica sottolineatura del "contrasto della disciplina interna con gli standard garantistici enucleati dalla Corte di giustizia" nella sentenza *H.K.* cfr. Andolina, (2021), 5, p. 1204 ss.; Rinaldini (2021), 5.

[45] Corte di giustizia, Quinta Sezione, sent. 4 ottobre 2018, *Link Logistic.*

[46] Così, con specifico riferimento al paragrafo 53 della sentenza in oggetto, Viganò (2022), p. 9.

[47] Sentenza *Link Logistic*, cit., punto 62.

[48] Corte di giustizia, Grande Sezione, sent. 24 giugno 2019, causa C-573/17 *Popławski.*

l'obbligo di disapplicazione della normativa nazionale contraria al diritto UE[49]. Rispetto alle norme UE prive di effetto diretto il giudice nazionale è tenuto solo a effettuare l'interpretazione conforme della norma interna[50]: sempreché – come si vedrà in seguito – non si tratti di interpretazione conforme *in malam partem*, la quale è ammissibile solo rispetto alle norme UE dotate di effetto diretto. È dunque lecito considerare la sentenza *Link Logistic* alla stregua di un vero e proprio incidente di percorso nella giurisprudenza della Corte di giustizia[51], reso più problematico dalla generalizzata vincolatività di tale giurisprudenza[52]. Del resto, non è certo un caso se la sentenza *Link Logistic* sia stata una delle poche rispetto alle quali la Corte di giustizia si è sentita in dovere di effettuare un esplicito *overruling* ad opera della sentenza *NE* (a volte citata anche come *NE II*), sulla quale avremo in seguito modo di soffermarci.

4.2. *Sentenze interpretative con effetti* in malam partem *sulla norma penale nazionale.*

Veniamo ora alla seconda ipotesi di sentenze interpretative problematiche: quella che si verifica nei casi in cui la Corte di giustizia dà risposte che conferiscono alla norma UE un significato tale da implicare una dilatazione dell'ambito applicativo della fattispecie penale. Ciò accade – come già ricordato – quando la sentenza della Corte di giustizia richiede implicitamente al giudice nazionale di interpretare estensivamente un elemento costitutivo della fattispecie per conformarlo alle esigenze del diritto UE, ovvero quando la suddetta sentenza vuole portare il giudice in questione a disapplicare tutto o in parte (o a investire il Giudice delle leggi del compito di dichiarare totalmente o parzialmente incostituzionale) una norma esimente o una causa estintiva della punibilità. Si tratta, in sostanza, delle ipotesi in cui la pronuncia della Corte di giustizia si prefigge d'indurre il giudice nazionale ad adottare provvedimenti dotati di effetti penali *in malam partem*[53].

Al riguardo, va subito detto che in un primo tempo gli effetti *in malam partem* del diritto UE sul diritto penale interno non erano stati oggetto di particolari contestazioni in ambito nazionale. Anzi – a seguito delle risalenti sentenze della Corte di giustizia che, dopo aver sancito i principi dell'effetto diretto[54] e del primato[55], segnalavano l'obbligo di conformare il diritto nazionale al diritto (allora) comunitario[56] – i giudici italiani avevano da subito preso l'abitudine di riconoscere l'incidenza non solo *in bonam partem*, ma anche *in malam partem* del diritto UE sul diritto penale nazionale. Talora addirittura, nella consapevolezza di tale obbligo, i nostri giudici avevano ecceduto nel loro "zelo comunitario" effettuando interpretazioni conformi con effetti di sfavore che erano di fatto forme deprecabili di analogia *in malam partem*[57], come tali destinate a essere stigmatizzate dalla dottrina, in quanto appunto esorbitanti il limite dell'interpretazione estensiva imposto dal principio di legalità[58].

Tuttavia, a partire dagli anni '80 del secolo scorso, era stata la stessa Corte di giustizia a

[49] Sent. *Popławski,* cit., punto 109: "Il principio del primato del diritto dell'Unione dev'essere interpretato nel senso che esso non impone a un giudice nazionale di disapplicare una disposizione del diritto nazionale incompatibile con le disposizioni di una decisione quadro, (…) non avendo tali disposizioni effetto diretto".

[50] *Ivi,* punto 109 " (…) Le autorità degli Stati membri, compresi i giudici, sono tuttavia tenute a procedere, quanto più possibile, a un'interpretazione conforme del loro diritto nazionale che consenta loro di garantire un risultato compatibile con la finalità perseguita dalla decisione quadro di cui trattasi".

[51] Cfr., da ultimo e per tutti, Gallo (2022a), p. 591; Groussot, Loxa (2022); Tsolka, (2022), 2, p. 135; Viganò (2022), p. 9.

[52] Anche se, come si sa, il giudice nazionale ha la possibilità di disattendere le statuizioni della Corte di giustizia volte alla disapplicazione della norma interna contrastante col diritto UE attraverso il ricorso diretto ai controlimiti, ovvero invocando attraverso un apposito rinvio pregiudiziale la clausola di identità nazionale prevista dall'articolo 4, par.2, TUE, e così ventilando il rischio di ricorrere ai controlimiti e in tal modo convincendo la Corte di giustizia a ridimensionare le sue pretese. Al riguardo cfr., *infra, sub* par. parr. 4.3 ss.

[53] Per completezza, va detto che un ulteriore effetto *in malam partem* suggerito dalla sentenza interpretativa potrebbe essere quello di orientare la discrezionalità del giudice in sede di commisurazione della pena verso il massimo edittale. Sul punto cfr., volendo, Bernardi (2023), p. 10-11 nt. 41.

[54] Corte di giustizia, sent. 5 febbraio 1963, 5 febbraio 1963, causa 24/62, *van Gend & Loos.*

[55] Corte di giustizia, Sent. 15 luglio 1964, causa C 6/64, *Costa c. Enel.*

[56] Cfr., per tutte, sent. 4 febbraio 1988, causa 157/86, *Murphy*; sent. 13 febbraio 1990, causa 106/89, *Marleasing*; sent. 16 dicembre 1993, causa C-334/92, *Wagner Miret*; sent. 14 luglio 1994, causa 91/92, *Faccini Dori/Recreb*; sent. 12 settembre 1996, causa 168/95, *Arcaro*; sent. 12 dicembre 1996, cause riunite 74/95 e 129/95, *Procedimenti penali c. X.*

[57] Cfr. ad esempio, all'interno di una vasta casistica, Cass. pen., sent. 13 ottobre 1969, in *Foro it.,* 1970, II, c. 57; Trib. Viterbo, 1° dicembre 1981, in *Giur. agr. it.,* 1984, p. 39 ss.; Cass., 6 novembre 1985, in *Cass. pen.,* 1987, p. 103; Pret. Terni, 7 gennaio 1993, in *Dir. com. scambi intern.*, 1994, p. 381.

[58] Cfr., esemplificativamente, Mezzetti (1994), p. 25; Bernardi, (1999), par. 3.1., lett. *a).*

porre un freno alle forme di incidenza *in malam partem* del diritto europeo innescate da una direttiva inattuata. In relazione a tali ipotesi i giudici di Lussemburgo avevano infatti avuto modo di precisare: "il principio che ordina di non applicare la legge penale in modo estensivo a discapito dell'imputato, che è il corollario del principio della previsione legale dei reati e delle pene, e più in generale del principio di certezza del diritto, osta a che siano intentati procedimenti penali a seguito di un comportamento il cui carattere censurabile non risulti in modo evidente dalla legge"[59].

Questa precisazione – che peraltro, va ribadito, riguardava solo le direttive inattuate – era stata accolta con grande soddisfazione dalla dottrina; e addirittura la parte più garantista di quest'ultima si era convinta che la Corte di giustizia avesse avallato la tesi secondo cui dall'interazione tra norme penali nazionali e norme UE non possano mai conseguire effetti *in malam partem*, a prescindere da ogni considerazione in merito al fatto che le norme UE siano prive o no di effetto diretto. Di qui il fuoco di sbarramento ancor oggi (anzi, oggi più che mai) opposto a ogni effetto di sfavore in materia penale derivante dal diritto UE e dalla sua interpretazione da parte della Corte di giustizia[60].

Tuttavia, per contestare la fondatezza di quest'ultima tesi dottrinaria a carattere particolarmente garantista, basti qui sottolineare come non esista nessun motivo plausibile per ammettere – come pacificamente si ammette – che l'interazione tra una norma penale nazionale e un'altra norma nazionale possa determinare, in sede di interpretazione sistematica, un effetto *in malam partem*, e contestualmente negare che un analogo effetto *in malam partem* possa discendere dall'interazione tra una norma penale interna e una norma UE *con efficacia diretta*.

Le norme UE di questo tipo, infatti, da un lato sono gerarchicamente sovraordinate alle norme interne e dall'altro lato non sono certo meno democraticamente legittimate delle norme nazionali a carattere sublegislativo o addirittura delle norme di *soft law* varate da enti privati o da autorità amministrative, laddove è unanimemente ammesso che questi due ultimi tipi di norme possano avere effetti *in malam partem* in sede di interpretazione sistematica della (o di integrazione con la) norma penale[61].

Inoltre, al pari delle norme interne subegislative o di *soft law*, anche le norme UE sono conoscibili dai singoli soggetti, per cui sembra non pertinente l'accusa di imprevedibilità delle interazioni con effetti di sfavore prodotte dalle seconde, ove la stessa accusa non venga mossa anche alle analoghe interazioni prodotte dalle prime.

Infine, altrettanto poco convincente appare la tesi volta a ricondurre il divieto di incidenza *in malam partem* delle fonti UE alla carenza di competenza penale diretta dell'Unione, stante che – per limitarsi a un solo esempio – anche le regioni sono prive di competenza penale, ma ciononostante è pacificamente ammesso che le fonti giuridiche da esse varate possono incidere sfavorevolmente in ambito penale[62].

4.2.1. *Norme penali interne in tema di rifiuti e sentenze interpretative con effetti di sfavore.*

In ogni modo, non mancano certo casi di rinvii pregiudiziali cui hanno fatto seguito sentenze della Corte di giustizia atte a evidenziare obblighi di interpretazione conforme e disapplicazione *in malam partem*. Essi si rinvengono, ad esempio, nel molto discusso settore dei ri-

[59] Corte di giustizia, sent. 12 dicembre 1996, cause riunite 74/95 e 129/95, *Procedimenti penali c. X*, punto 25.

[60] Tra gli studiosi radicalmente contrari ai suddetti effetti di sfavore cfr., in particolare, Manes (2012a), p. 21; Id. (2012b), p. 64; Valentini (2012), p. 169.

[61] Per quanto concerne le norme sublegislative interne, basti pensare al reato di "Produzione, traffico e detenzione illeciti di sostanze stupefacenti o psicotrope previsto dall'art. 73 del Testo unico sugli stupefacenti (D.P.R. 309/1990 e successive modificazioni), il quale per la concreta individuazione delle sostanze da considerare stupefacenti rimanda a un decreto del Ministero della Salute che prevede ed aggiorna le tabelle contenenti l'indicazione delle suddette sostanze (cfr. art. 13 del Testo unico). Per quanto invece concerne le norme di *soft law*, basti penare all'art. 9 codice etico dell'Autorità per l'energia elettrica ed il gas, all'art. 6 codice etico dell'Autorità per le garanzie nelle comunicazioni, all'art. 9 codice etico dell'Autorità garante della concorrenza e del mercato e all'art. 7 codice di comportamento dell'Autorità per la vigilanza sui lavori pubblici. È infatti pacificamente ammesso che tutte queste norme – volte a vietare l'accettazione di regali di non modico valore da parte di soggetti operanti nei settori di competenza di tali Autorità — inducono a interpretare estensivamente gli artt. 318 e 320 c.p., i quali puniscono il pubblico ufficiale o l'incaricato di pubblico servizio "che, per compiere un atto del suo ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetta la promessa".

[62] Per più ampi sviluppi in merito sia alle tesi volte a negare la possibilità che il vincolo dell'interpretazione conforme al diritto UE possa implicare effetti di sfavore, sia agli argomenti atti a contrastare le tesi in questione cfr. Bernardi (2023), p. 40 ss.

fiuti, a sua volta riconducibile al più ampio settore ambientale, che è poi quello maggiormente interessato dalle procedure di infrazione nei confronti dell'Italia[63].

In particolare, numerose pronunce della Corte di giustizia in materia di rifiuti – a cominciare dalla sentenza *Vessoso e Zanetti*[64] – hanno sancito l'obbligo di dilatare la nozione di rifiuto per effetto della normativa (allora) comunitaria, con conseguente estensione delle ipotesi penalmente sanzionate di mancato rispetto delle regole relative allo smaltimento dei rifiuti.

La capacità del diritto europeo di ampliare l'ambito del penalmente rilevante indipendentemente dal volere del legislatore nazionale divenne ancora più evidente con le sentenze *Tombesi*[65] e *Niselli*[66], anch'esse in materia di rifiuti. In entrambe le sentenze, tra loro assai simili, la Corte ebbe modo di affermare che la illegittima modifica in senso restrittivo, da parte del diritto nazionale, di un elemento normativo della fattispecie di cui una fonte UE forniva una puntuale definizione poteva implicare la disapplicazione della norma interna di favore responsabile di tale modifica, con conseguente riespansione della norma generale indebitamente compressa. La Corte di giustizia ebbe modo altresì di precisare che, in ragione della sua disapplicazione, quest'ultima norma non poteva inibire la condanna di quanti avessero commesso il fatto in un momento precedente alla sua entrata in vigore, tale condanna non ponendosi in contrasto col principio di legalità penale.

Le succitate sentenze, invero, furono accolte con perplessità da una parte dei commentatori; tant'è che proprio in relazione ad esse la dottrina italiana incominciò per la prima volta a ipotizzare il ricorso ai controlimiti costituzionali rispetto al diritto UE[67]. Peraltro, come ammesso da quella stessa dottrina, si sarebbe trattato di un uso dei controlimiti non solo disinvolto, ma addirittura del tutto infondato, visto che le fonti europee incidenti *in malam partem* sulla disciplina penale italiana in materia di rifiuti si limitavano a paralizzare il principio di *retroattività favorevole* nel caso in cui le norme nazionali di favore incompatibili con la normativa UE fossero state disapplicate; laddove va ricordato che all'epoca dei fatti tale principio, diversamente dal principio di *irretroattività della norma di sfavore*, non era affatto di rango costituzionale[68], e men che meno faceva parte del nucleo intangibile della nostra Suprema Carta cui rimanda la teoria dei controlimiti[69].

Ovviamente, è impossibile in questa sede approfondire tutte le tematiche penalistiche poste dalla saga relativa ai rapporti tra normativa penale italiana e diritto UE in tema di rifiuti. Anche perché questa saga si arricchisce di continuo di ulteriori capitoli, quasi sempre poco lusinghieri per il nostro Paese. Basti ricordare, cursoriamente, che l'Italia è stata a più riprese condannata dalla Corte di giustizia per violazione degli obblighi UE in tema di rifiuti[70]; che ciclicamente – nel tentativo di colmare per via interpretativa le lacune legislative in materia – la nostra Corte di Cassazione prende posizione in merito alla corretta individuazione dei confini della nozione di "rifiuto", estendendone la portata alla luce del diritto UE[71]; che a seguito di rinvii pregiudiziali la Corte di giustizia continua a pronunciare sentenze che invitano i giudici nazionali a interpretare con estremo rigore le norme penali vigenti in tema di

[63] In questo senso cfr., ad esempio, *Le procedure di infrazione rientranti nella competenza del Ministero della transizione ecologica - Gli strumenti per la prevenzione e la riduzione*, in *www.camera.it*. Cfr. altresì, da ultimo, Dipartimento per le politiche europee, *Infrazioni, Commissione europea archivia cinque procedure*, in *www.politicheeuropee.gov.it*, 5 ottobre 2022, ove si ricorda che "L'ambiente con 16 procedure aperte resta il settore dove più alta è l'incidenza delle infrazioni (il 19% sul totale)".

[64] Corte di giustizia, Prima Sezione, sent. 28 marzo 1990, cause riunite C-206/88 e C-207/88, *procedimento penale contro G. Vessoso e G. Zanetti*. A giudizio della Corte "La nozione di rifiuto, ai sensi dell'art. 1 delle direttive del Consiglio 75/442/CEE e 78/319/CEE, non dev'essere intesa nel senso che esclude le sostanze e gli oggetti suscettibili di riutilizzazione economica. Tale nozione non presuppone che il detentore che si disfa di una sostanza o di un oggetto abbia l'intenzione di escluderne ogni riutilizzazione economica da parte di altre persone".

[65] Corte di giustizia, Sesta Sezione, sent. 25 giugno 1997, cause riunite C-304/94, C-330/94, C-342/94 e C-224/95, *Procedimenti penali a carico di Euro Tombesi e Adino Tombesi (C-304/94), Roberto Santella (C-330/94), Giovanni Muzi e altri (C-342/94) e Anselmo Savini (C-224/95)*.

[66] Corte di giustizia, Seconda Sezione, sent. 11 novembre 2004, causa C-457/02, *Procedimento penale a carico di Antonio Niselli*.

[67] Cfr. A. Borzì (2005), p. 26.

[68] Sulla problematica evoluzione nella giurisprudenza costituzionale italiana del principio di retroattività favorevole "sotto l'influsso di (…) fonti pattizie e arresti di corti internazionali" cfr. Viganò (2011). In argomento cfr. altresì, per tutti, Poli (2012); Martufi (2013), p. 488 ss.; Mazzacuva (2016), p. 244 ss.

[69] Bernardi (2017d), p. LXXXIV-LXXXVI.

[70] Cfr., ad esempio, Sez. Grande, sent. 2 dicembre 2014, causa C-196/13. In tale sentenza l'Italia è stata condannata a una somma forfettaria di 40 milioni di euro per non avere dato esecuzione a una precedente sentenza di condanna nei suoi confronti (Corte di giustizia, terza sez., sentenza 26 aprile 2007, causa C-135/05) causata dall'inadempimento delle direttive europee sui rifiuti. Alla succitata somma vanno aggiunti 42,8 milioni di euro per ogni semestre di ritardo nell'attuazione delle misure necessarie a dare piena esecuzione alla sentenza del 2007 or ora citata. In argomento cfr. Croci (2015).

[71] Cfr., per tutte, Terza sezione penale, sent. 16 novembre 2016, n. 48316, in merito alla quale cfr., ad esempio, G. Guagnini (2016).

rifiuti[72]; che, nonostante tutto, le procedure di infrazione in materia a carico del nostro Stato si susseguono[73].

La prima, banale conclusione che si può trarre da una generalissima panoramica della lontananza esistente tra le aspettative europee in tema di rifiuti e lo stato della normativa penale e della prassi italiana di settore è che i molti rinvii pregiudiziali effettuati dai giudici italiani in questa tormentata materia e le conseguenti sentenze interpretative della Corte di giustizia da un lato hanno consentito di prendere contezza del "diritto vivente UE"[74] e, in taluni casi, di sanzionare condotte la cui illiceità discende dall'interazione tra norme nazionali e norme europee in materia; ma dall'altro lato non possono consentire al giudice interno di interpretare estensivamente le norme penali di settore al di là di quanto ammesso dal principio di legalità[75]. Ovviamente, poi, tali rinvii pregiudiziali e tali sentenze nemmeno possono ambire a colmare del tutto certi divari "culturali" di cui è espressione la nostra legislazione e le nostre abitudini nel settore ambientale; settore nel quale, invero, è stata accertata dalla Corte di giustizia l'esistenza in Italia di un problema strutturale. Espressioni di questo problema sono: la tendenza a disattendere in modo generalizzato e persistente gli obblighi concernenti lo smaltimento dei rifiuti di ogni tipo e la gestione delle discariche[76]; la propensione a persistere negli inadempimenti anche dopo le sentenze di condanna della Corte di giustizia[77]; l'attitudine a incorrere in nuove procedure di infrazione per il mancato recepimento di recenti direttive in tema di rifiuti[78].

La scarsa sensibilità dell'Italia al problema ambientale potrebbe indurre ad auspicare la previsione anche in ambito UE un qualcosa di simile alla "procedura di sentenza pilota". Procedura attraverso la quale – come noto – la Corte EDU può accertare non solo l'inadempimento nel caso concreto sottoposto al suo esame, ma anche il "problema strutturale sottostante", vale a dire la l'esistenza nell'ordinamento dello Stato membro di una legislazione e/o di una prassi amministrativa o giudiziaria tali da comportare una violazione sistemica e continuativa della CEDU. Trapiantata in ambito UE questa procedura potrebbe servire a far meglio interagire tra loro Corte di giustizia e Stato inadempiente, in vista di una soluzione del problema sistemico individuato dalla Corte.

4.3. *Sentenze interpretative in tendenziale conflitto con principi/diritti costituzionali.*

Passo infine alla terza ipotesi di sentenze interpretative problematiche: quella in cui, a seguito di un rinvio pregiudiziale, la Corte di giustizia dà risposte che conferiscono alla norma UE di cui viene chiesta l'interpretazione un significato tale da far sì che l'eventuale adeguamento ad essa della norma penale nazionale per via interpretativa, ovvero la disapplicazione totale o parziale della stessa norma da parte del giudice interno, potrebbe contrastare con i dettami della Costituzione nazionale. Donde la necessità di vagliare se questo eventuale contrasto concerna i principi supremi e i diritti fondamentali sanciti dalla Suprema Carta, e se dunque sussistano le condizioni per le quali il suddetto contrasto possa implicare il ricorso ai

[72] Al riguardo cfr., emblematicamente, Corte di giustizia, Decima Sezione, sent. 28 marzo 2019, Cause riunite C-487/17 – C-489/17, *Procedimento penale a carico di Alfonso Verlezza e altri*. In tale sentenza, infatti, la Corte ha affermato che "2) Il principio di precauzione deve essere interpretato nel senso che, qualora, dopo una valutazione dei rischi quanto più possibile completa tenuto conto delle circostanze specifiche del caso di specie, il detentore di un rifiuto che può essere classificato sia con codici corrispondenti a rifiuti pericolosi sia con codici corrispondenti a rifiuti non pericolosi si trovi nell'impossibilità pratica di determinare la presenza di sostanze pericolose o di valutare le caratteristiche di pericolo che detto rifiuto presenta, quest'ultimo deve essere classificato come rifiuto pericoloso".

[73] Per un desolante elenco, aggiornato al dicembre 2020, delle procedure pendenti contro l'Italia per mancato recepimento o sbagliata applicazione della normativa UE in tema di rifiuti cfr. M. Bavazzano (2020).

[74] Sia pure con le precisazioni di cui *supra, sub* par. 4.1, lett. *a)* e *b)*.

[75] Come ovvio, infatti, riconoscere la possibilità per le norme UE con effetto diretto di incidere sfavorevolmente sull'interpretazione delle norme penali nazionali non significa affatto legittimare il giudice nazionale a effettuare operazioni più o meno mascherate di analogia *in malam partem*. Operazioni, queste, peraltro effettuate a più riprese. In merito agli eccessi giurisprudenziali dell'interpretazione conforme *in malam partem* per ragioni di "fedeltà comunitaria" e dei relativi scivolamenti nell'analogia effettuati dai giudici italiani e avallati da una parte della dottrina nei primi decenni della costruzione europea cfr. Bernardi (2023), p. 13 ss.

[76] Cfr. M. Bavazzano (2020).

[77] Cfr., *supra, sub* nt. 70.

[78] Cfr. le procedure di infrazione 2020/0209 e 2020/0210 dovute al mancato recepimento della direttiva 2020/362 e della direttiva 2020/363, entrambe concernenti i veicoli fuori uso. Fortunatamente, almeno queste procedure sono state infine archiviate: cfr. *Procedure di infrazione archiviate nel 2021*, in *www.politicheeuropee.gov.it*, 22 novembre 2021.

controlimiti[79].

Specialmente in materia penale sentenze interpretative siffatte stanno divenendo meno infrequenti, essenzialmente per due ordini di ragioni. In primo luogo, come in precedenza sottolineato, col succedersi dei Trattati sono aumentati gli ambiti di competenza del diritto UE ricchi di ricadute sul diritto penale interno, e di conseguenza si sono moltiplicate le norme penali nazionali considerate attuative del diritto UE, dunque obbligate a conformarvisi. In secondo luogo, la Corte di giustizia ha assunto sempre più un ruolo protagonistico nel potenziare gli effetti della normativa europea in ambito penale, estendendo per via pretoria le competenze attribuite prima alla Comunità e poi all'Unione[80].

Ovviamente, con l'aumento delle interrelazioni tra diritto penale nazionale e diritto UE, sono destinati ad aumentare anche i contrasti tra di essi ricchi di ricadute in ambito costituzionale. A ciò si aggiunga che, con la crescita un po' ovunque delle formazioni politiche di impronta sovranista, i Paesi membri appaiano sempre meno inclini a sottomettersi all'Unione, e sempre più gelosi delle proprie prerogative sovrane e della loro identità costituzionale[81]; di conseguenza le Corti costituzionali nazionali sembrano vieppiù propense a impadronirsi dello strumento del rinvio pregiudiziale per ventilare il ricorso ai controlimiti o addirittura per brandirli risolutamente al fine di bloccare le pretese della Corte di giustizia in merito all'adeguamento del diritto penale interno al diritto UE.

Qui mi limiterò a ricordare due casi concernenti rinvii pregiudiziali cui hanno fatto seguito sentenze interpretative alquanto problematiche sotto il profilo dei principi/diritti previsti dalle Costituzioni nazionali: il primo caso (*Taricco*) riguarda una eclatante ipotesi di incidenza disapplicativa *in malam partem*; il secondo (*NE*) attiene a una recentissima ipotesi di incidenza disapplicativa *in bonam partem.*

4.3.1. *Il caso* Taricco.

Passo dunque al caso *Taricco* e al tanto discusso "dialogo" intercorso tra la Corte di giustizia e la nostra Corte costituzionale dopo che, in risposta ad un ricorso pregiudiziale, la prima aveva chiesto al giudice nazionale la disapplicazione *in malam partem* della normativa italiana in tema di prescrizione.

Questo caso giurisprudenziale è stato senza alcun dubbio, tra quelli italiani, il più commentato di sempre, risultando per alcuni anni al centro del dibattito penalistico, europeistico e costituzionalistico. Del resto, anche nel nostro Dipartimento il caso *Taricco* è stato a più riprese analizzato in appositi seminari e incontri[82]; peraltro, queste occasioni di dibattito rimontano ormai ad alcuni anni fa, cosicché sembra opportuno riassumere qui per sommi capi il caso in questione, per poi provare a trarre da esso alcune conclusioni a carattere generale.

4.3.1.1. *(segue). Il rinvio pregiudiziale che ha innescato il caso, l'obbligo di disapplicazione della prescrizione sancito dalla Corte di giustizia e i problemi di legalità connessi a tale obbligo.*

Il caso *Taricco* nasce all'inizio del 2014 su iniziativa del GUP presso il Tribunale di Cu-

[79] Si allude, essenzialmente, a casi in cui tale contrasto investa settori normativi "non integralmente armonizzati" dalla normativa UE. Infatti, come affermato dalla Corte di giustizia (sent. 26 febbraio 2013, in causa C-617/10, *Fransson*, punto 29; sent. 26 febbraio 2013, in causa C-399/11, *Melloni*, punto 60) e come riconosciuto anche dalla nostra Corte costituzionale nella ordinanza n. 216 del 2021, punto 7.3, "è (…) precluso agli Stati membri condizionare l'attuazione del diritto dell'Unione, nei settori oggetto di integrale armonizzazione, al rispetto di standard puramente nazionali di tutela dei diritti fondamentali, laddove ciò possa compromettere il primato, l'unità e l'effettività del diritto dell'Unione". In questi ultimi settori, dunque, "I diritti fondamentali al cui rispetto la [normativa UE è vincolata (…), sono, piuttosto, quelli riconosciuti dal diritto dell'Unione europea, e conseguentemente da tutti gli Stati membri allorché attuano il diritto dell'Unione: diritti fondamentali alla cui definizione, peraltro, concorrono in maniera eminente le stesse tradizioni costituzionali comuni agli Stati membri (artt. 6, par. 3, TUE e 52, par. 4, CDFUE)".

[80] Sul punto cfr. Bernardi (2017d), p. LXVI ss.

[81] In argomento cfr. già, esemplificativamente e con varietà di accenti, O. Pollicino (2012); M. Luciani (2016), p. 72 ss.; più recentemente J. Scholtes (2021), p. 534 ss. Cfr. altresì, da ultimo, P. Faraguna (2022) p. 65 ss.

[82] Il più importante dei quali è stato senz'altro il convegno "Il caso Taricco e il dialogo tra le Corti" del 24 febbraio 2017.

neo[83]. Nel corso di un processo per reati rientranti nel novero delle c.d. frodi comunitarie, questo giudice acquisisce la consapevolezza che il processo in questione non potrà concludersi prima del decorso dei termini di prescrizione. Nel dubbio che talune norme del TFUE[84], unitamente a una fonte di diritto derivato[85], inibiscano "ad uno Stato di mantenere una norma che consenta di prosciogliere i presunti autori dei suddetti reati nonostante l'azione penale sia stata tempestivamente esercitata"[86], il GUP effettua dunque un rinvio pregiudiziale alla Corte di giustizia concernente la conformità o meno al diritto UE della disciplina italiana della prescrizione.

Anche se sulla base di altre e più pertinenti norme UE di diritto primario e derivato che obbligano gli Stati membri a prevedere sanzioni "effettive, proporzionate e dissuasive"[87], l'Avvocato generale si convince della fondatezza dei dubbi del GUP di Cuneo, ritenendo che "una normativa nazionale sulla prescrizione dei reati la quale, per motivi sistemici, comporta in numerosi casi la non punibilità dei responsabili" delle suddette frodi "deve essere disapplicata dai giudici nazionali in procedimenti penali pendenti"[88].

Il punto di vista dell'Avvocato generale viene accolto dalla Corte di giustizia, la quale nella ormai celeberrima sentenza *Taricco*[89] ritiene che la disciplina italiana della prescrizione si ponga in insanabile contrasto con l'art. 325 parr. 1 e 2 TFUE[90] "nell'ipotesi in cui detta normativa nazionale impedisca di infliggere sanzioni effettive e dissuasive in un *numero considerevole di casi di frode grave* che ledono gli interessi finanziari dell'Unione europea"[91]. La Corte riconosce l'effetto diretto della norma in questione e – in ragione del primato di quest'ultima sul diritto interno – afferma che "Il giudice nazionale è tenuto a dare piena efficacia all'articolo 325, paragrafi 1 e 2, TFUE disapplicando, all'occorrenza, le disposizioni nazionali che abbiano per effetto di impedire allo Stato membro interessato di rispettare gli obblighi impostigli dall'articolo 325, paragrafi 1 e 2, TFUE"[92].

All'evidenza, la sentenza *Taricco* della Corte di giustizia poneva enormi problemi al giudice nazionale. E questo non tanto e non solo perché secondo una parte della dottrina – come in precedenza ricordato – una norma UE, anche se dotata effetto diretto, non potrebbe mai produrre effetti penali *in malam partem*: si è infatti già avuto modo di prendere posizione contro questa tesi, certo suggestiva ma priva di solide basi argomentative[93]. In realtà, i problemi più gravi posti dalla pronuncia dei giudici del Kirchberg erano legati al fatto che essa veniva a vulnerare il principio di legalità penale in tutti i suoi corollari "astorici" e "storici"[94], e giungeva financo ad intaccare lo stesso principio di separazione dei poteri. In ogni caso, i fondamentali problemi sollevati dalla sentenza in esame riguardavano innanzitutto il principio di legalità nei suoi corollari di determinatezza e irretroattività sfavorevole.

In particolare, quanto al primo di questi corollari, risultavano vaghe e imprecisa le espressioni "frode grave" e "numero considerevole di casi", con conseguente impossibilità per il giudice interno di ben focalizzare le ipotesi in cui dover disapplicare la prescrizione. Quanto poi al principio di irretroattività sfavorevole, agli occhi del giurista italiano esso appariva macro-

[83] GUP Tribunale di Cuneo, *Ordinanza di rimessione alla Corte di giustizia dell'Unione europea*, 17 gennaio 2014, in *Dir. pen. cont.*
[84] Per la precisione, gli artt. 101, 107 e 119 TFUE.
[85] Per la precisione, la direttiva 2006/112/CE del Consiglio del 28 novembre 2006, *relativa al sistema comune d'imposta sul valore aggiunto*.
[86] GUP Tribunale di Cuneo, *Ordinanza di rimessione alla Corte di giustizia dell'Unione europea*, cit.
[87] Per una elencazione di tali norme cfr. *Conclusioni dell'avvocato generale Juliane Kokott* presentate il 30 aprile 2015, in *curia.europa.eu*, punto 36.
[88] *Ivi*, punto 128.3.
[89] Grande sezione, sent. 8 settembre 2015, causa C-105/14, *Taricco*.
[90] In base a tale norma "1. L'Unione e gli Stati membri combattono contro la frode e le altre attività illegali che ledono gli interessi finanziari dell'Unione stessa mediante misure adottate a norma del presente articolo, che siano dissuasive e tali da permettere una protezione efficace negli Stati membri e nelle istituzioni, organi e organismi dell'Unione. 2. Gli Stati membri adottano, per combattere contro la frode che lede gli interessi finanziari dell'Unione, le stesse misure che adottano per combattere contro la frode che lede i loro interessi finanziari".
[91] Sent. *Taricco*, punto 66.1 (corsivo non testuale). Nello stesso paragrafo la Corte di giustizia afferma la sussistenza di un insanabile contrasto con diritto UE della suddetta normativa nazionale anche nell'ipotesi "in cui preveda, per i casi di frode che ledono gli interessi finanziari dello Stato membro interessato, termini di prescrizione più lunghi di quelli previsti per i casi di frode che ledono gli interessi finanziari dell'Unione europea, circostanze che spetta al giudice nazionale verificare".
[92] *Ibidem*. In base all'art. 325 TFUE "1. L'Unione e gli Stati membri combattono contro la frode e le altre attività illegali che ledono gli interessi finanziari dell'Unione stessa mediante misure adottate a norma del presente articolo, che siano dissuasive e tali da permettere una protezione efficace negli Stati membri e nelle istituzioni, organi e organismi dell'Unione. 2. Gli Stati membri adottano, per combattere contro la frode che lede gli interessi finanziari dell'Unione, le stesse misure che adottano per combattere contro la frode che lede i loro interessi finanziari".
[93] Al riguardo cfr. *supra, sub* par. 4.2.
[94] Come noto, i corollari "storici" del principio di legalità sono quelli – variabili da un Paese all'altro e da un'epoca all'altra – deputati a stabilire quali siano gli organi legittimati a produrre norme penali; i corollari "astorici" sono invece quelli – almeno tendenzialmente accolti ovunque e in tutte le epoche – di determinatezza, accessibilità, prevedibilità, irretroattività della norma penale (e dello stesso diritto penale vivente di fonte giurisprudenziale). In argomento cfr., in particolare, Palazzo (1999), p. 205.

scopicamente vulnerato da una disapplicazione della prescrizione da effettuarsi anche nei casi di frode commessi in un momento precedente al deposito della sentenza *Taricco*.

Nonostante questo, è verosimile ritenere che la Corte di giustizia non immaginasse che la disapplicazione della prescrizione da lei imposta potesse comportare significativi problemi sul piano della legalità penale. E ciò in quanto, di regola, nei Paesi europei la disciplina della prescrizione afferisce al diritto penale processuale, nel quale i corollari del principio di legalità assumono profili diversi da quelli propri del diritto penale sostanziale, specie per quanto concerne il corollario della irretroattività sfavorevole. Stante però che nell'ordinamento italiano la prescrizione afferisce diritto penale sostanziale, nel nostro Paese la sentenza *Taricco* ha comprensibilmente creato un grande sconcerto e dato la stura a una valanga di commenti dottrinali variamente orientati circa l'opportunità o meno di ricorrere ai controlimiti per paralizzare gli effetti di questa pronuncia.

4.3.1.2. *(segue). Le differenti reazioni dei giudici nazionali alla sentenza* Taricco*, il rinvio pregiudiziale della Corte costituzionale, la sentenza* M.A.S. *della Corte di giustizia, la definitiva risposta della Corte costituzionale.*

Anche le prime reazioni dei giudici italiani alla presa di posizione della Corte di giustizia sono state di segno diverso. Così, mentre in relazione a un caso di frodi comunitarie la terza sezione della Corte di cassazione[95] decideva di disapplicare la prescrizione, rispetto a casi analoghi la Corte di appello di Milano[96] e successivamente la stessa terza sezione della Corte di cassazione[97] ritenevano che la sentenza Taricco entrasse in conflitto coi tutta una serie di articoli della nostra Costituzione[98] concernenti taluni principi supremi e diritti fondamentali; di conseguenza, queste ultime due Corti sospendevano i relativi processi e sollevavano dinanzi al giudice delle leggi la questione di legittimità costituzionale dell'art. 2 della legge 2 agosto 2008, n. 130 relativo alla *Ratifica ed esecuzione del Trattato di Lisbona*[99].

Dal canto suo la Corte costituzionale, invece di decidere in merito a tale questione, sospendeva il giudizio e – ribadendo la sua natura di "giurisdizione nazionale" ai sensi dell'art. 267 TFUE anche per quanto concerne i giudizi instaurati in via incidentale[100] – effettuava un rinvio pregiudiziale alla Corte di giustizia sull'interpretazione dell'articolo 325 TFUE[101]. In questo rinvio il nostro giudice delle leggi si riagganciava ad alcuni passaggi della sentenza Taricco per adombrare il rischio (peraltro diplomaticamente definito "sommamente improbabile") di dover ricorrere all'estremo rimedio dei controlimiti laddove e gli effetti sul diritto interno derivanti da tale articolo risultassero in insanabile contrasto coi principi supremi e i diritti fondamentali della nostra Costituzione[102]. Con l'evidente intento di favorire un ripensamento della Corte di giustizia, la Corte costituzionale ricordava innanzitutto che nell'ordinamento italiano l'istituto della prescrizione afferisce al diritto penale sostanziale e sottolineava che nel sistema costituzionale del nostro Paese il principio di legalità penale ha un coefficiente garantistico più elevato di quello proprio del corrispondente principio inscritto nell'art. 49.1 CDFUE. Richiamava poi l'attenzione della Corte di giustizia sull'art. 53 CDFUE, in base al quale "Nessuna disposizione della presente Carta deve essere interpretata come limitativa o lesiva dei diritti dell'uomo e delle libertà fondamentali riconosciuti (…) dalle costituzioni degli Stati membri". Ancora, la Corte costituzionale ipotizzava che l'art. 325 TFUE sarebbe contrario all'art. 49.1 CDFUE laddove imponesse al giudice nazionale un obbligo di disappli-

[95] Sent. n. 2210 del 17 settembre 2015, *Pennacchini*, Rv. 266121.
[96] App. Milano, Sez. II, ord. n. 339 del 18 settembre 2015, *De Bortoli e altri.*
[97] Sez. 3, ord. n. 28346 del 30 marzo 2016, *Cestari*, Rv. 267259 -
[98] Artt. 3, 11, 25 comma secondo, 27, comma terzo, 101, comma secondo, Cost.
[99] Per la precisione, l'incidente di legittimità costituzionale concerneva l'articolo in oggetto "nella parte in cui autorizza alla ratifica e rende esecutivo l'art. 325, paragrafi 1 e 2, del Trattato sul funzionamento dell'Unione europea (TFUE), sottoscritto a Roma il 25 marzo 1957 (Testo consolidato con le modifiche apportate dal Trattato di Lisbona 13 dicembre 2007), come interpretato dalla sentenza della Grande Sezione della Corte di giustizia dell'Unione europea 8 settembre 2015 in causa C-105/14, Taricco".
[100] Cfr. *supra, sub* par. 4, nt. 25.
[101] Corte cost., ord. n. 24 del 2017, reperibile in *www.giurcost.org*.
[102] *Ivi*, punto 2: "Se l'applicazione dell'art. 325 del TFUE comportasse l'ingresso nell'ordinamento giuridico di una regola contraria al principio di legalità in materia penale, come ipotizzano i rimettenti, questa Corte avrebbe il dovere di impedirlo".

cazione della prescrizione in casi tutt'altro che "chiari e precisi".

Nonostante una certa raffinatezza argomentativa assai lodate da larga parte della dottrina, l'ordinanza in questione non risultava a mio giudizio esente da critiche qui impossibili da riproporre per esteso. Mi limito quindi a ricordare che a più riprese non ho apprezzato alcuni passaggi di questa ordinanza[103]; passaggi rivelatori – sempre a mio giudizio – di un approccio "sovranista" ai rapporti tra ordinamento nazionale e ordinamento UE che nel caso di specie si è tradotto in una difesa a spada tratta della disciplina italiana della prescrizione, viceversa bisognosa di una integrale riforma. In particolare, lungi dall'"aprire" alla natura – se non esclusivamente processuale – quantomeno "mista" o "ibrida" della prescrizione[104], la Corte costituzionale ha insistito nell'affermare la natura esclusivamente sostanziale di tale istituto, e dunque l'ineludibile riconducibilità di quest'ultimo all'interno del principio di legalità penale[105]. In tal modo l'obbligo di disapplicare la prescrizione, derivante dal contrasto della disciplina italiana di quest'ultima col diritto UE, sarebbe stato paralizzato grazie alla teoria dei controlimiti, dal giudice delle leggi mai esplicitamente menzionata, ma nel rinvio pregiudiziale insistentemente sottintesa e valorizzata nella sua tradizionale configurazione[106]. In sostanza, quindi, il "dialogo" imbastito dalla Corte costituzionale solo a prima vista sembrava collocarsi in un contesto di "costituzionalismo cooperativo", assumendo in effetti un accento spiccatamente "nazionalista" che sovrastava ogni prospettiva europeista.

Avvertendo il concreto pericolo del ricorso ai controlimiti da parte della Corte costituzionale, la Corte di giustizia nella sentenza *M.A.S* (spesso ribatezzata "*Taricco 2*")[107] decideva di non seguire la posizione intransigente suggerita dall'avvocato generale, volta a ribadire il primato del diritto UE anche a discapito della identità costituzionale del nostro Stato. I giudici di Lussemburgo riconoscevano dunque, con fare conciliante, che "i requisiti di prevedibilità, determinatezza e irretroattività inerenti al principio di legalità dei reati e delle pene si applicano, nell'ordinamento giuridico italiano, anche al regime di prescrizione relativo ai reati in materia di IVA"[108] attuativi del diritto UE; di conseguenza essi giungevano ad ammettere che tali requisiti "ostano a che, in procedimenti relativi a persone accusate di aver commesso reati in materia di IVA prima della pronuncia della sentenza Taricco, il giudice nazionale disapplichi le disposizioni del codice penale in questione"[109].

La Corte di giustizia, comunque, non si limitava a concessioni circoscritte alla questione della irretroattività. Essa infatti riconosceva che, nel caso in cui la sentenza *Taricco* "conduca a una situazione di incertezza nell'ordinamento giuridico italiano quanto alla determinazione del regime di prescrizione applicabile, incertezza che contrasterebbe con il principio della determinatezza della legge applicabile (…), il giudice nazionale non sarebbe tenuto a disapplicare le disposizioni del codice penale"[110].

In sostanza, dunque, preso atto che nell'ordinamento italiano la disciplina della prescrizione deve rispettare tutti i corollari della legalità penale sostanziale, la Corte di giustizia faceva retromarcia rispetto alla sentenza *Taricco*[111], consentendo ai giudici italiani di non disapplicare la prescrizione nell'ambito dei processi concernenti "frodi comunitarie".

[103] Cfr. Bernardi (2017e), p. 109 ss.; Id. (2017c), p. 48 ss.; Id. (2017f), p. 17 ss.

[104] Tesi, questa, rilanciata da una parte della dottrina italiana proprio a seguito della sentenza *Taricco* e della attitudine del diritto UE a favorire processi di armonizzazione financo in relazione alla parte generale del diritto penale: cfr., per tutti, Salcuni (2015), p. 10 ss.; Faraguna, Perini (2016) p. 15 s.; Viganò (2016), p. 266 ss.; Silvani (2009), *passim*.

[105] Così Bignami (2017), p. 38 ss. Cfr. altresì, più o meno esplicitamente, Riccardi (2017), p. 369 ss.; Sotis, (2017), p. 446 ss.; Viganò (2017), p. 475 ss.

[106] Nell'ordinanza in esame la Consulta, invero, fa chiaramente intendere che a suo giudizio i controlimiti non sono stati affatto "europeizzati" dal Trattato di Lisbona, e dunque non sono stati affidati esclusivamente alla Corte di giustizia, ma restano nelle sue mani. Pertanto, sempre a giudizio della Consulta, è "ragionevole attendersi che (…) il giudice europeo provveda a stabilire il significato della normativa dell'Unione, rimettendo alle autorità nazionali la verifica ultima circa l'osservanza dei principi supremi dell'ordinamento nazionale" (par. 6, ultimo comma).

[107] Grande camera, sent. 5 dicembre 217, causa C-42/17, *M.A.S., M.B.*

[108] Punto 58.

[109] Punto 60. In questo stesso paragrafo della sentenza la Corte di giustizia prosegue affermando che "Infatti, la Corte ha già sottolineato, al paragrafo 53 di tale sentenza, che a dette persone potrebbero, a causa della disapplicazione di queste disposizioni, essere inflitte sanzioni alle quali, con ogni probabilità, sarebbero sfuggite se le suddette disposizioni fossero state applicate. Tali persone potrebbero quindi essere retroattivamente assoggettate a un regime di punibilità più severo di quello vigente al momento della commissione del reato".

[110] Punto 59.

[111] Ma, invero, in nome del rispetto dell'identità costituzionale nazionale qualcosa la Corte di giustizia sembrava essere disposta a concedere già in occasione della sentenza *Taricco*, quando al punto 53 affermava che "se il giudice nazionale dovesse decidere di disapplicare le disposizioni nazionali di cui trattasi, egli dovrà allo stesso tempo assicurarsi che i diritti fondamentali degli interessati siano rispettati. Questi ultimi, infatti, potrebbero vedersi infliggere sanzioni alle quali, con ogni probabilità, sarebbero sfuggiti in caso di applicazione delle suddette disposizioni di diritto nazionale". Anche se poi, a dire il vero, sosteneva che quanto da lei richiesto non implicasse una violazione dei diritti in questione (cfr. punto 58).

L'ultima tappa della saga *Taricco* si è comunque avuta con la sentenza 115/2018 della Corte costituzionale, chiamata a giudicare in merito alla questione di legittimità costituzionale[112] del già ricordato art. 2 della Legge 2 agosto 2008, n. 130, concernente la *Ratifica ed esecuzione del Trattato di Lisbona*. In questa sentenza veniva ribadito che la situazione in presenza della quale – a giudizio della Corte di giustizia – i giudici interni dovrebbero disapplicare la prescrizione risulta in insanabile contrasto col fondamentalissimo principio di legalità nei suoi corollari di irretroattività sfavorevole e determinatezza. In definitiva, per la Corte costituzionale, la "regola *Taricco*" fissata dalla Corte di giustizia (la regola, cioè, secondo cui la prescrizione deve essere disapplicata laddove essa impedisca di infliggere sanzioni effettive e dissuasive in un numero considerevole di casi di frode grave di rilievo UE) confligge irrimediabilmente con un principio supremo del nostro sistema costituzionale e deve dunque essere ignorata dal giudice interno[113].

Di più: secondo il nostro giudice delle leggi la "*regola Taricco*" renderebbe l'art. 325 TFUE incapace di offrire ai singoli soggetti "una percezione sufficientemente chiara ed immediata" dei casi di inapplicabilità della prescrizione, cosicché nemmeno una ulteriore precisazione per via giurisprudenziale della *regola* in questione riuscirebbe a sanare "l'eventuale originaria carenza di precisione del precetto penale"[114]. Infine, rincarando la dose, la Corte costituzionale è giunta ad affermare che la "regola *Taricco*" si pone in contrasto non solo con principi supremi inscritti nella nostra Suprema Carta, ma anche con "lo stesso diritto dell'Unione"[115], cosicché l'inapplicabilità della "regola" in oggetto discenderebbe, oltreché dalla Costituzione italiana, persino dal diritto UE.

4.3.1.3. *Brevi osservazioni in margine alla saga* Taricco.

Cosa ha insegnato la saga *Taricco,* ormai da tempo conclusa? Certamente, dovrebbe aver insegnato alla Corte di giustizia maggiore attenzione e cautela, stante la constatazione che le argomentazioni contenute nella sua prima sentenza sono apparse particolarmente fragili[116], e che tutto fuorché felice è stata la sua presa di posizione circa l'obbligo per il giudice nazionale di disapplicare la prescrizione in casi non ben precisati, senza porsi troppo il problema del devastante impatto di tale obbligo sul nostro ordinamento.

E ancora, dato che l'obbligo in questione veniva a porsi in conflitto quantomeno con un principio supremo della nostra Costituzione nelle sue diverse articolazioni, la saga sembra aver confermato che bene ha fatto la Corte costituzionale a (non *opporre*, ma) *esporre* i controlimiti, così da indurre i giudici di Lussemburgo a correggere il tiro nella sentenza *M.A.S.* per rispettare la nostra identità costituzionale.

Tuttavia, se il "dialogo" non è certo mancato ed è servito a evitare gli effetti perversi di una disapplicazione della prescrizione nelle intenzioni dei giudici di Lussemburgo destinata ad operare addirittura in relazione a casi concernenti illeciti penali realizzati prima della sentenza *Taricco*[117], il "tono" utilizzato dal nostro giudice delle leggi avrebbe potuto, a mio giudizio, essere diverso; così come diversi avrebbero potuto essere alcuni passaggi dell'ordinanza n. 24 del 2017 e della sentenza n. 115 del 2018 caratterizzati da una "attitudine oppositiva e non cooperativa"[118] e, sempre a mio giudizio, marcatamente connotati in chiave sovranista.

[112] In riferimento agli artt. 3, 11, 24, 25 comma 2, 27 comma 3 e 101 comma 2, Cost.

[113] Come conseguenza dell'inapplicabilità della "regola *Taricco*", la Corte costituzionale "dichiara non fondate le questioni di legittimità costituzionale dell'art. 2 della legge 2 agosto 2008, n. 130 (Ratifica ed esecuzione del Trattato di Lisbona che modifica il Trattato sull'Unione europea e il Trattato che istituisce la Comunità europea e alcuni atti connessi, con atto finale, protocolli e dichiarazioni, fatto a Lisbona il 13 dicembre 2007), sollevate dalla Corte di cassazione, in riferimento agli artt. 3, 11, 24, 25, secondo comma, 27, terzo comma, e 101, secondo comma, della Costituzione, e dalla Corte d'appello di Milano, in riferimento all'art. 25, secondo comma, Cost., con le ordinanze indicate in epigrafe".

[114] Punto 11.

[115] " (…) in quanto rispettoso dell'identità costituzionale degli Stati membri" (punto 11). Ai sensi dell'art. 4, secondo comma, TUE, infatti, "l'Unione rispetta l'uguaglianza degli Stati membri davanti ai trattati e la loro identità nazionale insita nella loro struttura fondamentale, politica e costituzionale (…)".

[116] Cfr., esemplificativamente, Gallo (2018), p. 885 ss.

[117] In effetti, indipendentemente dalla natura sostanziale o processuale della prescrizione, è evidente che consentire la retroattività degli effetti sfavorevoli per il reo derivanti dalla disapplicazione dei limiti temporali della prescrizione potrebbe irrimediabilmente penalizzare ogni legittima strategia difensiva tesa a rinunciare ai benefici dei riti alternativi per lucrare una imminente prescrizione. Al riguardo cfr., anche in relazione al contrasto della "regola *Taricco*" col principio di legalità penale previsto dall'art. 7 CEDU e 49 CDFUE, Bernardi (2017c), p. 58 s.

[118] Così, con specifico riferimento alla sent. 115 del 2018, Amalfitano, Pollicino (2018).

La Corte costituzionale si è infatti dimostrata inflessibile nello stigmatizzare i cedimenti palesati dalla Corte di giustizia rispetto al corollario legalista della determinatezza, ma ha mostrato questa inflessibilità solo con i giudici europei, data la sua tradizionale tendenza a chiudere un occhio sulle carenze di chiarezza e precisione delle norme penali varate dal legislatore italiano[119].

Lo stesso dicasi per quanto concerne l'atteggiamento di chiusura mostrato in occasione del caso *Taricco* dalla Corte costituzionale rispetto a ogni eventuale attribuzione di profili processuali alla disciplina italiana della prescrizione. E, invero, la costituzionalizzazione della natura sostanziale dalla prescrizione operata dalla succitata sentenza 115/2018[120] appare espressiva di un irrigidimento indotto o almeno favorito dalla volontà di "prevalere" sulla Corte di giustizia più ancora che da convinzioni di natura dogmatica. Questo sospetto parrebbe confermato dalla "flessibilizzazione dello "statuto costituzionale" della prescrizione"[121] successivamente effettuata dalla Corte costituzionale nella sentenza n. 278 del 2020; sentenza nella quale il nostro giudice delle leggi, esauritasi la tenzone coi giudici di Lussemburgo, "sembra riconoscere un fondamento (anche) processuale alla prescrizione, pur mantenendone ferma la qualificazione formale in termini sostanzialistici"[122].

In definitiva, sembra possibile affermare che nel caso *Taricco* il "dialogo" tra le Corti si sia trasformato in un vero e proprio "duello"[123] o quantomeno in una "lotta" nella quale le due protagoniste, al pari dei lottatori di sumo, hanno dato vita a uno scontro incruento ma accanito[124] in merito alle reciproche competenze[125]; scontro finalizzato al riconoscimento del primato assoluto del diritto UE ovvero dell'identità costituzionale nazionale, e dunque alla verifica di chi fra le due contendenti fosse legittimata ad avere l' "ultima parola"; uno scontro che ha visto la Corte costituzionale prevalere, e nella sentenza 115 del 2018 persino maramaldeggiare, evidenziando la carenza di "cultura penalistica" dei giudici di Lussemburgo e arrogandosi prerogative destinate a svilire il ruolo della Corte di giustizia e della sua giurisprudenza[126]. Al contempo, tuttavia, la Corte costituzionale ha accuratamente evitato di prendere in considerazione il problema dell'impunità che da tempo preoccupa l'Unione europea[127] e dunque ha ignorato certe criticità del nostro sistema penale: un sistema nel quale i procedimenti che si concludono con una dichiarazione di avvenuta prescrizione, lungi dall'essere l'eccezione, divengono, quantomeno in relazione a certi tipi di reato, quasi la regola[128]; un sistema penale pertanto caratterizzato, specie in taluni settori ricchi di ricadute in sede eurounitaria, da un tasso di ineffettività talmente elevato[129] da indurre la Corte di giustizia a una reazione scomposta rivelatasi, come si è visto, infelicissima.

Ora, è proprio questo atteggiamento sovranista della Corte costituzionale a rendere non

[119] Cfr. Donini (2018), p. 23: "La Corte (e se non la Consulta, la Corte di Cassazione) ha salvato – e male ha fatto – le norme più indeterminate, dal "vecchio" art. 323 c.p. all'ingente quantità degli stupefacenti, al disastro innominato, a tutti i casi delle aggravanti indefinite. Che ora la Corte rinneghi (solo implicitamente, si comprende) decenni di decisioni di inammissibilità per essere le norme reinterpretabili in chiave più tassativa, non ci delude. Ne siamo lieti" (par. 10). Nel prosieguo del suo scritto l'a. dimostra peraltro di dubitare del fatto che l'intransigente in tema di determinatazza palesata dalla Corte costituzionale in occasione del caso *Taricco* sia destinata a perdurare: "Il fatto è che non crediamo davvero che si pensi di mettere in discussione la prassi e la teoria per cui è solo la "norma" a risultare indeterminata, non la "disposizione" in sé, salvo casi appunto più estremi. Pensiamo invece che si volesse – giustamente – contrastare il "governo dei giudici di Lussemburgo" e che per farlo si sia scelta una strada non ben percorribile nella normalità dei casi".

[120] Cfr., per tutti, Cupelli (2018b).

[121] Per usare le parole di Siracusa (2023), p. 225. Cfr. altresì, tra gli altri, Martire, Pistone (2021), in particolare p. 176.

[122] Siracusa (2023), p. 225. A giudizio dell'a. "Soltanto in apparenza dunque la decisione in commento si uniforma pienamente alla pronuncia sul caso Taricco. Di fatto, la valorizzazione delle istanze di carattere processuale che concorrono a determinare la durata "non-tabellare" della prescrizione costituisce un'implicita presa d'atto dell'insostenibilità a lungo termine di una lettura in senso forte della natura sostanziale della prescrizione, che sia in grado di sbarrare la strada alla considerazione degli indiscutibili riflessi processuali dell'istituto. Più in generale poi, i punti citati ampliano sul piano dogmatico la ratio costituzionale della prescrizione del reato a profili di natura processuale" (p. 235).

[123] Termine, questo, non a caso ricorrente tra i commentatori del caso in questione. Cfr., ad esempio, Faraguna (2017), p. 532; Venturi (2022).

[124] A dire il vero, non è la prima volta che rispetto al "dialogo tra le Corti" ricorro alla metafora dei "lottatori giapponesi di sumo": cfr. Bernardi (2016) p. 18 e p. 90. Ma è un fatto che questa metafora si attaglia perfettamente a quanto accaduto nell'ambito del caso *Taricco*.

[125] Sul punto cfr., puntualmente, Cannizzaro (2017), p. 57.

[126] Emblematica, in tal senso, la "pretesa della Consulta di stabilire in modo autentico ed insindacabile se le norme sovranazionali siano, o no, 'determinate'": Ruggeri (2018), p. 498 s., in particolare nt. 36. Sul punto cfr. altresì, per tutti, Amalfitano (2019), p. 8 ss.; Amalfitano, Pollicino (2018).

[127] Cfr., fondamentalmente, Marin, Montaldo (2020).

[128] Cfr., ad esempio, i dati numerici e statistici riportati in Camera dei Deputati, *La riforma della prescrizione nella legge n. 103 del 2017*, in *temi.camera.it*.

[129] In un interessante e provocatorio scritto caratterizzato da un forte scetticismo in merito a un "dialogo tra le Corti" che, a giudizio dell'a., "non c'è mai stato", ricorda come il caso *Taricco* concerna "una lesione degli interessi finanziari dell'Unione, grave, protratta e forse destinata a perpetuarsi" Gradoni (2017).

del tutto soddisfacente l'uso da essa fatto del rinvio pregiudiziale di interpretazione alla Corte di giustizia: perché il "dialogo tra le Corti" dovrebbe servire non solo a impedire indebite "invasioni di campo" della Corte di giustizia, ma anche a prendere coscienza delle storture dell'ordinamento nazionale in prospettiva europea e a porvi rimedio; anche se non necessariamente ricorrendo alle cure suggerite dai giudici del Kirchberg[130].

Eppure, nonostante quanto appena detto, è possibile concordare con quella dottrina – non solo costituzionalistica[131] e penalistica[132], ma anche europeistica[133] – per la quale il confronto tra Corte costituzionale e Corte di giustizia occasionato dal caso *Taricco* sia risultato "proficuo".

Al riguardo, è innanzitutto auspicabile che la stagione del duro confronto tra le due Corti – testimoniata, oltre che dalla ordinanza n. 24 del 2017 e della sentenza n. 115 del 2018, anche dalla sentenza n. 269 del 2017 della Corte costituzionale sul tema della "doppia pregiudizialità" – sia servita, per così dire, a oliare il meccanismo del rinvio pregiudiziale da parte della Corte costituzionale, caratterizzato all'evidenza da significative peculiarità[134] che rendono tale meccanismo particolarmente esposto a tensioni da stemperare piuttosto che esacerbare[135]. Positivi indizi in tal senso sembrerebbero venire sia dalle ordinanze di rinvio n. 117 del 2019 e n. 182 del 2020, nelle quali la Consulta sembra essersi orientata a fare un uso del rinvio pregiudiziale meno antagonistico (tanto da indurre a ritenere tali provvedimenti dei "gesti di riconciliazione"[136] nei confronti della Corte di giustizia), sia dalle ordinanze di rinvio n. 216 e 217 del 2021, non a caso considerate alla stregua di "un calumet della pace" porto alla Corte di Giustizia da una Corte costituzionale peraltro ormai attribuitasi il ruolo di "arbitro degli equilibri dell'ordinamento multilivello"[137].

Vi è poi un'altra e più specifica ragione per considerare proficuo il dibattito occasionato dal caso *Taricco*. È infatti difficilmente confutabile che il caso in questione abbia portato all'attenzione generale il tema della prescrizione, evidenziando la necessità di una complessiva rivisitazione della sua disciplina. Comunque sia, è un fatto che durante e dopo la saga Taricco ci sono state ben tre leggi di riforma della prescrizione, e precisamente: la legge n. 103 del 2017, volta ad ampliare i periodi di sospensione e interruzione del corso della prescrizione ; la l. 9 gennaio 2019, n. 3, "c.d. legge Spazzacorrotti" entrata in vigore dall'inizio del 2020, che ha previsto il blocco della prescrizione dopo la pronuncia della sentenza di primo grado (sia di assoluzione che di condanna) o del decreto penale di condanna; la legge 27 settembre 2021, n. 134, la quale ha introdotto alcune modifiche alla disciplina della prescrizione in sostanziale continuità con il regime inaugurato con la l. 3/2019.

A questo punto viene spontaneo domandarsi se, considerate nel loro complesso, queste leggi vadano nel senso di innalzare l'effettività del sistema, e dunque in qualche misura recepiscano le preoccupazioni che avevano indotto la Corte di giustizia a concepire quella "regola *Taricco*" poi massacrata dal nostro giudice delle leggi. Almeno in prima battuta verrebbe fatto di rispondere in senso positivo, ove si guardi al processo di riduzione dell'area della prescrizione attuato con queste leggi. Non va però dimenticato che la succitata l. 134 del 2021 ha anche introdotto il nuovo istituto dell'improcedibilità: istituto in base al quale, trascorso un certo lasso di tempo, il processo viene interrotto e cessa di esistere, precludendo al giudice ogni esame del merito della causa, e imponendogli di dichiarare il non doversi procedere[138]. Di qui il rischio che, ove non si riescano a comprimere i tempi processuali, l'improcedibilità diventi

[130] In merito a quanto ci si sarebbe potuti aspettare dalla Corte costituzionale nell'ambito del caso *Taricco* cfr., ad esempio, Bin (2016). Secondo l'a. "Nel merito la Corte di giustizia ha però ragione. La disciplina italiana della prescrizione in materia penale è inaccettabile e favorisce in modo intollerabile chi compie frodi finanziarie. Questo è l'argomento più forte in mano ai fautori della sent. Taricco. Nello stesso giudizio in cui la Corte costituzionale potrebbe ridimensionare la sent. Taricco per l'inaccettabile estensione dell'"effetto diretto" e dei conseguenti obblighi dei giudici nazionali, essa potrebbe però accoglierne le giuste censure della legislazione italiana. Lo strumento c'è: la Corte potrebbe sollevare davanti a se stessa la questione di legittimità della legge italiana e risolverla con una sentenza di accoglimento. La "non manifesta infondatezza" della questione è in re ipsa, ben motivata dalla stessa sentenza Taricco: ad eventuali parametri sostanziali (artt. 3, 11, 25.2, 27.3, 101.2 ecc.) si può quindi aggiungere anche la violazione degli artt. 11 e 117.1 Cost., avendo la Corte di giustizia abbondantemente motivato a proposito della violazione da parte della legge italiana degli obblighi fissati dal diritto UE".

[131] Cfr., in una prospettiva marcatamente "nazionalista", Luciani (2017), p. 63 ss.; Id. (2017b), p. 479 ss.

[132] Cfr., esemplificativamente e all'interno di una vastissima bibliografia, Cupelli (2018).

[133] Cfr., per tutti, Amalfitano, Aranci, (2022), p. 7.

[134] In merito alle quali cfr., ad esempio, Passaglia (2010), in particolare p. 27 ss.

[135] Significativa, al riguardo, la tendenza a considerare i controlimiti non tanto come muri, come argini capaci di opporsi alle pretese del diritto UE di snaturare i sistemi costituzionali nazionali, quanto snodi (o – se si preferisce – cerniere, ponti), quanto insomma strumenti di dialogo tra gli ordinamenti nazionali e l'ordinamento europeo. In argomento cfr., ad esempio, Palazzo (2017), p. 277 ss.

[136] Venturi (2022).

[137] Ivi.

[138] Salvo che l'imputato rinunci a tale opportunità.

una nuova via capace di fare strame dei requisiti di efficacia e dissuasività della risposta sanzionatoria pretesi dall'Unione in relazione ai reati di rilievo UE. Proprio per questo un recente documento della Commissione europea manifesta preoccupazione per l'introduzione in Italia del suddetto istituto[139].

In definitiva, si può concludere nel senso della persistente problematicità del dialogo tra giudici nazionali e giudici europei quando i rinvii pregiudiziali sollevano questioni relative a contrasti tra il diritto interno e il diritto UE dovuti a problemi strutturali dell'ordinamento nazionale; problemi rispetto ai quali la Corte di giustizia – come dimostrato dal caso *Taricco* e da altri più recenti e ancor più eclatanti casi[140] – risulta indotta a suggerire in via interpretativa soluzioni molto radicali, non di rado in più o meno esplicita tensione coi principi supremi e diritti fondamentali della Costituzione nazionale.

4.3.2. *Il recentissimo caso* NE.

Il secondo e ultimo caso relativo a rinvii pregiudiziali cui hanno fatto seguito sentenze interpretative molto problematiche in ragione del loro rapporto di tensione coi principi supremi previsti dalle Costituzioni nazionali concerne il caso *NE*. Si tratta di un caso abbastanza recente, innescato da due rinvii pregiudiziali effettuati (non da un giudice italiano, ma) da un tribunale amministrativo regionale austriaco giustamente preoccupato del fatto che le sanzioni applicabili al caso in giudizio sulla base della normativa austriaca attuativa di una direttiva UE potessero eccedere il limite imposto dal principio europeo di proporzionalità inscritto nella suddetta direttiva così come in moltissime altre fonti di diritto derivato e financo nel terzo comma dell'art. 49 CDFUE[141]. Al primo di questi due rinvii pregiudiziali la Corte di giustizia rispondeva con una ordinanza[142] che confermava i sospetti del giudice del rinvio, in quanto dichiarava la non conformità al principio di proporzionalità inscritto nella direttiva della disciplina sanzionatoria prevista dalle norme nazionali d'attuazione[143]. Successivamente – preso

[139] Commissione europea – Documento di lavoro dei servizi della Commissione – *Relazione sullo Stato di diritto 2022 Capitolo sulla situazione dello Stato di diritto in Italia* che accompagna il documento *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – Relazione sullo Stato di diritto 2022 La situazione dello Stato di diritto nell'Unione europea*, 13 luglio 2022, in *ec.europa.eu:* "Le nuove disposizioni in materia di giustizia penale mirano a migliorare l'efficienza e necessitano di un attento monitoraggio per garantire il mantenimento dell'efficacia del sistema giudiziario. La riforma per l'efficienza del processo penale [si allude alla l. 27 settembre 2021, n. 134, la quale ha introdotto l'articolo 344 *bis* del Codice di procedura penale con effetto dal 19 ottobre 2021] comprende anche alcune disposizioni applicabili ai reati commessi dopo il 1º gennaio 2020, con la fissazione di termini massimi per la conclusione dei procedimenti dinanzi alla Corte d'appello e alla Corte suprema di cassazione, pena l'improcedibilità. Per problemi di efficienza soprattutto a livello delle Corti d'appello, le nuove misure rischiano di incidere negativamente sui processi penali e in particolare su quelli in corso, che potrebbero essere automaticamente resi improcedibili. Sebbene siano previste eccezioni e siano in vigore norme temporanee, l'efficacia del sistema giudiziario penale richiede un attento monitoraggio a livello nazionale per garantire un giusto equilibrio tra l'introduzione delle nuove disposizioni e i diritti di difesa, i diritti delle vittime e l'interesse pubblico all'efficienza del procedimento penale".

[140] Cfr., in particolare, Corte di giustizia, Grande Sezione, sent. 21 dicembre 2021, domanda di pronuncia pregiudiziale proposta dall'*Înalta Curte de Casație și Justiție, Tribunalul Bihor* — Romania, cause riunite C-357/19, C-379/19, C-547/19, C-811/19 e C-840/19. La sentenza in questione affronta la questione relativa al potere di disapplicare le decisioni della Corte costituzionale (nel caso di specie, la *Curtea Constituțională* romena) non conformi al diritto dell'Unione. Al riguardo, la Corte di giustizia è giunta ad affermare che "Il principio del primato del diritto dell'Unione deve essere interpretato nel senso che osta a una normativa o a una prassi nazionale ai sensi della quale i giudici ordinari nazionali sono vincolati dalle decisioni della corte costituzionale nazionale e non possono, a pena di commettere un illecito disciplinare, disapplicare, di propria iniziativa, la giurisprudenza risultante da tali decisioni, laddove ritengano, alla luce di una sentenza della Corte, che tale giurisprudenza sia contraria all'articolo 19, paragrafo 1, secondo comma, TUE, all'articolo 325, paragrafo 1, TFUE o alla decisione 2006/928".

[141] In base al quale "Le pene inflitte non devono essere sproporzionate rispetto al reato".

[142] Ord. 19 dicembre 2019, causa C-645/18, *NE/Bezirkshauptmannschaft Hartberg-Fürstenfeld*.

[143] La Corte ha dichiarato che "l'articolo 20 della direttiva 2014/67 (…) deve essere interpretato nel senso che esso osta a una normativa nazionale che prevede, in caso di inadempimento di obblighi in materia di diritto del lavoro relativi alla dichiarazione di lavoratori e alla conservazione di documenti salariali, l'imposizione di sanzioni pecuniarie di elevato importo che: non possono essere inferiori a un importo predefinito; sono imposte cumulativamente per ogni lavoratore interessato e senza massimale; alle quali si aggiunge un contributo alle spese del procedimento pari al 20% dell'importo delle sanzioni pecuniarie in caso di rigetto del ricorso proposto avverso la decisione che le impone". Merita di essere sottolineato che l'ordinanza in questione ricalca in larga misura un altro provvedimento della Corte di giustizia immediatamente precedente. Si allude alla sent. della Sesta Sezione 2 settembre 2019, cause riunite C-64/18, C-140/18, C-146/18 e C-148/18, *Maksimovic e altri*, la quale ha dichiarato contraria al diritto UE sanzioni pecuniarie del tutto analoghe a quelle di cui alla sent. *NE* e adottate per il medesimo tipo di violazioni. Peraltro, nella sentenza *Maksimovic e altri* – innescata da una serie di rinvii pregiudiziali relativi all'interpretazione dell'articolo 56 TFUE, degli articoli 47 e 49 CDFUE, della direttiva 96/71/CE del 16 dicembre 1996, relativa al distacco dei lavoratori nell'ambito di una prestazione di servizi e della direttiva 2014/67/UE del 15 maggio 2014 di analogo oggetto – la non conformità di tali sanzioni al diritto UE veniva fatta discendere dalla loro incompatibilità (non con il principio di proporzione di cui al terzo comma dell'art. 49 CDFUE, ma) con l'art. 56 TFUE sul divieto di restrizioni alla libera prestazione dei servizi all'interno dell'Unione. Infatti, a giudizio della Corte di giustizia, "l'effettiva attuazione degli obblighi la cui violazione è sanzionata da una normativa siffatta potrebbe

atto che il legislatore austriaco non aveva ancora modificato le norme nazionali *sub iudice*, che nel tentativo di ovviare per via giurisprudenziale a questa sproporzione i giudici austriaci di grado superiore avevano adottato provvedimenti tra loro contrastanti e che era assai dubbia la possibilità per i giudici nazionali di applicare tali norme conformemente alla direttiva UE – il giudice del rinvio effettuava un secondo rinvio pregiudiziale nel quale domandava alla Corte di giustizia se e come le suddette norme potessero trovare una applicazione che risultasse rispettosa del diritto UE[144].

Anche se il caso in esame non riguarda in prima battuta l'Italia, esso appare di estremo interesse in quanto tocca problematiche a carattere generalissimo ricche di implicazioni sul nostro sistema. La peculiarità di questo caso è che, per una volta, i problemi di costituzionalità posti dalla sentenza della Corte di giustizia che qui ci si accinge a illustrare per sommi capi discendono non dai suoi effetti *in malam partem*, ma da quelli *in bonam partem*.

4.3.2.1. *La sentenza* NE *e la problematica incidenza del principio europeo di proporzione sulle sanzioni applicabili nei Paesi membri.*

Tutto ciò premesso veniamo dunque alla sentenza *NE*[145], che rappresenta, uno degli ultimi capitoli della lunga storia concernente l'incidenza dei principi di diritto UE – e in particolare del principio di proporzionalità – sulle risposte punitive (a carattere sia penale sia amministrativo sia financo civile)[146] previste dal diritto interno per le violazioni di norme attuative del diritto UE.

In questa sentenza la Grande camera chiede al giudice interno di disapplicare in parte la sanzione assai severa (54.000 euro) irrogata a *NE* dall'amministrazione austriaca in base all'altrettanto severa normativa nazionale attuativa della direttiva 2014/67/UE[147] *relativa al distacco dei lavoratori nell'ambito di una prestazione di servizi*. La legislazione austriaca prevede infatti, in caso di "inosservanza di obblighi connessi alla dichiarazione di lavoratori e alla conservazione della documentazione salariale"[148], sanzioni pecuniarie con un minimo edittale elevato e per di più proporzionali al numero di lavoratori coinvolti in tali violazioni[149]. Dette sanzioni sono pertanto destinate a raggiungere, in certi casi, importi molto elevati e comunque eccessivi, mentre l'art. 20 della direttiva stabilisce – al pari di quanto previsto in moltissimi altri atti di diritto derivato – che le misure punitive applicabili in caso di violazione delle disposizioni nazionali adottate in attuazione della direttiva devono essere, oltre che "effettive e dissuasive", anche "proporzionate". Laddove, in base alla giurisprudenza della Corte di giustizia, possono dirsi "proporzionate" ai sensi del suddetto articolo[150] – così come ai sensi dell'art. 49, paragrafo 3 CDFUE che la sentenza *NE* ricorda implicitamente richiamato anch'esso dall'art. 20 della direttiva[151] – solo le sanzioni non superiori allo stretto necessario[152].

essere assicurata da misure meno restrittive, quali la fissazione di ammende con un importo meno elevato o l'introduzione di un massimale per tali sanzioni, senza necessariamente accompagnare queste ultime a pene detentive sostitutive" (punto 47). " Pertanto, si deve ritenere che una normativa come quella di cui al procedimento principale ecceda i limiti di quanto è necessario per garantire il rispetto degli obblighi in materia di diritto del lavoro relativi al conseguimento di autorizzazione amministrativa e alla conservazione della documentazione salariale e per assicurare il conseguimento degli obiettivi perseguiti" (punto 48). Va rilevato che né l'ordinanza 19 dicembre 2019, *NE* né la sentenza *Maksimovic e altri* hanno specificato quali conseguenze discendessero dalla contrarietà al diritto UE delle sanzioni *sub iudice.*

[144] Cfr., per una più articolata rassegna delle prime fasi del caso *NE,* cfr. le *Conclusioni dell'Avvocato generale Michal Bobek* presentate il 23 settembre 2021 nell'ambito della Causa C-205/20, *NE*, c. *Bezirkshauptmannschaft Hartberg-Fürstenfeld*, cit. Cfr. altresì, per tutti, Tsolka, (2022), p. 131 ss.; F. Viganò (2022), p. 6 ss.

[145] Corte di giustizia, Grande Sezione, sent. 8 marzo 2022, causa C-205/20, *NE.*

[146] Alla luce del concetto di "materia penale" accolto dalla Corte di giustizia così come dalla Corte EDU. Cfr., *supra, sub* par. 1, nt. 1. Per un'analoga estensione alle sanzioni amministrative del principio costituzionale di proporzionalità cfr. sent. n. 112 del 2019 nonché, da ultimo, sent. n. 46 del 2023.

[147] Per la precisione, direttiva 2014/67/UE del 15 maggio 2014, *concernente l'applicazione della direttiva 96/71/CE relativa al distacco dei lavoratori nell'ambito di una prestazione di servizi e recante modifica del regolamento (UE) n. 1024/2012 relativo alla cooperazione amministrativa attraverso il sistema di informazione del mercato interno («regolamento IMI»).*

[148] Cfr. Sent. *NE*, cit., punto 49.

[149] Per una meticolosa ricostruzione della disciplina sanzionatoria austriaca prevista in relazione alle suddette violazioni cfr. sent. *NE,* cit., punti 4-7.

[150] Che rinvia immediatamente al principio generale di proporzionalità UE (cfr. sent. *NE*, cit., punto 31, prima parte).

[151] Sent. *NE*, cit., punto 31, seconda parte.

[152] Merita di essere ricordato che nel diritto UE il principio di proporzionalità si articola nei tre sottoprincipi di idoneità, necessità e proporzionalità in senso stretto: cfr., per tutti, Scaccia (2006), p. 249 ss.; Cognetti (2011), cap. IV. Ora, è appunto al secondo di tali sottoprincipi che va ricondotto il principio di sussidiarietà/*extrema ratio* della sanzione penale: cfr., con specifico riferimento al diritto UE

La Corte di giustizia motiva la sua presa di posizione affermando che "il principio del primato del diritto dell'Unione deve essere interpretato nel senso che esso impone alle autorità nazionali l'obbligo di disapplicare una normativa nazionale, parte della quale è contraria al requisito di proporzionalità delle sanzioni (…), nei soli limiti necessari per consentire l'irrogazione di sanzioni proporzionate"[153]. Conformemente al principio di proporzionalità UE e al suo primato sul diritto interno, la Corte chiede dunque che il giudice nazionale prescinda dai limiti minimi di pena previsti in relazione alle violazioni accertate, così da poter irrogare una sanzione inferiore a quella, sproporzionata per eccesso, applicabile in base alla legge austriaca.

Secondo la Corte di giustizia, questa riconfigurazione della sanzione da parte del giudice sarebbe consentita in considerazione del fatto che:

il principio di proporzionalità è "un principio generale del diritto dell'Unione", che "si impone agli Stati membri nell'attuazione di tale diritto, anche in assenza di armonizzazione della normativa dell'Unione nel settore delle sanzioni applicabili"[154];

"Il requisito di proporzionalità delle sanzioni previsto da detta disposizione [vale a dire dall'art. 20 della direttiva 2014/67] è di carattere incondizionato"[155], così come "presenta carattere imperativo"[156] il principio di proporzionalità di cui all'art. 49, paragrafo terzo, CDFUE;

all'opposto di quanto in precedenza affermato nella sentenza *Link Logistic*[157] (ma, come vedremo, in tendenziale sintonia con quanto affermato dalla risalente giurisprudenza della Corte di giustizia relativa al principio *non scritto* di proporzionalità sanzionatoria) – il principio *scritto* di proporzionalità UE, anche ove contenuto in una direttiva, è dotato di effetto diretto[158] in quanto (non solo, come sopra ricordato, incondizionato, ma anche) preciso, consistendo "nel divieto, enunciato in termini generali e inequivocabili (…) di prevedere sanzioni sproporzionate"[159];

"il principio di irretroattività della legge penale, che è inerente al principio di legalità dei reati e delle pene", non risulta violato dall'applicazione di una pena inferiore al minimo legale, dato che tale principio "non osta (…) all'applicazione (…) di pene più lievi"[160];

"anche a voler supporre che la circostanza che un'autorità nazionale debba disapplicare una parte della medesima normativa nazionale sia tale da generare una certa ambiguità quanto alle norme giuridiche applicabili a detti illeciti, tale circostanza non lede i principi della certezza del diritto e della legalità dei reati e delle pene"[161];

per finire, "poiché il requisito di proporzionalità previsto all'articolo 20 della direttiva 2014/67 implica una limitazione delle sanzioni, che deve essere rispettata da tutte le autorità nazionali incaricate di applicare tale requisito nell'ambito delle loro competenze, consentendo nel contempo a dette autorità di irrogare sanzioni diverse in funzione della gravità dell'illecito sulla base della normativa nazionale applicabile, non può ritenersi che un siffatto requisito violi il principio della parità di trattamento"[162] di cui all'art. 20 CDFUE[163].

È appena il caso di ricordare che la soluzione proposta dalla Corte di giustizia nella sentenza *NE* (in base alla quale, come detto, occorre "disapplicare le disposizioni nazionali nei soli limiti in cui esse ostano all'irrogazione di sanzioni proporzionate"[164]) risulta in sintonia con quanto già posto in essere da una parte dei giudici austriaci dopo la succitata ordinanza del 19 dicembre 2019 della medesima Corte. Mentre infatti alcuni giudici si erano conformati al

dopo il Trattato di Lisbona, Portero Henares (2010), p. 255 ss., e ivi ulteriori riferimenti bibliografici.

[153] Sent. *NE*, cit., punto 57.

[154] Sent. *NE*, cit., punto 31.

[155] Sent. *NE*, cit., punto 22.

[156] Sent. *NE*, cit., punto 31.

[157] Nella quale ¬– come già accennato in precedenza – la Corte sosteneva contraddittoriamente "da un lato, che non si può ritenere che il requisito di proporzionalità (…) possieda effetto diretto e, dall'altro lato, che il giudice nazionale, in virtù del proprio obbligo di adottare tutte le misure appropriate, di carattere generale o particolare, per garantire il rispetto di tale disposizione, deve interpretare il diritto nazionale conformemente alla disposizione medesima, o, qualora tale interpretazione conforme non risulti possibile, disapplicare ogni disposizione nazionale laddove, nelle circostanze del caso di specie, l'applicazione di tale disposizione conduca ad un risultato contrario al diritto dell'Unione" (punto 62).

[158] Sent. *NE*, cit., punto 32.

[159] Sent. *NE*, cit., punto 27. A sua volta, tale divieto tende a configurarsi come un diritto soggettivo "a non subire sanzioni sproporzionate". Cfr., con specifico riferimento al principio di proporzione della pena di cui all'art. 49 CDFUE, *Conclusioni dell'Avvocato generale Michal Bobek*, cit., punto 48.

[160] Sent. *NE*, cit., punto 48.

[161] Sent. *NE*, cit., punto 53.

[162] Sent. *NE*, cit., punto 56.

[163] In base al quale "Tutte le persone sono uguali davanti alla legge".

[164] Sent. *NE*, cit., punto 44.

punto di vista della Corte costituzionale austriaca (la quale ha ritenuto, *tout court*, che non poteva essere applicata la vigente disciplina sanzionatoria incompatibile col diritto UE in vigore e che dunque non poteva essere inflitta alcuna sanzione in base alle disposizioni dichiarate sproporzionate dalla Corte di giustizia)[165], per adeguarsi al diritto dell'Unione la Corte suprema amministrativa austriaca aveva affermato di rinunciare a moltiplicare la pena per il numero di lavoratori coinvolti nell'illecito[166] e su questa scia una parte dei giudici amministrativi si era orientata ad applicare una pena inferiore al minimo legale, anche se con esiti assai variabili da un giudice all'altro[167].

Nonostante dunque il fatto che, in nome del primato e dell'effetto diretto del principio di proporzione delle sanzioni previsto dal diritto UE, la sentenza *NE* imponga ai giudici austriaci forme di parziale disapplicazione della sanzione già adottate da una parte della magistratura amministrativa austriaca, il tasso di "creatività" di tale soluzione ha sollevato più di una perplessità sia in Austria (in particolare, come appena ricordato, da parte della Corte costituzionale) sia in altri Paesi UE[168], inducendo taluni commentatori a contestare la lesione dei principi supremi di legalità, certezza del diritto, separazione dei poteri inscritti nelle Costituzioni nazionali.

4.3.2.2. *A monte della sentenza* NE*: l'evoluzione dei vincoli posti dal diritto UE alle scelte sanzionatorie nazionali attuative della normativa europea.*

Ancorché indubbiamente innovativa, la sentenza *NE* della Corte di giustizia non può sorprendere più di tanto. Essa sembra infatti costituire nient'altro che una tappa del lungo percorso caratterizzato dalla crescente tendenza del diritto UE a condizionare, per via sia legislativa sia giurisprudenziale, le scelte dei Paesi membri in merito alle misure punitive adottabili in sede di attuazione sanzionatoria delle fonti di diritto derivato[169].

Quanto al livello legislativo, basti qui ricordare, il succedersi di fonti UE di diritto primario (ma anche di diritto derivato) vieppiù corredate di principi e diritti dotati di ricadute in materia penale, nonché il processo evolutivo delle direttive UE. Attraverso la previsione di direttive sempre più dettagliate, e successivamente attraverso l'attribuzione all'Unione di specifiche competenze penali atte a consentire il varo di strumenti (prima convenzioni e decisioni quadro di "terzo pilastro" e poi direttive) contenenti obblighi di incriminazione, i vincoli sanzionatori posti dall'Unione a carico degli Stati UE si sono fatti sempre più stringenti. Si è passati così da direttive che si limitavano a dettare agli Stati membri i comportamenti da vietare senza nulla dire in merito alle sanzioni da essi adottabili, a direttive corredate di indicazioni sanzionatorie oltremodo vaghe[170], e quindi a direttive che circoscrivono in misura crescente la discrezionalità sanzionatoria nazionale precisando financo la natura, la tipologia ed anche, almeno in parte, i limiti edittali[171] delle misure punitive che i Paesi membri sono chiamati a comminare, così da giungere all'imposizione di modelli sanzionatori almeno parzialmente uniformi[172].

Quanto poi al livello giurisprudenziale, è sufficiente segnalare la progressiva tendenza della Corte di giustizia sia a creare per via pretoria "principi di diritto non scritto" ricchi di ricadute sulle misure punitive nazionali adottate nei settori di competenza UE[173], sia a implementare e arricchire con sempre nuovi corollari i principi/diritti UE "di diritto scritto" destinati a vinco-

[165] Cfr. Cfr., *Conclusioni dell'Avvocato generale Michal Bobek*, cit. punto 17, Per contro, ancora altri giudici "hanno continuato ad applicare sanzioni cumulative" (sent. *NE*, cit., punto 19).
[166] Cfr., *Conclusioni dell'Avvocato generale Michal Bobek*, cit. punto 17, nt. 13.
[167] Cfr., *amplius*, *Conclusioni dell'Avvocato generale Michal Bobek*, cit. punto 19.
[168] Primi fra tutti la Polonia e la Repubblica Ceca, i cui governi (come ricordato al punto 45 della sentenza *NE*) non hanno celato i loro dubbi in merito all'ammissibilità di forme siffatte di ortopedia commisurativa alla luce dei supremi principi costituzionali.
[169] Attuazione sanzionatoria concernente norme previste sia da direttive UE sia da regolamenti UE, laddove questi ultimi risultino privi di una propria disciplina punitiva.
[170] Cfr., ad esempio, la direttiva 68/151/CEE in materia di società, la quale all'art. 6 si limitava a imporre di sanzionare con "misure adeguate" taluni inadempimenti pubblicitari.
[171] In genere, attraverso la previsione della misura minima di massimo edittale.
[172] Cfr., per tutti, Bernardi (2008), p. 76 ss.; Vozza (2015), p. 16 ss., con ulteriori riferimenti bibliografici; *amplius* e fondamentalmente Satzger (2020).
[173] Cfr., *supra, sub* par. 2, nt 8.

lare in vario modo le scelte sanzionatorie nazionali in sede di attuazione del diritto UE[174], sia a riconoscere efficacia diretta ai suddetti principi/diritti, e dunque a generalizzare il ricorso al meccanismo disapplicativo da parte dei giudici nazionali in caso di contrasto della normativa interna con tali principi/diritti[175].

In ogni caso, limitandoci qui a qualche breve osservazione circoscritta al ruolo crescente del principio UE di proporzionalità delle sanzioni in ambito nazionale, merita di essere sottolineato che la risalente affermazione fatta dalla Corte di giustizia nella sentenza *Amsterdam Bulb*[176] – affermazione in base alla quale gli Stati sarebbero liberi di scegliere il tipo e la misura delle sanzioni atte ad assicurare l'esecuzione degli obblighi comunitari[177] – veniva già all'epoca integrata da tutta una serie di precisazioni volte a circoscriverne la portata. Sin dagli anni '70 del secolo scorso era infatti emersa la possibilità del diritto UE di condizionare le soluzioni punitive nazionali adottate in attuazione del diritto europeo, stante che alcuni principi di diritto inscritti nei Trattati, in ragione del loro primato ed effetto diretto sul diritto nazionale, potevano indurre a ritenere comunitariamente illegittime talune scelte sanzionatorie nazionali in quanto contrastanti, appunto, coi suddetti principi.

Così, a partire da alcuni interessanti rinvii pregiudiziali, alla luce del principio di non discriminazione (art. 7 Tr. CEE) o del principio di libera circolazione (art. 48 Tr. CEE), la Corte di giustizia era arrivata in più occasioni a ritenere incongrue per eccesso (o per difetto) le opzioni sanzionatorie interne, considerato il tipo e/o l'entità delle misure punitive previste in ambito nazionale[178].

Tuttavia, sebbene nelle sentenze della Corte di giustizia di quell'epoca la conformità al diritto comunitario della disciplina sanzionatoria statuale venisse vagliata di volta in volta essenzialmente in rapporto a specifici principi/diritti inscritti nei Trattati – a partire da quelli relativi alle quattro libertà poste a fondamento del mercato interno –, un complessivo esame della giurisprudenza della Corte di Lussemburgo in materia rendeva evidente come i giudici di Lussemburgo utilizzassero a tal fine anche e soprattutto un generale principio di proporzione delle sanzioni atto a tradursi in un vero e proprio diritto fondamentale destinato a vincolare le scelte punitive tanto del legislatore quanto dei giudici dei Paesi membri[179]. In particolare, a partire dal secondo comma dell'art. 5 (divenuto poi art. 10) Tr. CEE[180], la Corte giungeva ad affermare che in sede di attuazione del diritto comunitario gli Stati membri devono evitare qualsiasi provvedimento sanzionatorio che, per la sua sproporzione, sia tale da compromettere gli scopi del Trattato. In risposta ad alcuni rinvii pregiudiziali, la Corte precisava inoltre che la nozione di proporzionalità ricavabile da tale norma non si limitava a precludere il ricorso a misure punitive nazionali manifestamente sproporzionate, ma faceva altresì dipendere la conformità comunitaria di tali misure dalla loro necessarietà in relazione alla tutela degli interessi in gioco e a tutta una serie di ulteriori fattori. Ad esempio, la valutazione in merito alla stretta proporzionalità della misura veniva ricavata dalla natura dell'illecito[181], dalla pericolosità dell'autore[182], dalla comparazione tra le sanzioni previste per violazioni di norme attuative del diritto europeo e le sanzioni previste per violazioni di norme puramente nazionali[183].

Proseguendo nella sua politica giudiziaria di indirizzamento delle scelte punitive nazionali, la Corte di giustizia giungeva così alla fondamentale sentenza del 1989 sul *mais greco*[184] nella quale offriva una interpretazione particolarmente penetrante dell'art. 5 Tr. CE, espressa in

[174] Cfr., esemplificativamente, Bernardi, (2012), p. 15 ss.
[175] Cfr, da ultimo e per tutti, Gallo, (2022b), p. 85 ss.
[176] Sente. 2 febbraio 1977, Causa 50/76, *Amsterdam Bulb BV* (domanda di pronunzia pregiudiziale proposta dal *College van Beroep voor het Bedrijfsleven*).
[177] Addirittura, in tale sentenza la Corte di giustizia aveva affermato che l'art. 5 TCE si limitava ad attribuire agli Stati membri *la facoltà* (e non *l'obbligo*) di scegliere le sanzioni idonee a garantire l'adempimento dei doveri derivanti dagli atti delle istituzioni comunitarie.
[178] Cfr., ad esempio, sent. 26 febbraio 1975, causa 67/74, *Bonsignore*: "Dato che le deroghe alle norme relative alla libera circolazione delle persone costituiscono delle eccezioni da interpretarsi in senso restrittivo, la nozione di "comportamento personale" sta a significare che un provvedimento d'espulsione può venir adottato soltanto per minacce all'ordine pubblico ed alla pubblica sicurezza che potrebbero essere poste in atto dall'individuo nei cui confronti il procedimento stesso è stato emanato". In ogni altro caso "Le questioni sottoposte a questa Corte vanno quindi risolte nel senso che l'art. 3, nn. 1 e 2 della direttiva n. 64/221 osta all'espulsione di un cittadino di uno Stato membro".
[179] Cfr., per tutti, Biancarelli, Maidani (1984), p. 455 ss.; Mari (1981), p. 159; Bernardi, (1988), p. 195-196.
[180] In base al quale gli Stati membri "si astengono da qualsiasi misura che rischi di compromettere la realizzazione degli scopi del presente Trattati".
[181] Cfr., per tutte, Corte di giustizia, sent. 8 aprile 1976, causa 48/75 *Royer*; sentenza 15 dicembre 1976, causa 41/76, *Donckerwolcke*; sent. 14 luglio 1977, causa 8/77, *Sagulo e altri.*
[182] Cfr. Corte di giustizia, sent. 22 maggio 1980, causa 1331/79, *Regina*.
[183] Cfr. Corte di giustizia, sent. 25 febbraio 1988, causa 299/86, *Drexl.*
[184] Cfr, Corte di giustizia, sent. 21 settembre 1989, causa 68/88, *Commissione c. Grecia*.

un trinomio destinato, con minime varianti, a durare sino ad oggi; un trinomio riproposto in moltissime sentenze della Corte di giustizia e quindi travasato in un gran numero di direttive UE. Le sanzioni previste in attuazione della normativa europea devono, quindi, essere "effettive, proporzionate e dissuasive"; fermo restando che i criteri dell'effettività e della dissuasività sottendono la verifica della efficacia e sufficiente severità della sanzione, mentre il criterio della proporzionalità – quello che a noi qui interessa – sottende la verifica della stretta necessità della sanzione. A sua volta, il vaglio della proporzionalità o meno della disciplina sanzionatoria nazionale adottata in settori di competenza dell'Unione viene effettuata dalla Corte di giustizia alla luce di un catalogo di principi UE continuamente ampliato[185].

Il crescente indirizzamento svolto dalla Corte di giustizia in merito alle scelte sanzionatorie nazionali attuative del diritto UE trova una ulteriore espressione nel mutamento del tipo di risposta offerto da questa Corte ai numerosi rinvii pregiudiziali effettuati dai giudici nazionali in merito alla portata del principio UE di proporzionalità onde valutare la conformità ad esso di talune scelte punitive del legislatore interno. Attraverso un rapido percorso che l'ha portata a travalicare la sua naturale funzione di mera interprete delle norme e dei principi previsti dalle fonti UE di diritto primario e derivato[186], la Corte ha infatti abbandonato assai presto l'abitudine a fornire risposte meramente esplicative della pregnanza del principio di proporzionalità, dunque chiarificatrici della portata di tale principio sul controllo della legittimità delle risposte sanzionatorie nazionali nei settori normativi di rilievo comunitario. I giudici di Lussemburgo hanno così preso a rispondere ai quesiti dei giudici del rinvio facendo chiaramente intendere se le sanzioni utilizzate dallo Stato nel caso di specie devono ritenersi sproporzionate in quanto eccessive in rapporto ai principi UE chiamati in causa, alla natura dell'illecito, al comportamento dell'autore e ad altri eventuali indici di gravità del fatto. Al giudice nazionale è stato così sottratto tutto il (o almeno gran parte del) potere discrezionale in merito al giudizio di conformità o meno al diritto UE della disciplina sanzionatoria nazionale[187].

4.3.2.3. *Sempre a monte della sentenza* NE*: i persistenti dubbi in merito alle soluzioni per porre rimedio alle scelte sanzionatorie nazionali contrarie al principio di proporzionalità.*

Se dunque, come sin qui visto, i vincoli proporzionalistici alla discrezionalità nazionale in merito alle scelte sanzionatorie attuative del diritto UE hanno subito un vistoso processo evolutivo, non altrettanto è avvenuto in relazione alle modalità attraverso le quali gli Stati membri devono porre rimedio alle carenze di proporzionalità della sanzione ricavabili dalle sentenze della Corte di giustizia.

In linea generale, infatti, la Corte si limita da sempre ad affermare che spetta essenzialmente al legislatore e al giudice dei Paesi membri porre rimedio a una normativa nazionale in tensione col diritto UE, aggiungendo al riguardo poche altre precisazioni. Per la Corte, cioè, laddove questa tensione non possa essere risolta in via interpretativa, il legislatore nazionale è tenuto ad abrogare, modificare o sostituire la norma interna in insanabile contrasto col diritto UE[188]; mentre il giudice è tenuto a disapplicare tale norma[189], *in toto* o limitatamente alla sola parte di questa confliggente col diritto UE.

[185] Cfr., per esempio, Corte di giustizia, sent. 14 ottobre 2021, causa C-231/20, *MT*, nella quale la proporzionalità delle sanzioni è valutata con riferimento all'art. 56 TFUE concernente il divieto delle restrizioni alla libera prestazione dei servizi all'interno dell'Unione; Id., sent. 5 maggio 2022, causa C-570/20, *BV*, nella quale la proporzionalità delle sanzioni è valutata con riferimento al diritto fondamentale garantito all'articolo 50 CDFUE relativo al *diritto di non essere giudicato o punito due volte per lo stesso reato*, in combinato disposto con l'articolo 52, paragrafo 1 CDFUE.

[186] Al riguardo cfr. *supra, sub* par. 4.1, nt. 26 e 27.

[187] Cfr., ad esempio la sent. 7 luglio 1976, causa 118/75, *Watson e Belmann*, nella quale la Corte di giustizia non si è limitata a dichiarare incompatibili con il principio di libera circolazione dei lavoratori (art. 48 Tr. CEE) le sanzioni sproporzionate rispetto alla gravità delle infrazioni relative alle formalità d'ingresso, in un Paese membro, di stranieri CEE. Essa ha infatti puntualizzato che "tra le sanzioni comminate per l'inosservanza delle formalità prescritte per la notifica e per la registrazione [dell'ingresso], è indubbiamente in contrasto con la disciplina comunitaria l'espulsione di soggetti tutelati dal diritto comunitario, in quanto tale provvedimento costituisce la negazione del diritto stesso conferito e garantito dal Trattato, come la Corte stessa ha già affermato in altre occasioni".

[188] Cfr. Corte di giustizia, sent. 15 ottobre 1986, causa 168/85, *Commissione c. Repubblica italiana.*

[189] Va comunque precisato che il dovere di disapplicazione non risulta a carico solo del giudice ordinario, ma anche del giudice amministrativo e in generale delle autorità amministrative: cfr., ad esempio, Corte di giustizia, sent. 22 giugno 1989, causa 103/88, *Costanzo*; sent. 18 giugno 1991, causa 295/89, *Donà*.

Ora, in caso di contrasto tra la norma sanzionatoria nazionale e il principio UE di proporzione[190], queste scarne precisazioni lasciano aperto il campo a tutta una serie di interrogativi qui impossibili da passare compiutamente in rassegna. Basti dire che, anche solo limitatamente all'obbligo di disapplicazione posto a carico del giudice, le scarne indicazioni fornite nel corso dei decenni dalla Corte di giustizia sono ben lungi da offrire una soluzione ai problemi che si pongono[191].

Prendiamo l'ipotesi della disapplicazione parziale, solo in apparenza facilmente risolvibile disapplicando appunto una parte del compasso edittale ovvero una delle sanzioni alternativamente o cumulativamente previste dal legislatore in relazione a una data fattispecie[192]. In effetti, come risolvere il problema (che tocca tanto la proporzionalità quanto il principio di uguaglianza) derivante dal dover ricondurre casi concreti di differente disvalore (ancorché tutti rientranti nella medesima fattispecie astratta) all'interno di un compasso edittale la cui ampiezza è stata ridotta anche fortemente dall'opera di disapplicazione parziale del giudice?[193] E come stabilire il punto del compasso edittale a partire dal quale la disapplicazione deve iniziare a operare? Un esame della giurisprudenza della Corte di giustizia evidenzia come, in risposta al rinvio pregiudiziale che chiede lumi in merito alla congruenza della sanzione nazionale, essa si limiti a far capire al giudice del rinvio che la pena edittale – una parte della pena edittale – risulta sproporzionata, ma non fornisce indicazioni in merito a quale sia l'entità della sanzione da ritenersi adeguata al fatto. Al riguardo, nemmeno un complessivo esame dell'ordinamento giuridico dell'Unione risulta di significativo aiuto. Infatti "il diritto dell'UE non contiene disposizioni che definiscano un catalogo di pene per i reati di un particolare tipo, applicabili uniformemente in tutti gli Stati membri e che potrebbero servire da punto di riferimento per l'esame del rispetto"[194] del principio di proporzionalità. La considerazione che il principio di proporzione della sanzione "in materia penale" di cui al comma terzo dell'art. 49 CDFUE risulta espressivo, come in genere si ritiene, di una proporzionalità (non "ordinale"[195], ma) "cardinale"[196] (o, se si preferisce, non "relativa" ma "assoluta")[197] non sembra risolutiva per superare tale carenza di indicazioni.

Gli interrogativi aumentano nei casi in cui dalle sentenze della Corte di giustizia emerge la radicale sproporzione della sanzione prevista dal legislatore nazionale. Sproporzione rinvenibile nei casi in cui la sanzione risulti esorbitante già nel suo minimo edittale, ovvero quando, per le più diverse ragioni oggettive o soggettive, risulti tipologicamente eccessiva rispetto alla relativa violazione interferente col diritto UE, come nei casi in cui sia prevista una pena

[190] Così come in caso di contrasto tra la norma sanzionatoria nazionale e le specifiche disposizioni in tema di sanzioni contenute nella direttiva di riferimento. In tal caso, quindi, la illegittimità della norma sanzionatoria nazionale discende dal suo contrasto non con un principio UE, ma con le suddette disposizioni.

[191] Cfr., ad esempio, la sentenza 22 marzo 2017, cause riunite C-497/15 e C-497/15, *Euro-Team Kft. e Spirál-Gép Kft.*, nella quale la Corte di giustizia si limita ad affermare che la pena prevista nella normativa nazionale di attuazione di una direttiva, anche se efficace e dissuasiva, può essere sproporzionata: "l'applicazione di una sanzione di importo forfettario per qualsivoglia violazione di taluni obblighi previsti dalla legge, senza graduazione dell'importo di detta sanzione in funzione della gravità dell'infrazione, risulta sproporzionata rispetto agli obiettivi contemplati dalla normativa dell'Unione".

[192] Emblematico, al riguardo, quanto affermato in relazione a un caso siffatto dalla Corte di giustizia nella sentenza 14 luglio 1977, causa 8/77, *Sagulo e altri*: "qualora uno Stato membro non abbia adattato la propria legislazione alle esigenze derivanti in materia dal diritto comunitario, il giudice nazionale dovrà far uso della libertà di valutazione riservatagli, al fine di pervenire all'applicazione di una pena adeguata alla natura e allo scopo [delle norme comunitarie] di cui si vuole reprimere l'infrazione".

[193] A suo tempo, mi ponevo appunto questo problema allorché osservavo: "Resta il fatto che, nel caso di specie, risulteranno comunque compromessi i consueti meccanismi di individualizzazione. Infatti la necessità di quantificare inderogabilmente la pena nei pressi del suo minimo edittale comporta, all'evidenza, l'impossibilità di far emergere sul piano sanzionatorio i1 diverso disvalore dei casi concreti riconducibili alla stessa fattispecie astratta": Bernardi (1988), p. 202.

[194] Dlugosz (2017), p. 293.

[195] In base alla quale la proporzionalità della prevista per un dato reato va valutata non "in se stessa", ma attraverso un raffronto con le pene previste in relazione agli altri reati afferenti al medesimo ordinamento (sulle nozioni di proporzionalità "ordinale " e "cardinale" della pena cfr. Viganò (2021), p. 162 ss., e ivi ulteriori riferimenti bibliografici). A livello europeo, tuttavia, questo concetto di proporzionalità "per relazione" appare difficilmente utilizzabile, a causa delle diverse valutazioni date dai Paesi membri in merito sia alla gravità del medesimo illecito "in materia penale" sia alla determinazione della sanzione "non sproporzionata".

[196] In base al principio di proporzionalità "cardinale" la "non eccessività" della sanzione viene ricavata (in termini assoluti) in base alla valutazione di gravità del relativo illecito effettuata dal singolo testo di diritto derivato UE. In argomento cfr. Tsolka (2022), p. 149. Cfr. altresì Asp, (2007), p. 207; Dlugosz (2017), p. 293 ss.

[197] Per il ricorso a questo binomio cfr., in particolare, Palazzo, (2023), p. 27.

detentiva[198], o una sanzione proporzionale e/o la confisca dell'oggetto dell'illecito[199], o l'espulsione dell'autore dallo Stato[200], o ancora una sanzione pecuniaria che incide pesantemente sul reddito del condannato[201].

Due, essenzialmente, le questioni da sempre – e volutamente – lasciate senza risposta dalla Corte di giustizia: quali possano essere le sanzioni congrue da prevedere e applicare in luogo di quelle considerate sproporzionale in base al diritto UE[202]; entro quali limiti possa operare l'intervento ortopedico del giudice nazionale per porre rimedio alla originaria, radicale carenza di proporzionalità della sanzione prevista dal legislatore dei Paesi membri per un illecito che interferisce col diritto UE.

Ma ecco che in relazione a quest'ultimo quesito la Corte di giustizia, nella sentenza *NE*, ha infine rotto il suo silenzio affermando che, come già in precedenza ricordato[203], "Il principio del primato del diritto dell'Unione deve essere interpretato nel senso che esso impone alle autorità nazionali l'obbligo di disapplicare una normativa nazionale, parte della quale è contraria al requisito di proporzionalità delle sanzioni previsto all'articolo 20 della direttiva 2014/67, *nei soli limiti necessari per consentire l'irrogazione di sanzioni proporzionate*"[204]. Si tratta di un'affermazione che – giova ripeterlo – propone una soluzione ortopedica già accolta dalla Corte suprema amministrativa austriaca e da una parte dei giudici amministrativi austriaci, i quali sono intervenuti sulla sanzione prevista dal legislatore, mantenendone inalterato il tipo epperò ritoccando in vario modo il suo limite minimo così da renderla più mite; e tuttavia resta un'affermazione coraggiosa, che è sin troppo facile prevedere esposta al fuoco di sbarramento di quei Paesi che, al pari della Polonia e della Repubblica Ceca, riterranno questo potere-dovere di disapplicazione contrario ai principi di certezza del diritto, di legalità penale e di parità di trattamento[205].

Ora, è verosimile credere che anche in Italia questa soluzione potrebbe essere osteggiata alla luce non solo del principio di legalità[206], ma anche del principio di uguaglianza. Vero è

[198] Emblematico, al riguardo, il caso relativo alla normativa italiana prevista rispetto ai "cittadini di paesi terzi il cui soggiorno è irregolare" portato all'attenzione della Corte di giustizia e sfociato nella sent. 28 aprile 2011, causa C-61/11 PPU, *El Dridi*: "La direttiva del Parlamento europeo e del Consiglio 16 dicembre 2008, 2008/115/CE, recante norme e procedure comuni applicabili negli Stati membri al rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare, in particolare i suoi artt. 15 e 16, deve essere interpretata nel senso che essa osta ad una normativa di uno Stato membro, come quella in discussione nel procedimento principale, che preveda l'irrogazione della pena della reclusione al cittadino di un paese terzo il cui soggiorno sia irregolare per la sola ragione che questi, in violazione di un ordine di lasciare entro un determinato termine il territorio di tale Stato, permane in detto territorio senza giustificato motivo".

[199] Corte di giustizia, sent. 15 dicembre 1976, causa 41/76. *Donckenvolcke*: "l'eventuale inosservanza da parte dell'importatore dell'obbligo di denuncia della provenienza originaria della merce non può comportare l'applicazione di sanzioni eccessive, tenuto conto dell'indole puramente amministrativa della sanzione. Sotto questo aspetto è indubbiamente incompatibile con le disposizioni del Trattato, in quanto equivale ad un ostacolo alla libera circolazione delle merci, la confisca della merce od ogni altra sanzione pecuniaria stabilita in funzione del valore della merce stessa".

[200] Cfr., ancora, la sent. 7 luglio 1976, causa 118/75, *Watson e Belmann*, cit. Particolarmente interessante, da ultimo, Grande Sezione, sent. 22 novembre 2022, causa C-69/21, *X*: "L'articolo 5 della direttiva 2008/115/CE del Parlamento europeo e del Consiglio, del 16 dicembre 2008, recante norme e procedure comuni applicabili negli Stati membri al rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare, in combinato disposto con gli articoli 1 e 4 della Carta dei diritti fondamentali dell'Unione europea nonché con l'articolo 19, paragrafo 2, di quest'ultima, deve essere interpretato nel senso che esso osta all'adozione di una decisione di rimpatrio o di un provvedimento di allontanamento nei confronti di un cittadino di un paese terzo, il cui soggiorno nel territorio di uno Stato membro è irregolare e che è affetto da una grave malattia, allorché sussistono gravi e comprovati motivi per ritenere che, in caso di rimpatrio, l'interessato possa essere esposto, nel paese terzo verso il quale verrebbe allontanato, al rischio reale di un aumento significativo, irrimediabile e rapido del suo dolore, a causa del divieto, in tale paese, della sola terapia analgesica efficace. Uno Stato membro non può stabilire un termine fisso entro il quale siffatto aumento debba concretizzarsi affinché esso possa essere d'ostacolo a tale decisione di rimpatrio o tale misura di allontanamento".

[201] Cfr. sent. 6 ottobre 2021, causa C-35/20, *A*: "L'articolo 21, paragrafo 1, TFUE e gli articoli 4 e 36 della direttiva 2004/38, letti alla luce dell'articolo 49, paragrafo 3, della Carta dei diritti fondamentali dell'Unione europea, devono essere interpretati nel senso che ostano a un regime di sanzioni penali in base al quale uno Stato membro sanziona l'attraversamento della sua frontiera nazionale, senza essere muniti di carta d'identità o di passaporto in corso di validità, con un'ammenda che può ammontare, a titolo indicativo, al 20% del reddito mensile netto dell'autore del reato, allorché una tale ammenda non è proporzionata alla gravità di tale reato, che è considerato di lieve entità". E ciò in quanto "il rispetto da parte dei cittadini dell'Unione delle formalità connesse all'esercizio del diritto alla libera circolazione può essere garantito, in modo sufficientemente dissuasivo, mediante misure meno restrittive di quelle previste da una normativa come quella controversa nel procedimento principale, quali, in particolare, la fissazione di ammende di importo corrispondente a una percentuale meno elevata del reddito mensile e l'introduzione di un massimale per l'importo delle ammende" (punto 91).

[202] Così, ad esempio, nella sentenza menzionata alla nt. precedente la Corte di giustizia afferma la sproporzione rispetto all'illecito considerato di un'ammenda che ammonta grossomodo al 20% del reddito mensile netto dell'autore del reato, suggerendo la previsione e applicazione di una ammenda "corrispondente a una percentuale meno elevata del reddito mensile", senza peraltro specificare quale percentuale del reddito debba considerarsi proporzionata.

[203] Cfr., *supra, sub* par. 4.3.2.1, nt. 153.

[204] Sent. *NE*, cit., punto 57, corsivo non testuale.

[205] Cfr., ancora, sent. *NE*, punto 45.

[206] A questo proposito nel lontano 1988 ebbi modo di sostenere – pur soffertamente, nella consapevolezza del vuoto di tutela causato dalla disapplicazione totale della norma attuativa del diritto UE corredata di sanzioni radicalmente sproporzionale – che alla luce del principio di

infatti che la nostra Corte costituzionale è ormai adusa a rimaneggiare le sanzioni viziate di sproporzione[207], il più delle volte sostituendone i compassi edittali[208], ovvero cancellandone i limiti minimi[209], ovvero ancora comprimendo l'ambito applicativo di talune misure fortemente afflittive[210]. Ma è altresì vero che – in base allo stato attuale della giurisprudenza costituzionale italiana in tema di doppia pregiudizialità – i giudici comuni sono liberi di optare per la soluzione che privilegia il ricorso in prima battuta alla Corte di giustizia[211] anziché alla Corte costituzionale[212]. Senza contare il fatto che gli stessi giudici, ove certi della sproporzione in prospettiva UE del limite minimo della sanzione prevista per un dato illecito dal legislatore nazionale, potrebbero (anzi, sarebbero tenuti a) evitare di adire i giudici di Lussemburgo e – forti della sentenza *NE* – dovrebbero disapplicare direttamente il minimo edittale fissato dal legislatore, per poi irrogare una sanzione a loro giudizio congrua all'illecito in esame e al tipo di autore. In entrambe le ipotesi – rinvio pregiudiziale alla Corte di giustizia, disapplicazione diretta – sarebbero evidenti i rischi di quei trattamenti diseguali già riscontrati nell'esperienza austriaca successiva alla ordinanza 19 dicembre 2019, *NE* della Corte di giustizia[213].

Per altro verso, se indubbiamente la sentenza *NE* evidenzia il desiderio della Corte di giustizia di vedere ampliati i poteri dei giudici nazionali in sede di commisurazione della sanzione (così da evitare provvedimenti di pura e semplice disapplicazione incapaci di salvaguardare la necessaria effettività e dissuasività della sanzione "pretoriamente ridisegnata"), essa lascia aperta la questione relativa ai limiti incontrati dai suddetti giudici in questa loro attività pretoria. Potrebbe la Corte di giustizia, in un prossimo futuro, imporre la disapplicazione di una sanzione "tipologicamente sproporzionata" e contestualmente – in nome della lotta all'impunità – investire il giudice nazionale del potere-dovere di applicare una sanzione di tipo diverso, più mite ma pur sempre corredata dal necessario coefficiente di efficacia e dissuasività? Per quanto questo possa sembrare oltremodo difficile, non è possibile escluderlo in radice[214]. Anzi,

legalità penale non fosse praticabile la soluzione attualmente stabilita dalla Corte di giustizia nella sentenza *NE*. Scrivevo infatti: "Restano tuttavia taluni delicati problemi circa i modi di adeguamento del diritto interno alle esigenze di 'proporzione comunitaria'. *Nulla quaestio*, ovviamente, nel caso in cui le sanzioni previste dalla legislazione nazionale risultino irrimediabilmente sproporzionate, sia a causa della loro entità (quando cioè già il minimo edittale si riveli eccessivo in prospettiva comunitaria) sia a causa della loro stessa natura (quando cioè in relazione al comportamento vietato siano previste dalla legge dello Stato pene qualitativamente inadeguate). In tali ipotesi, in linea di principio, la norma interna andrebbe dal giudice nazionale disapplicata tout-court, *non potendo egli certamente irrogare una pena diversa e/o più lieve di quella prevista dalla legge*": Bernardi (1988), p. 201-202, corsivo non testuale.

[207] Con specifico riferimento alla sentenza *NE* lo ricorda Viganò (2022), p. 18.

[208] Cfr., ad esempio, sent. n. 40 del 2019, la quale "dichiara l'illegittimità costituzionale dell'art. 73, comma 1, del decreto del Presidente della Repubblica 9 ottobre 1990, n. 309 (Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza), nella parte in cui in cui prevede la pena minima edittale della reclusione nella misura di otto anni anzichè di sei anni".

[209] Cfr. ad esempio, con riferimento alle sanzioni accessorie, cfr. sent. n. 222 del 2018, la quale al punto 2 del dispositivo: "dichiara l'illegittimità costituzionale dell'art. 216, ultimo comma, del regio decreto 16 marzo 1942, n. 267 (Disciplina del fallimento, del concordato preventivo e della liquidazione coatta amministrativa), nella parte in cui dispone: 'la condanna per uno dei fatti previsti dal presente articolo importa *per la durata di dieci anni* l'inabilitazione all'esercizio di una impresa commerciale e l'incapacità per la stessa durata ad esercitare uffici direttivi presso qualsiasi impresa', anziché: 'la condanna per uno dei fatti previsti dal presente articolo importa l'inabilitazione all'esercizio di una impresa commerciale e l'incapacità ad esercitare uffici direttivi presso qualsiasi impresa *fino a dieci anni*'" (corsivo non testuale).

[210] Il riferimento è alla sent. 112 del 2019, nella quale viene dichiarata "l'illegittimità costituzionale dell'art. 187-sexies del d.lgs. n. 58 del 1998, nel testo originariamente introdotto dall'art. 9, comma 2, lettera a), della legge 18 aprile 2005, n. 62 (Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2004), *nella parte in cui prevede la confisca obbligatoria, diretta o per equivalente, del prodotto dell'illecito e dei beni utilizzati per commetterlo, e non del solo profitto*" (corsivo non testuale).

[211] "Ormai – dice la Corte – va tutto bene ciò che decide il giudice, libero d'intraprendere la via che porta dapprima alla Consulta e poi a Lussemburgo, o viceversa": così, icasticamente, A. Ruggeri (2023), p. 137.
L'a. prosegue ricordando che "In tal modo, come si vede, due questioni in tutto identiche tra di loro potrebbero risultare definite, l'una, con la tecnica della 'non applicazione' della norma interna incompatibile con la norma sovranazionale e l'altra, di contro, con quella dell'annullamento, salva in ogni caso la sempre possibile esposizione dei 'controlimiti'".

[212] Come invece, non senza buoni motivi, suggerisce Viganò (2022). L'a. infatti auspica "la stabilizzazione nell'ordinamento di un'unica soluzione, grazie a una pronuncia con effetto *erga omnes*, che evita in partenza quella situazione di incertezza e di (inevitabile) disparità di trattamento che consegue alla individuazione, da parte di ciascun singolo giudice penale, di soluzioni per risolvere l'antinomia tra diritto nazionale e diritto UE" (p. 18).

[213] Cfr., ancora, *Conclusioni dell'Avvocato generale Michal Bobek*, cit. punto 19.

[214] In fondo, l'art. 49 CDFUE tiene strettamente legati tra loro i principi di legalità penale e di proporzionalità dei reati e delle pene. Posto quindi che in tale articolo il cuore della legalità delle pene si esprime nel divieto di irrogare "una pena più grave di quella applicabile al momento in cui il reato è stato commesso" (comma 1) e che il principio di proporzione si preoccupa di evitare il ricorso a sanzioni eccessive (comma 3), non sembrano da escludersi in radice prese di posizione "disinvolte" della Corte di giustizia. Prese di posizione, cioè, destinate a sacrificare, in nome del combinato disposto "proporzionalità-dissuasività", le scelte sanzionatorie effettuate dal legislatore, consentendo (*rectius*, dettando) al giudice di applicare una misura punitiva tipologicamente più mite di quella prevista dalla legge. Anche se è più agevole ritenere che il "senso della legalità" che in qualche modo accomuna i giudici di Lussemburgo, unitamente all'eventuale timore per essi di vedersi opporre i controlimiti, possa indurli a circoscrivere anche nel futuro i poteri "pretori" dei giudici nazionali, e dunque a non azzardare di imporre forme di disapplicazione traducentisi addirittura nella trasformazione per via giurisprudenziale delle tipologie sanzionatorie originariamente

proprio la succitata sentenza M.A.S. della Corte di giustizia[215] – pur così pronta a ritrattare le pretese dei giudici di Lussemburgo a sacrificare il principio di legalità penale in nome delle esigenze di effettività delle norme penali attuative del diritto UE – potrebbe paradossalmente favorire ulteriori sentenze europee ancor più generose della sentenza *NE* nei confronti del ruolo "creativo" dei giudici nazionali. Infatti, a ben vedere, la sentenza M.A.S. ha aperto una strada che si presta a calmierare *ex post* – e dunque a rendere meno temibile – il confronto tra la Corte di giustizia e le Corti costituzionali in relazione a prese di posizione della prima analoghe a quelle assunte dalla sentenza *NE* o assumibili dai suoi eventuali, futuri e ancor più spregiudicati, epigoni. La sentenza M.A.S. ha infatti evidenziato che, nei settori normativi non oggetto di un'armonizzazione completa da parte del diritto dell'Unione, resta sempre possibile per i giudici delle leggi dei Paesi membri far prevalere le esigenze di salvaguardia dell'identità costituzionale sulle pretese della Corte di giustizia, così da indurre i giudici comuni a disattendere l'obbligo di disapplicazione da essa sancito. In questa prospettiva, nel caso *NE* proprio l'Avvocato Generale ha ricordato che in relazione alle sanzioni applicabili nei settori sottratti a un'armonizzazione completa "le autorità e i giudici nazionali dovrebbero essere liberi di applicare standard diversi (superiori) per la tutela dei diritti fondamentali. Ciò potrebbe potenzialmente includere approcci più rigorosi nei confronti del principio di legalità delle sanzioni, laddove tale requisito esista effettivamente nel diritto nazionale"[216].

Insomma, anziché vedere i possibili avanzamenti della giurisprudenza della Corte di giustizia paralizzati in partenza dal timore dei controlimiti, non sembra del tutto incongruo immaginare questi avanzamenti favoriti (almeno sul nascere) da un franco dibattito tra giudici del Kirchberg e giudici della Consulta; una "collaborazione dialettica" che secondo taluni potrebbe "ridimensionare il ricorso alla logica dei controlimiti"[217], o che quantomeno potrebbe far sì che i controlimiti eventualmente lumeggiati in sede di rinvio pregiudiziale non costituiscano più un "rigido muro di confine fra ordinamenti", ma diventino un effettivo "punto di snodo e cerniera tra UE e Stati membri"[218]. Fermo restando che i controlimiti restano saldamente nelle mani delle Corti costituzionali, le quali mantengono l'ultima parola su di essi, essendo superata o comunque minoritaria la tesi secondo cui a seguito del trattato di Lisbona sarebbe ormai la Corte di giustizia a tenere le redini dell'implementazione e del bilanciamento dei principi e diritti fondamentali espressivi dell'identità costituzionale nazionale[219]. Cosicché, in definitiva, se da un lato il concetto dell'identità nazionale (comprensivo dell'identità costituzionale) previsto all'art. 4.2 TUE sembra prestarsi a favorire, specie sul versante dei supremi principi costituzionali, la logica di un'Europa a geometria variabile atta a favorire gli avanzamenti degli approcci pragmatici e funzionalistici propri della giurisprudenza UE, dall'altro lato l'approdo raggiunto dalla sentenza *NE* appare già alquanto ardito per quei (non pochi) Paesi membri fedeli al principio di stretta legalità in materia penale[220]; tanto ardito da far ritenere non probabile che la Corte di giustizia possa in un prossimo futuro premere per un ulteriore avanzamento delle prerogative pretorie dei giudici nazionali in sede di commisurazione della pena.

5. Considerazioni conclusive.

Il processo di costruzione europea attuato da una organizzazione regionale evolutasi col tempo sino a trapassare da Comunità economica a Unione dotata di competenze nelle più diverse materie, ivi compresa quella penale, ha comportato il varo ininterrotto di norme sovranazionali (penali e non penali) destinate a incidere sugli ordinamenti giuridici dei Paesi membri. Al tradizionale problema di una attuazione sanzionatoria sufficientemente omoge-

previste dal legislatore. Cfr. tuttavia, in una diversa prospettiva, quanto osservato nel prosieguo del testo con riferimento alla sentenza *M.A.S.*

[215] Cfr., *supra, sub* par. 4.3.1.2.

[216] *Conclusioni dell'Avvocato generale Michal Bobek*, cit. punto 111.

[217] Così de Vergottini (2021), p. VIII.

[218] Queste formule antinomiche sono ormai ricorrenti. Cfr., ad esempio, Passaglia (2010), p. 27. Sul ruolo dinamico e dialettico de controlimiti cfr., altresì, per tutti, F. Palazzo (2017), p. 287.

[219] Sul tema della "europeizzazione dei controlimiti", riconducibile in particolare agli artt. 4.2 e 6.3 TUE, 67 TFUE, e 53 CDFUE cfr., per tutti, Arnold (2014), p. 149 e ss.; Ruggeri (2006). Volendo cfr. altresì, anche per ulteriori riferimenti bibliografici, A. Bernardi (2017d), p. XXV.

[220] Tant'è che dall'esame della recente giurisprudenza della Corte di giustizia una attenta dottrina è giunta alla conclusione che tale organo si sia fatto "pochi scrupoli nel picconare alle fondamenta la stessa costruzione della commisurazione edittale su un sistema di minimi e massimi sanzionatori all'interno dei quali si trovi a operare la discrezionalità del giudice": Recchia, (2022), p. 892.

nea delle norme extrapenali UE da parte di Stati caratterizzati da sistemi punitivi (penali e amministrativi) ancora alquanto diversi tra loro si è così aggiunto il problema della esatta trasposizione nei sistemi interni delle norme penali UE. Entrambi questi problemi sono poi acuiti dall'esigenza che le norme sanzionatorie nazionali varate su impulso europeo si conformino ai principi/diritti sanciti sia dalla Costituzione nazionale sia dal diritto dell'Unione; si conformino, dunque, a due categorie di principi/diritti oggetto di continue rielaborazioni giurisprudenziali espressive delle esigenze, a volte non convergenti, proprie dei rispettivi sistemi di appartenenza.

Nell'attuale fase storica la soluzione dei suddetti problemi potrebbe risultare facilitata sia dal progressivo perfezionamento dei meccanismi di collaborazione tra legislatori nazionali e legislatore europeo, sia dall'evoluzione delle forme di dialogo tra giudici nazionali e Corte di giustizia[221]. Eppure, le interazioni tra norme UE e norme nazionali rivelano difficoltà sempre maggiori a causa della loro moltiplicazione e crescente complessità; anche perché la vieppiù evidente incidenza delle fonti UE sulle norme interne – specie su quelle in "materia penale" – ha favorito, per reazione, una acuita attenzione da parte degli Stati alla salvaguardia della sovranità nazionale in tale materia così come nella materia – ad essa strettamente connessa – dei principi supremi e dei diritti fondamentali.

L'esame dei problemi posti in ambito penale (e più in generale in ambito sanzionatorio) dalle sentenze interpretative della Corte di giustizia appare prezioso per capire quanto la cosiddetta europeizzazione del diritto penale sia irta di ostacoli e per riflettere su questi ultimi in vista, perlomeno, di una loro attenuazione.

In effetti, questi ostacoli emergono con grande evidenza già in sede di interpretazione conforme delle norme interne "in materia penale" al diritto UE. Provocatoriamente, si potrebbe affermare che questo canone ermeneutico chiede davvero troppo al giudice nazionale: gli chiede, nientemeno, di verificare se la norma interna afferente alla suddetta materia possa essere interpretata in modo tale da non entrare in conflitto insanabile con una qualsivoglia delle innumerevoli e tipologicamente variegate norme UE[222], il cui contenuto e il cui ambito di applicazione (non di rado controversi) sono a loro volta oggetto di precisazioni da parte di un numero sterminato di sentenze della Corte di giustizia spesso caratterizzate da un significativo tasso di creatività. Ben può comprendersi, quindi, quanto preziosa possa essere la procedura di rinvio pregiudiziale, imprescindibile momento di apertura di un "dialogo" tra giudici nazionali e giudici europei da questi ultimi caldamente sollecitato[223]; dialogo all'esito del quale la Corte di giustizia fornisce risposte in cui la conformità o meno della norma nazionale al diritto UE viene se del caso adombrata, come già ricordato, anche sulla base di norme europee diverse da quelle inizialmente prese in considerazione del giudice del rinvio[224].

Al contempo, però, la procedura in questione pretende davvero molto dalla Corte di giustizia. Quest'ultima infatti – già lo si è accennato[225] – su questioni delicatissime sollevate dal giudice del rinvio è chiamata a fornire risposte redatte di volta in volta nelle più varie lingue dell'Unione[226], persuasivamente motivate e formulate in modo tale da poter essere apprezzate da giudici appartenenti a Paesi con culture giuridiche diverse[227], dunque abituati a "stili giudiziari" altrettanto diversi[228]. Consapevole di doversi

[221] Appare infatti indiscutibile che il dialogo tra la Corte di giustizia ed i giudici nazionali abbia favorito il processo d'integrazione europea.
[222] Basti pensare al fatto che a più riprese la Corte di giustizia ha sancito l'obbligo di interpretazione conforme persino in relazione alle norme UE di *soft law* (cfr. sent. 13 dicembre 1989, causa C-322/88, *Grimaldi*; sent. 11 settembre 2003, causa C-207/01, *Altair Chimica*, 2003), ancorché in genere queste norme siano ritenute a carattere meramente "persuasivo". In merito al problema della vincolatività di tali norme cfr., diffusamente, A. Poggi, *Soft law nell'ordinamento comunitario*, reperibile in *www.archivio.rivistaaic.it*.
[223] Al riguardo cfr., fondamentalmente, Corte di giustizia, sent. 6 ottobre 1982, causa 283/81, *Cilfit*, ove si sottolineano le "particolari difficoltà" che presenta l'interpretazione del diritto comunitario (punto 17 e 21) nonché il "rischio di divergenze di giurisprudenza all'interno della comunità" (punto 21) e si rammenta che prima di "astenersi dal sottoporre la questione [interpretativa] alla Corte risolvendola sotto la propria responsabilità" (punto 16) in ragione del fatto che "la corretta applicazione del diritto comunitario si impon[e] con tale evidenza da non lasciare adito ad alcun ragionevole dubbio sulla soluzione da dare alla questione sollevata (…) il giudice nazionale deve maturare il convincimento che la stessa evidenza si imponga anche ai giudici degli altri Stati membri ed alla Corte di giustizia" (punto 16).
[224] Cfr. *supra, sub* par. 2, nt. 13.
[225] Cfr. *supra, sub* par. 4.1.
[226] In effetti, il regime linguistico della Corte di giustizia costituisce un *unicum* che richiede ai traduttori sforzi enormi (eppure non sempre sufficienti) per dialogare al meglio con le parti processuali, oltreché per assicurare la diffusione della giurisprudenza di tale organo in tutti i Paesi membri.
[227] Cfr., in particolare, S.A. Romano (2007), p. 666 ss.
[228] Cfr., per tutti, Aa. Vv. (1988); Ranieri (1996), p. 181 ss.

calare in un contesto di pluralismo giuridico[229], nei suoi arresti la Corte di giustizia prova a fare del suo meglio, attingendo dalle differenti tradizioni nazionali e al contempo tentando di "trascenderle con qualcosa di comune o immaginato come tale"[230]; ma, per quanti sforzi faccia, accontentare tutti risulta quasi impossibile, cosicché i malintesi sono nient'affatto infrequenti.

I problemi, comunque, non discendono certo solo dalla difficoltà di adottare una tecnica argomentativa consona a giudici della più diversa estrazione: in realtà le differenti culture dei Paesi membri non possono non influenzare financo il contenuto delle sue sentenze interpretative[231]. Queste ultime, infatti, devono fare i conti con le singole identità nazionali e le possibili obiezioni che alla luce di queste identità possono essere mosse a quanto queste sentenze più o meno implicitamente richiedono in vista del rispetto delle istanze integratrici insite nel diritto UE.

Alla luce anche solo di queste poche osservazioni, ben si comprende, quindi, la estrema complessità del dialogo tra giudici nazionali ed europei; un dialogo fatalmente condizionato da fattori emotivi di matrice politica e ideologica forieri di prese di posizione avventate, se non di veri e propri passi falsi, da parte degli uni e degli altri.

Tale complessità emerge con chiarezza già dall'esame delle sentenze della Corte di giustizia sibilline, vaghe, contraddittorie. Come si è visto, la necessità di fornire risposte ritagliate sulle esigenze del caso concreto ha a volte indotto i giudici europei a far dipendere la legittimità UE delle fonti interne in materia penale da elementi fattuali alla valutazione dei quali il giudice del rinvio può rivelarsi scarsamente attrezzato; con il risultato di vanificare l'apporto di tali sentenze interpretative in merito alla valutazione delle conformità della normativa nazionale al diritto UE[232]. Altre volte le sentenze dei giudici di Lussemburgo si sono rivelate incapaci di precisare il contenuto delle norme UE, e dunque di far emergere le loro ricadute sul diritto sanzionatorio dei Paesi membri[233]. Altre volte ancora le affermazioni della Corte di giustizia sono risultate così carenti di valide argomentazioni da indurre il sospetto che la pretesa vincolatività dei suoi enunciati risiedesse solo nell'autorità di questa istituzione[234] anziché nella sua autorevolezza[235], nella persuasività delle motivazioni addotte a sostegno delle proprie tesi[236].

Le difficoltà di dialogo tra i giudici nazionali e la Corte di giustizia sono comunque accresciute dalla persistente e spesso inconscia diffidenza dei primi verso fonti e giurisdizioni "esterne" atte a condizionare il diritto penale interno, e dunque a incrinare il potere sovrano dello Stato in questo settore normativo tradizionalmente espressivo dell'autarchia nazionalista in ambito valoriale. Non si spiega diversamente la ritrosia ad accettare che, attraverso l'esame delle fonti europee così come implementate dai giudici di Lussemburgo, l'interpretazione conforme di una norma penale nazionale possa declinarsi *in malam partem*, laddove – come ho insistito a ricordare – una analoga declinazione di tale norma è pacificamente ammessa in sede di interpretazione sistematica di quest'ultima con qualsivoglia testo di diritto interno, persino se di *soft law*[237].

In ogni modo, le forme di dialogo più aspre si riscontrano quando le sentenze interpretative della Corte di giustizia pretendono di riplasmare al ribasso taluni principi supremi e diritti fondamentali dell'ordinamento nazionale, quale innanzitutto il principio di legalità in materia penale e i diritti individuali ad esso correlati. In tali casi – eccezion fatta nelle ipotesi in cui le suddette sentenze concernono l'interpretazione di norme o principi UE incidenti su norme nazionali afferenti a settori normativi integralmente armonizzati dal diritto europeo[238] – la Corte costituzionale italiana, al pari di altre Corti sorelle di Paesi membri, tende ormai a esporre i controlimiti e a invocare il rispetto dell'identità costituzionale nazionale assicurato dall'art. 4.2 TUE. A questo proposito, nei limiti concessi da una relazione a convegno, ho

[229] È la stessa Corte di giustizia a considerarsi un "luogo in cui le culture giuridiche dialogano quotidianamente": cfr. *curia.europa.eu.*
[230] C. Schönberger (2015), p. 510.
[231] Su tali questioni cfr. già Rivero (1958), p. 295 ss.
[232] È questo, appunto, quanto accaduto nella sentenza *Smanor*, in merito alla quale cfr. *supra, sub* par. 4.1, lett. *a),* nt. 32.
[233] Una eventualità siffatta si è verificata nella sentenza *H.K.*, ricordata *supra, sub* par. 4.1, lett. *b).*
[234] E, corrispettivamente, nell'accettazione del comando, a prescindere dal contenuto dello stesso e dalle argomentazioni che lo supportano. Cfr., per talune interessanti considerazioni sulla legittimazione del potere, Duso (2007); Id. (2005), p. 176 ss.
[235] In argomento cfr., per tutti, Berruti, Barone, Pardolesi, Granieri, Scoditti (2013), c. 181 ss.
[236] Emblematico, al riguardo, la sentenza *Link Logistic*, di cui *supra, sub* par. 4.1, lett. *c).*
[237] Cfr. *supra, sub* parr. 4.2 e 4.2.1.
[238] Settori nei quali – giova ripeterlo – "come affermato dalla Corte di giustizia è (…) precluso agli Stati membri condizionare l'attuazione del diritto dell'Unione (…) al rispetto di standard puramente nazionali di tutela dei diritti fondamentali, laddove ciò possa compromettere il primato, l'unità e l'effettività del diritto dell'Unione": Corte cost., ordinanza n. 216 del 2021, punto 7.3.

ritenuto opportuno soffermarmi sui casi *Taricco* e *NE* esponendone brevemente gli sviluppi.

Del caso *Taricco* si è discusso all'infinito e i suoi esiti sono stati oggetto di valutazioni oltremodo diversificate qui impossibili anche solo da riassumere. Credo però sia indiscutibile che il rinvio pregiudiziale del GUP di Cuneo abbia dato il via a un confronto tra la Corte di giustizia e la nostra Corte costituzionale caratterizzato da un significativo livello di conflittualità e da evidenti invasioni di campo da entrambe le parti: un confronto nel quale la Corte di giustizia è sembrata voler assumere i panni del legislatore interno[239], e la Corte costituzionale volersi sostituire alla Corte di giustizia[240]; un confronto nel quale i controlimiti, per quanto non esplicitamente opposti, sono stati sempre ben presenti sullo sfondo, obbligando i giudici di Lussemburgo a frenare le loro pretese in merito all'effettività della tutela del diritto UE in nome del rispetto dei principi/diritti irrinunciabili inscritti nella Suprema Carta nazionale. Un confronto, però, nel quale è mancata ogni forma, anche solo implicita, di autocritica in merito alle carenze (anche, ma non solo) di effettività del nostro sistema sanzionatorio.

Il caso *NE* ha sinora avuto in Italia una eco assai meno forte, complice il fatto che il nostro Paese non ha ritenuto di dover presentare osservazioni nel relativo procedimento. Eppure, non esiste una ragione per non condividere lo sconcerto che la sentenza *NE* ha suscitato in Austria. In risposta ad un rinvio pregiudiziale originato del legittimo dubbio che la disciplina sanzionatoria contenuta in una norma interna di rilievo comunitario confliggesse col principio di proporzionalità UE, la Corte di giustizia non si è limitata a dare a questo principio una interpretazione tale da confermare la sussistenza di tale conflitto, ma ha adottato qualcosa di molto simile a una sentenza additiva di principio della Corte costituzionale[241]. Ha cioè adottato una sentenza che non mira a inficiare la norma nazionale sotto osservazione, ma che neppure – una volta dichiarata l'illegittimità della disposizione oggetto del giudizio "nella parte in cui non commina una sanzione adeguata" – si spinge sino a dettare i nuovi limiti della sanzione da considerarsi alla luce del diritto UE proporzionati alla gravità dell'illecito in questione. La sentenza *NE*, in effetti, si limita a indicare il principio generale (per l'appunto, quello di proporzionalità UE) cui il giudice nazionale deve attingere per utilizzare la norma interna pertinente dopo aver fatto carta straccia dei limiti edittali della sanzione dettati del legislatore nazionale. Si tratta, dunque, di una sentenza cui – a causa del margine di discrezionalità interpretativa più accentuato di quello lasciato al giudice nazionale dalle comuni sentenze additive in materia penale – possono essere indirizzate con ancora maggior vigore le critiche mosse dalla dottrina alle sentenze additive (non di principio) della Corte costituzionale in tale materia; critiche dovute all'attitudine di tali sentenze a stravolgere i rapporti tra potere giudiziario e potere legislativo[242] e che per questa ragione risultano rarissimamente utilizzate in ambito penale[243]. Si tratta di una sentenza che, verrebbe provocatoriamente da dire, in attesa che il legislatore intervenga con una disciplina *erga omnes* conforme al principio indicato dalla Corte di giustizia, rispetto a certi casi di rilievo europeo pretende di imporre ai Paesi membri una concezione "alla francese" della legalità penale, posto che tradizionalmente oltralpe il limite legale della pena è solo quello massimo, al di sotto del quale il giudice è libero di scendere pressocché all'infinito per ragioni di equità legate alle particolarità del caso concreto.

Si potrebbe continuare quasi all'infinito a soffermarsi sulle sorprese che riservano le sentenze della Corte di giustizia in materia penale innescate da un rinvio pregiudiziale per interpretazione, sui problemi che esse pongono nello stesso momento in cui cercano di risolvere quelli sottoposti ai giudici del Kirchberg. I pochi casi rievocati in questa relazione si sono limitati a illustrare alcuni dei nodi gordiani che costellano il diritto multilivello europeo, a ricordare quanto sia faticosa la strada che conduce a una maggiore armonizzazione dei sistemi sanzionatori dei Paesi UE. In ogni caso, alla costruzione di questa strada concorrono significativamente le infinite, più o meno centrate, domande a carattere interpretativo poste dai giudici nazionali del rinvio e le altrettante risposte, più o meno persuasive, che giungono da Lussemburgo. Di certo, anche in futuro a partire da queste domande non mancheranno casi giudiziari controversi capaci di calamitare l'attenzione degli operatori del diritto e di suscitare un dibat-

[239] Anzi, a imporre soluzioni non consentite nemmeno al legislatore nazionale, come quella (poi rientrata grazie alla sentenza *M.A.S.*) di disapplicare la prescrizione ai procedimenti già in corso, in deroga al divieto di retroattività penale sfavorevole.
[240] Cfr., *supra, sub* par. 4.3.1.3, nt. 126.
[241] Il cui dispositivo, come noto, "dichiara – con formule variabili e atipiche – la disposizione impugnata costituzionalmente illegittima nella parte in cui non prevede (…) una soluzione normativa non del tutto precisata": Parodi (2018), p. 386.
[242] Cfr., in particolare, Salazar, Carmela (2000), p. 253 ss. Ricorda (anche se per confutarla) "la preoccupazione che le sentenze additive incorporino spazi riservati al legislatore" Corte costituzionale (2008).
[243] Cfr., anche per i relativi riferimenti giurisprudenziali, Ruggeri, Spadaro (2022), p. 208.

tito reso più interessante e acceso dalla diversità degli ordinamenti degli Stati membri e dalle molte e variegate idee di Europa che condizionano le prese di posizione dei singoli giuristi.

Bibliografia

Aa.Vv. (1981), *Droit communautaire et droit pénal* (Milano-Bruxelles, A. Giuffre, E. Bruylant).

Aa. Vv. (1988) *La sentenza in Europa. Metodo, Tecnica e Stile* (Padova, Cedam).

Aa.Vv. (2016), *La crisi della legalità. Il "sistema vivente" delle fonti penali* (Napoli, Edizioni Scientifiche Italiane).

Amalfitano, Chiara (2019): "Rapporti di forza tra corti, sconfinamento di competenze e complessivo indebolimento del sistema UE?", *La Legislazione Penale*, pp. 1-36.

Amalfitano, Chiara, Pollicino, Oreste (2018): "Jusqu'ici tout va bien… ma non sino alla fine della storia. Luci, ombre ed atterraggio della sentenza n. 115/2018 della Corte costituzionale che chiude (?) la saga Taricco", *Diritti comparati*, pp. 1-11.

Amalfitano, Chiara, Aranci, Matteo (2022): "Mandato di arresto europeo e due nuove occasioni di dialogo tra Corte costituzionale e Corte di giustizia", *Sistema penale*, 10, pp. 5-34.

Andolina, Elena (2021), "La sentenza della Corte di giustizia UE nel caso H.K. c. Prokuratuur: un punto di non ritorno nella lunga querelle in materia di data retention?", *Processo penale e giustizia*, 5, pp. 1204-1217.

Arnold, Rainer (2014), "L'identità costituzionale: un concetto conflittuale", in Di Blase, Antonietta (editor), *Convenzioni sui diritti umani e Corti nazionali* (Roma, RomaTrE-Press), p. 149-156.

Asp, Petter (2007), "Two notions of Proportionality", in Nuotio, Kimmo (editor), *Festschrift in Honour of Raimo Lahti* (Helsinki, University of Helsinki).

Barbareschi, Simone (2022): *Corte costituzionale e certezza dei diritti. Tendenze nomofilattiche del giudizio sulle leggi* (Napoli, Editoriale Scientifica).

Bavazzano, Maddalena (2020), "Le procedure di infrazione europea a carico dell'Italia in materia di rifiuti", *www.arpat.toscana.it.*

Bernardi, Alessandro (1988): "'Principi di diritto' e diritto penale europeo", *Annali dell'Università di Ferrara - Scienze giuridiche*, vol. II, pp. 75-213.

Bernardi, Alessandro (1999): "I tre volti del 'diritto penale comunitario'", *Rivista italiana di diritto pubblico comunitario*, 2, pp. 333-379.

Bernardi, Alessandro (2008), "L'armonizzazione delle sanzioni in Europa: linee ricostruttive", *Rivista italiana di diritto e procedura penale*, p. 76-132.

Bernardi (2012), "I principi di sussidiarietà e di legalità nel diritto penale europeo", *Rivista trimestrale di diritto penale dell'economia*, pp. 15-67.

Bernardi, Alessandro (editor) (2015): *L'interpretazione conforme al diritto dell'Unione europea. Profili e limiti di un vincolo problematico* (Napoli, Jovene).

Bernardi, Alessandro (2016): "Il difficile rapporto tra fonti penali interne e fonti sovranazionali", in Aa.Vv., *La crisi della legalità. Il "sistema vivente" delle fonti penali* (Napoli, Edizioni Scientifiche Italiane), pp. 7-92.

Bernardi, Alessandro (editor) (2017a): I *controlimiti. Primato delle norme europee e difesa dei principi costituzionali* (Napoli, Jovene).

Bernardi, Alessandro, Cupelli, Cristiano (eds.) (2017b): *Il caso Taricco e il dialogo fra le Corti. L'ordinanza n. 24/2017 della Corte costituzionale* (Napoli, Jovene).

Bernardi, Alessandro (2017c): "L'ordinanza Taricco della Corte costituzionale alla prova della pareidolia", *Rivista italiana di diritto e procedura penale*, pp. 48-85.

Bernardi, Alessandro (2017d): "Presentazione. I controlimiti al diritto dell'Unione europea e il loro discusso ruolo in ambito penale", in Bernardi, Alessandro (editor), *I controlimiti. Primato delle norme europee e difesa dei principi costituzionali* (Napoli, Jovene), pp. VII-CXXXIV.

Bernardi, Alessandro (2017e): "La Corte costituzionale sul caso Taricco: tra dialogo cooperativo e controlimiti", *Quaderni costituzionali*, pp. 109-111.

Bernardi, Alessandro (2017f): "Note critiche sull'ordinanza Taricco della Corte costituzionale", in Bernardi, Alessandro, Cupelli, Cristiano (eds.) (2017b): *Il caso Taricco e il dialogo fra le Corti. L'ordinanza n. 24/2017 della Corte costituzionale* (Napoli, Jovene), pp. 17-36.

Bernardi, Alessandro (2023): "Sull'interpretazione conforme al diritto UE con effetti *in malam partem*", *Sistema penale,* 3 febbraio 2023, pp. 1-49.

Berruti, Giuseppe Maria, Barone, Carlo Maria, Pardolesi, Roberto, Granieri, Massimiliano, Scoditti, Enrico (2013), "La giurisprudenza fra autorità e autorevolezza: la dottrina delle corti", *Il Foro Italiano*, c. 181 ss.

Biancarelli, Jacques, Maidani, Dominique (1984), *L'incidence du droit communautaire sur le droit pénal des Etats membres,* in *Revue de science criminelle et de droit pénal comparé*, pp. 225-262 e 455-472.

Bignami, Marco (2017): "Note minime a margine dell'ordinanza *Taricco*", in Bernardi, Alessandro, Cupelli, Cristiano (eds.): *Il caso Taricco e il dialogo fra le Corti. L'ordinanza n. 24/2017 della Corte costituzionale* (Napoli, Jovene), pp. 37-46.

Bin, Roberto (2016): "Taricco, una sentenza sbagliata: come venirne fuori?", *Diritto penale contemporaneo*, pp.1-9.

Borzì, Antonio (2005): "Interpretazione autentica, disapplicazione e giudizio di costituzionalità in una vicenda di contrasto tra diritto interno e ordinamento comunitario. A proposito della sentenza della Corte di giustizia, 11 novembre 2004, causa c-457/02, Niselli", *Federalismi.it – Rivista telematica*, pp. 1-27.

Calzolaio, Ermanno (2009): "Il valore di precedente delle sentenze della Corte di giustizia", *Rivista critica del diritto privato*, 2009, pp. 41-72.

Cannizzaro, Enzo: (2017): "Sistemi concorrenti di tutela dei diritti fondamentali e controlimiti costituzionali", in Bernardi, Alessandro (editor) (2017a): I *controlimiti. Primato delle norme europee e difesa dei principi costituzionali* (Napoli, Jovene), pp. 45-61.

Capelli, Fausto (1988): "'Yogourt francese e pasta italiana' (due sentenze e una proposta di soluzione)", *Diritto comunitario e degli scambi internazionali*, pp. 389-404.

Chignola, Sandro, Duso, Giuseppe (eds.) (2005), *Sui concetti giuridici e politici della costituzione dell'Europa*, Milano, 2005.

Cognetti, Stefano (2011): *Principio di proporzionalità: profili di teoria generale e di analisi sistematica* (Torino, Giappichelli).

Conte, Giuseppe, Fusaro, Andrea, Somma, Alessandro, Zeno Zencovich, Vincenzo (eds.) (2018), Dialoghi con Guido Alpa. Un volume offerto in occasione del suo LXXI compleanno (Roma, RomaTre-Press).

Corte costituzionale (2008), "Problemi dell'omissione legislativa nella giurisprudenza costituzionale", in *www.cortecostituzionale.it*.

Corte di giustizia (2019): "Raccomandazioni all'attenzione dei giudici nazionali, relative alla presentazione di domande di pronuncia pregiudiziale", 2019/C 380/01, punto 10, */eur-lex.europa.eu.*

Croci, Filippo (2015), "Quanto ci costa la violazione degli obblighi 'comunitari'? La recente 'condanna' dell'Italia ex art. 260, par. 2, TFUE in materia di rifiuti e il mancato versamento di fondi strutturali", *rivista.eurojus.it.*

Cupelli, Cristiano (2018): "Aspettando (di nuovo) la Corte costituzionale... sul caso Taricco ritorna la Cassazione", *Diritto penale contemporaneo*, 4, pp. 200-205.

Cupelli, Cristiano (2018b), "La Corte costituzionale chiude il caso Taricco e apre a un diritto penale europeo 'certo'", *Diritto penale contemporaneo*, 6, pp. 227-237.

de Vergottini, Giuseppe (2021), *La Corte costituzionale tra riaccentramento e riequilibrio del sistema*, in *Federalismi.it*, p. IV-XIV.

Dies-Picazo, Luis, Garcia Rivas, Nicolas (eds.), *Los derechos fundamentales en el derecho penal europeo* (Cizur Menor, Aranzadi).

Donini, Massimo (2018), "Lettura critica di Corte cost. n. 115/2018. La determinatezza *ante applicationem* e il vincolo costituzionale alla prescrizione sostanziale come controlimiti alla regola Taricco", *Dir. pen. cont.*, pp. 1-26.

Donini, Massimo, Foffani, Luigi (eds.) (2018): *La "materia penale" tra diritto nazionale ed europeo* (Torino, Giappichelli).

Dlugosz, Johanna (2017), "The Principle of Proportionality in European Union Law as a Prerequisite for Penalisation", *pressto.amu.edu.pl*, pp. 283-300.

Duso, Giuseppe (2007), La logica del potere. Storia concettuale come filosofia politica (Monza, Polimetrica).

Duso, Giuseppe (2005), "Il potere e la nascita dei concetti politici moderni", in Chignola, Sandro, Duso, Giuseppe (eds.), *Sui concetti giuridici e politici della costituzione dell'Europa*, Milano, 2005, p. 176 ss.

Faraguna, Pietro, Perini, Pietro (2016): "L'insostenibile imprescrittibilità del reato. La Corte d'appello di Milano mette la giurisprudenza 'Taricco' alla prova dei controlimiti", *Diritto penale contemporaneo*, pp. 1-17.

Faraguna, Pietro (2017): "Diritto UE e principio di legalità penale: il 'caso Taricco' ritorna alla Corte di Giustizia", *Studium iuris*, pp. 532-540.

Faraguna, Pietro (2022): "L'Unione rispetta le identità nazionali incostituzionali? Considerazioni sui più recenti sviluppi nella giurisprudenza della Corte di giustizia e delle corti costituzionali nazionali in materia di identità costituzionale", in Montanari, Laura, Cozzi, Alessia Ottavia, Milenković, Marko, Ristić, Irena (eds.), We, the People of the United Europe: Reflections on the European State of Mind, (Napoli, Editoriale Scientifica), p. 65 ss.

Gallo, Daniele (2018) "La Corte costituzionale chiude la 'saga Taricco': tra riserva di legge, opposizione de facto del controlimite e implicita negazione dell'effetto diretto", *European Papers*, pp. 885-895.

Gallo, Daniele (2022), "Rethinking direct effect and its evolution: a proposal", *European Law Open*, 1, p. 576-605.

Gallo, Daniele (2022b), *Il primato e l'effetto diretto nell'ordinamento dell'Unione europea*, in Lattanzi, Giorgio, Grasso Gianluca, Lembo, Sara, Condinanzi, Massimo, Amalfitano, Chiara (eds.), *I diritti fondamentali fra Carte e Costituzioni europee* (Roma, IPZS S.p.A), pp. 85-98.

Gambardella, Marco (2021): "Il primato del diritto dell'Unione e la Carta dei diritti fondamentali: il principio di proporzionalità della risposta sanzionatoria", *Cassazione penale*, 1, pp. 26-43.

Gardini, Gianluca (2015): "Rinvio pregiudiziale, disapplicazione, interpretazione conforme: i deboli anticorpi europei e la 'forza sovrana' dell'atto amministrativo inoppugnabile", in Bernardi, Alessandro (editor): *L'interpretazione conforme al diritto dell'Unione europea. Profili e limiti di un vincolo problematico* (Napoli, Jovene), pp. 301-339.

Gradoni, Lorenzo (2017): "Il dialogo tra Corti, per finta", *SIDIBlog*.

Grasso, Giovanni (1989): *Comunità europee e diritto penale* (Milano, Giuffré).

Groussot, Xavier, Loxa, Alezini (2022), "Of The Practicability of Direct Effect and the 'Doctrine of Change'", *www.researchgate.net'*, pp. 1-5.

Guagnini, Giulia (2016): "La Cassazione ritorna sulla nozione 'oggettiva' di rifiuto", *www.tuttoambiente.it*.

Iannone, Celestina (2019): "Le ordinanze di irricevibilità dei rinvii pregiudiziali dei giudici italiani", *www.dirittounioneeuropea.eu*, pp. 249-280.

Jacob, Robert (editor) (1996), *Le juge et le jugement dans les traditions juridiques européennes* (Paris, LGDJ).

Lamarque, Elisabetta (2015): "L'interpretazione conforme al diritto dell'Unione europea secondo la Corte costituzionale italiana", in Bernardi, Alessandro (editor): *L'interpretazione conforme al diritto dell'Unione europea. Profili e limiti di un vincolo problematico* (Napoli, Jovene), pp. 91-108.

Lattanzi, Giorgio, Grasso Gianluca, Lembo, Sara, Condinanzi, Massimo, Amalfitano, Chiara (eds.) (2022), *I diritti fondamentali fra Carte e Costituzioni europee* (Roma, IPZS S.p.A).

Lenaerts, Koen, Gutierrez-Fons, José A. (2020): *Les méthodes d'interprétation de la Cour de justice de l'Union européenne* (Bruxelles, Bruylant).

Luciani, Massimo (2016): "Chi ha paura dei controlimiti?", *www.rivistaaic.it*, 4, pp. 72-77.

Luciani, Massimo (2017): "Il brusco risveglio. I controlimiti e la fine mancata della storia costituzionale", in Bernardi, Alessandro (editor): I *controlimiti. Primato delle norme europee e difesa dei principi costituzionali* (Napoli, Jovene), pp. 63-87.

Luciani, Massimo (2017a): "*Intelligenti pauca*. Il caso Taricco torna (catafratto) a Lussemburgo", *Osservatorio AIC*, 1, pp. 479-489.

Manes, Vittorio (2012a): "Metodo e limiti dell'interpretazione conforme alle fonti sovranazionali in materia penale", *Archivio penale*, 1, p. 1-50.

Manes, Vittorio (2012b): *Il giudice nel labirinto. Profili delle intersezioni tra diritto penale e fonti sovranazionali* (Roma, Dike Giuridica).

Mangiameli, Stelio (editor) (2006): *L'ordinamento europeo*, II, *L'esercizio delle competenze* (Milano, Giuffré).

Mari, Luigi (1981), "Quelques réflexions sur la 'mesure excessive' de la sanction pénale par rapport au droit communautaire", in Aa.Vv., *Droit communautaire et droit pénal* (Milano-Bruxelles, A. Giuffre, E. Bruylant), pp. 150-166.

Marin, Luisa, Montaldo, Stefano (eds.), (2020), *The Fight Against Impunity in EU Law*, *Hart Studies in European Criminal Law* (Oxford, Hart).

Martire, Dario, Pistone, Tommaso (2021), "Sospensione della prescrizione, principio di legalità e bilanciamento sempre possibile. Considerazioni a margine della sentenza n. 278 del 2020 della Corte costituzionale", *Osservatorio costituzionale*, 3, pp. 166-188.

Martufi, Adriano (2013): "Eccezioni alla retroattività favorevole e diritti fondamentali", *Diritto penale e processo*, pp. 488-505.

Mazzacuva, Francesco (2016), "Art. 7. *Nulla poena sine lege*", in Ubertis, Giulio, Viganò, Francesco (eds.), *Corte di Strasburgo e giustizia penale* (Torino, Giappichelli), pp. 244 ss.

Mengozzi, Paolo (2015): "A European Partnership of Courts. Judicial Dialogue between the EU Court of Justice and National Constitutional Courts", *Diritto dell'Unione Europea*, 3, pp. 701-720.

Mezzetti, Enrico (1994): *La tutela penale degli interessi finanziari dell'Unione europea* (Padova, Cedam).

Montanari, Laura, Cozzi, Alessia Ottavia, Milenković, Marko, Ristić, Irena (eds.) (2022), We, the People of the United Europe: Reflections on the European State of Mind, (Napoli, Editoriale Scientifica).

Nuotio, Kimmo (editor) (2007), *Festschrift in Honour of Raimo Lahti* (Helsinki, University of Helsinki).

Palazzo, Francesco (1999): *Introduzione ai principi di diritto penale* (Torino, Giappichelli).

Palazzo, Francesco (2017): *Armonizzazione europea e costituzionalismo penale tra diritto e politica*, in Bernardi, Alessandro (editor): *I controlimiti. Primato delle norme europee e difesa dei principi costituzionali* (Napoli, Jovene), pp. 273-287.

Palazzo, Francesco (2023), *Corso di diritto penale. Parte generale* (Torino, Giappichelli).

Panunzio, Sergio P. (editor) (2007), *I costituzionalisti e la tutela dei diritti nelle corti europee: il dibattito nelle riunioni dell'Osservatorio costituzionale presso la Luiss Guido Carli dal 2003 al 2005* (Padova, Cedam)

Parodi, Giampaolo (2022): "Effetti diretti della Carta dei diritti fondamentali dell'Unione europea e priorità del giudizio costituzionale", *Rivista AIC*, 4, pp. 128-145.

Parodi, Giampaolo (2018): *Il giudice di fronte alle sentenze additive di principio nella prassi recente*, in Conte, Giuseppe, Fusaro, Andrea, Somma, Alessandro, Zeno Zencovich, Vincenzo (eds.), Dialoghi con Guido Alpa. Un volume offerto in occasione del suo LXXI compleanno (Roma, RomaTre-Press), pp. 385-403.

Passaglia, Paolo (editor) (2010): *Corti costituzionali e rinvio pregiudiziale alla Corte di giustizia*, *www.cortecostituzionale.it*.

Petroni, Giovanni (2021): "Il caso Prokuratuur: il difficile dialogo tra le Corti e le conseguenze della sentenza della Corte di giustizia nell'ordinamento nazionale", *Giustizia insieme*.

Poli, Flavia (2012): "Il principio di retroattività della legge penale più favorevole nella giurisprudenza costituzionale ed europea", *Rivista AIC*, 3, pp. 1-29.

Pollicino, Oreste (2012): "Qualcosa è cambiato? la recente giurisprudenza delle Corti costituzionali dell'Est vis à vis il processo di integrazione europea", *www.dirittocomparati.it*, pp. 1-32.

Portero Henares, Manuel (2010), "¿Principio de efectiva protección de bienes jurídicos? Derecho penal europeo y principio de proporcionalidad, Garantías penales", in Dies-Picazo, Luis, Garcia Rivas, Nicolas (eds.), *Los derechos fundamentales en el derecho penal europeo* (Cizur Menor, Aranzadi), pp. 305-326.

Postiglione, Miriam (2019): *Il valore del "precedente" nella giurisprudenza del giudice dell'Unione europea*, Tesi dottorale (Milano).

Ranieri, Filippo (1996), "Styles judiciaires dans l'histoire européenne: modèles divergents ou traditions communes? ", in Jacob, Robert (editor), *Le juge et le jugement dans les traditions juridiques européennes* (Paris, LGDJ), pp. 181-195.

Recchia, Nicola (2020): *Il principio di proporzionalità nel diritto penale. Scelte di criminalizzazione e diritti fondamentali* (Torino, Giappichelli).

Recchia, Nicola (2022), "La proporzione sanzionatoria nella triangolazione tra giudici comuni, Corte costituzionale e Corte di Giustizia", *Quaderni costituzionali*, 4, pp. 871-898.

Riccardi, Giuseppe (2017), "'Patti chiari, amicizia lunga'. La Corte costituzionale tenta il 'dialogo' nel caso Taricco, esibendo l'arma dei controlimiti", in Bernardi, Alessandro, Cupelli, Cristiano (eds.): *Il caso Taricco e il dialogo fra le Corti. L'ordinanza n. 24/2017 della Corte costituzionale* (Napoli, Jovene), pp. 355-378.

Rinaldini, Federica (2021): "Data retention e procedimento penale. Gli effetti della sentenza della Corte di giustizia nel caso H.K. sul regime di acquisizione dei tabulati telefonici e telematici: urge l'intervento del legislatore", *Giurisprudenza Penale Web,* 5, pp. 1-13.

Rivero, Jean (1958), "Le problème de l'influence des droits internes sur la Cour de Justice de la CECA", *Annuaire français de droit international*, 4, pp. 295-308.

Romano, Salvatore Alberto (2007), "Tecniche argomentative e diritti fondamentali; La Corte di Giustizia delle Comunità europee e i diritti nazionali; Diritti e rapporti tra le corti", in Panunzio, Sergio P. (editor), *I costituzionalisti e la tutela dei diritti nelle corti europee: il dibattito nelle riunioni dell'Osservatorio costituzionale presso la Luiss Guido Carli dal 2003 al 2005* (Padova, Cedam), pp. 666-695.

Rossi, Lucia Serena (2022): "Un dialogo da giudice a giudice'. Rinvio pregiudiziale e ruolo dei giudici nazionali nella recente giurisprudenza della Corte di giustizia", *Quaderni AISDUE*, 4, p. 50-84.

Ruggeri, Antonio (2006), "Trattato costituzionale, europeizzazione dei 'controlimiti' e tecniche di risoluzione delle antinomie tra diritto comunitario e diritto interno (profili problematici)", *www.forumcostituzionale.it*.

Ruggeri, Antonio (2018): "Taricco, amaro finale di partita", *Consulta OnLine*, 3, pp. 488-499.

Ruggeri, Antonio (2021): "Il giudice e la 'doppia pregiudizialità': istruzioni per l'uso", *Federalismi.it*, 6, pp. 211-230.

Ruggeri, Antonio (2022): "I diritti fondamentali, tra riconoscimento normativo ed effettività della tutela", *www.movimentoeuropeo.it*, pp. 1-18.

Ruggeri, Antonio, Silvestri, Gaetano, (eds.) (2000), *Corte costituzionale e Parlamento. Profili problematici e ricostruttivi* (Milano, Giuffré).

Ruggeri, Antonio, Spadaro, Antonino (2022): *Lineamenti di diritto costituzionale* (Torino, Giappichelli).

Ruggeri, Antonio (2023), "Rapporti interordinamentali ed effettività della tutela dei diritti fondamentali", *La Rivista Gruppo di Pisa*, 1, pp. 121-141.

Salcuni, Giandomenico (2015): "Legalità europea e prescrizione del reato", *Archivio Penale (Web)*, 3, pp. 1-15.

Satzger, Helmut (2020) (eds.), *Harmonisierung strafrechtlicher Sanktionen in der Europäischen Union – Harmonisation of Criminal Sanctions in the European Union* (Baden Baden, Nomos).

Scholtes, Julian (2021): "Abusing Constitutional Identity", *German Law Journal*, 22, pp. 534-556.

Schönberger, Christoph (2015): "'Mi attendu, mi dissertation'. Le style des décisions de la Cour de justice de l'Union européenne", *Droit et société*, 3, pp. 505-519.

Scaccia, Gino (2006): "Il principio di proporzionalità", in Mangiameli, Stelio (editor): *L'ordinamento europeo*, II, *L'esercizio delle competenze* (Milano, Giuffré), pp. 225-274.

Silvani, Simona (2009): *Il giudizio del tempo. Uno studio sulla prescrizione del reato* (Bologna, Il Mulino).

Siracusa, Licia (2023): *Oblio e memoria del reato nel sistema penale* (Torino, Giappichelli), 2023.

Salazar, Carmela (2000), "'Guerra e pace' nel rapporto Corte-Parlamento: riflessioni su pecche e virtù delle additive 'di principio' quali decisioni atte a rimediare alle 'omissioni incostituzionali' del legislatore", in Ruggeri, Antonio, Silvestri, Gaetano, (eds.), *Corte costituzionale e Parlamento. Profili problematici e ricostruttivi* (Milano, Giuffré), pp. 253 ss.

Sotis, Carlo (2012): "I principi di necessità e proporzionalità della pena nel diritto dell'Unione europea dopo Lisbona", *Diritto penale contemporaneo – Rivista trimestrale*, 1, pp. 111-122.

Sotis, Carlo (2017), *Tra Antigone e Creonte io sto con Porzia. Riflessioni su Corte costituzionale 24 del 2017 (caso* Taricco), in Bernardi, Alessandro, Cupelli, Cristiano (eds.): *Il caso Taricco e il dialogo fra le Corti. L'ordinanza n. 24/2017 della Corte costituzionale* (Napoli, Jovene), pp. 435-454.

Tsolka, Olga (2022) : "Direct Effect of the 'Proportionality Requirement of [Criminal] Sanctions': Considerations on the European Court of Justice Overruling in the Case 'NE II' (C-205/20)", in *EuCLR European Criminal Law Review*, 2, pp. 131-149.

Ubertis, Giulio, Viganò, Francesco (eds.) (2016), *Corte di Strasburgo e giustizia penale* (Torino, Giappichelli).

Valentini, Vico (2012): "Legalità penale convenzionale e obbligo d'interpretazione conforme alla luce del nuovo art. 6 TUE", *Diritto penale contemporaneo – Rivista trimestrale*, 2, pp. 167-179.

Venturi, Filippo (2022), "Le ordinanze n. 216 e 217 del 2021 della Corte Costituzionale: il rinvio pregiudiziale come calumet della pace nell'ordinamento (penale) multilivello", *Diritti comparati*.

Vespaziani Alberto (2017): "Quaeta non movere? Recensione a "Le opinioni dissenzienti dei giudici costituzionali. Uno studio comparativo" di Alessandra Di Martino, Napoli, 2016", *Diritti comparati*.

Viganò, Francesco (2011): "Sullo statuto costituzionale della retroattività della legge più favorevole. Un nuovo tassello nella complicata trama dei rapporti tra Corte costituzionale e Corte EDU: riflessioni a margine della sentenza n. 236/2011", *Diritto penale contemporaneo*, p. 1-22.

Viganò, Francesco (2016): "Il caso Taricco davanti alla Corte costituzionale: qualche riflessione sul merito delle questioni, e sulla reale posta in gioco", in Bernardi, Alessandro (editor): I *controlimiti. Primato delle norme europee e difesa dei principi costituzionali* (Napoli, Jovene), pp. 233-272.

Viganò, Francesco (2017), "Le parole e i silenzi. Osservazioni sull'ordinanza n. 24/2017 della Corte costituzionale sul caso Taricco", in Bernardi, Alessandro, Cupelli, Cristiano (eds.): *Il caso Taricco e il dialogo fra le Corti. L'ordinanza n. 24/2017 della Corte costituzionale* (Napoli, Jovene), pp. 475-491.

Viganò, Francesco (2021), *La proporzionalità della pena. Profili di diritto penale e costituzionale* (Torino, Giappichelli).

Viganò, Francesco (2022): "La proporzionalità della pena tra diritto costituzionale italiano e diritto dell'Unione europea: sull'effetto diretto dell'art. 49, paragrafo 3, della Carta alla luce di una recentissima sentenza della Corte di giustizia. Nota a Corte di giustizia UE, Grande Sezione, sent. 8 marzo 2022, C-205/20, NE", *Sistema penale*, pp. 1-19.

Viscardini Donà, Wilma. (2013): "Riflessioni sull'efficacia diretta della normativa dell'Unione europea e sull'effetto utile della giurisprudenza della Corte di giustizia", *Diritto comunitario e degli scambi internazionali*, pp. 345-372.

Vozza, Donato (2015), "Le tecniche gradate di armonizzazione delle sanzioni penali nei recenti interventi dell'Unione europea", *Diritto penale contemporaneo – Rivista trimestrale,* 3, pp. 16-33.

The Crime of Money Laundering: A Touchstone for The Principles of *Il Manifesto del diritto penale liberale e del giusto processo*

Il reato di riciclaggio: un banco di prova per i principii del Manifesto del diritto penale liberale e del giusto processo

El delito de lavado de activos: una prueba para los principios del Manifiesto del derecho penal liberal y del debido proceso

Matthias Jahn
Professore di diritto e procedura penale presso la Goethe-Universität Frankfurt am Main e Giudice presso la Corte d'appello regionale di Francoforte
jahn@jur.uni-frankfurt.de

Federica Helferich
Dottoranda di ricerca in diritto penale presso l'Università degli Studi di Firenze e la Goethe-Universität Frankfurt am Main
federica.helferich@unifi.it

Money Laundering, Fundamental Rights, Fair Trial

Riciclaggio, Diritti fondamentali, Giusto processo

Lavado de activos, Derechos fundamentales, Debido Proceso

Abstracts

Far from being an *acquis* in the national penal legislation, the core principles of liberal criminal law are constantly at risk of being violated by the current developments of both substantial and procedural criminal law. For this reason, such principles have been reaffirmed by the *Manifesto del diritto penale liberale e del giusto processo* issued by the *Unione delle Camere Penali Italiane* in 2019 and publicly discussed in Bologna in November 2022. Building on that forum, this article intends, on the one hand, to illustrate how these principles stand in a line of continuity with the so-called *Frankfurter Schule für Strafrecht*. On the other hand, this paper compares the *Manifesto's* Principles number 2, 3, 5, 11 and 15 with the Italian and German criminal provisions on money laundering, highlighting the instrumental nature of this offence and its paradigmatic suitability to violate the principles of liberal criminal law.

Gli attuali sviluppi del diritto penale sostanziale e processuale espongono i principii fondamentali del diritto penale liberale – ben lontani dal costituire un *acquis* delle legislazioni penali nazionali – a un rischio costante di violazione. Per questa ragione, tali principii sono stati riaffermati nel *Manifesto del diritto penale liberale e del giusto processo*, edito dall'*Unione delle Camere Penali Italiane* nel 2019 e oggetto di un dibattito a Bologna, nel novembre 2022. Prendendo le mosse da tale incontro, il presente articolo intende, da un lato, mostrare la continuità tematica tra tali principii e la c.d. *Frankfurter Schule für Strafrecht*, dall'altro lato, si propone di comparare i principii numero 2, 3, 5, 11 e 15 del *Manifesto* con la legislazione italiana e tedesca in materia di riciclaggio, evidenziando la natura strumentale di tale reato e la sua paradigmatica attitudine a violare i principii di un diritto penale liberale.

Lejos de ser una cuestión indiscutida, los principios esenciales del derecho penal están en constante riesgo de ser infringidos por los actuales desarrollos del derecho penal tanto sustantivo como procesal. Por esta razón, estos principios fueron reafirmados en el Manifiesto del derecho penal liberal y del debido proceso, publicado por la Unione delle Camere Penali Italiane en 2019 y objeto de debate en Bolonia en noviembre de 2022. A partir de este encuentro, el presente artículo tiene como objetivo, por un lado, mostrar la continuidad temática entre estos principios y la llamada Frankfurter Schule für Strafrecht, y, por otro lado, comparar los principios número 2, 3, 5, 11 y 15 del Manifiesto con la legislación italiana y alemana sobre el delito de lavado de dinero, destacando la naturaleza instrumental de este delito y su propensión paradigmática a violar los principios de un derecho penal liberal.

Sommario

1. Introduction. The *Manifesto* on the trail of the *Frankfurter Schule des Strafrechts*.

The *Manifesto del diritto penale e del giusto processo*, issued by the *Unione delle Camere Penali Italiane* (UCPI) in 2019 and discussed in Bologna, 18-19 November 2022, during the International Congress "*I principii del Manifesto: un dibattito per i penalisti europei*", is clearly an expression of liberal criminal law. The reader of the *Manifesto* will easily find a deep connection with the thoughts developed by the so-called Frankfurt School of Criminal Law (*Frankfurter Schule des Strafrechts*)[1].

1.1. *Then…*

Indeed, many criminal law scholars interpreted the joint papers issued by the "founders" of the *Schule*[2] – namely Professors Winfred Hassemer, Klaus Lüderssen and Wolfgang Naucke – as a sort of "Manifesto" of the Frankfurt School, thus implying that their shared view on criminal law prevailed over their standpoints and works. Hassemer, Lüderssen and Naucke, however, repeatedly maintained that such a School ultimately did not exist[3] or, "if it ever existed […] it never was founded, but rather grew up spontaneously"[4] – let alone the existence of a Manifesto!

Indeed, what others labelled as "*Schule*" actually happened to be, from the viewpoint of the founders, a sort of academic affiliation, which shared the same *forma mentis* and critical approach towards criminal law[5]. Naucke, Hassemer and Lüderssen "naturally" agreed on considering criminal law as a source of "irresolvable problems"[6]. And, even if the answers they provided to these problems could diverge widely[7], what mattered and proved to be the true bond was the way the answers were looked for: that is, through the peculiar style of arguing and debating ("*Debattenstil*")[8] that the three Professors specifically developed at Goethe University in the early '70s.

With the help of a post-1968 dialogue-friendly environment, intellectual inventiveness and readiness to constant confrontation, debates rose everywhere – in classes, in elevators, during lunch and, of course, at the legendary *Dienstagsseminar*[9], an academic arena which still takes place after fifty (!) years, every Tuesday since the Winter Term 1973/74. This *esprit* and the critical attitude towards criminal law ended up being inherited by the "scholars" (Peter-Alexis Albrecht; Klaus Günther; Ulfrid Neumann; Cornelius Prittwitz; Felix Herzog…) and still bond legal doctrine nowadays.

[1] This article is based on the speech delivered at the conference of the *Unione delle Camere Penali Italiane* titled "*I principii del manifesto: un dibattito per i penalisti europei*" which took place on 18-19 November 2022 in Bologna. Sections 1 to 2.1. were written by Matthias Jahn; Sections 2.2. to 3 were written by Federica Helferich.

[2] See for instance Hassemer *et al.* (1979a); Hassemer *et al.* (1983b), as well as the publications issued in the book series "*Frankfurter Kriminalwissenschaftliche Studien*" (Peter Lang Verlag) and those edited by the Institut für Kriminalwissenschaften Frankfurt (1995a); Institut für Kriminalwissenschaften Frankfurt (1999b); Institut für Kriminalwissenschaften Frankfurt (2007c).

[3] Naucke (2010), p. 434.

[4] Hassemer (2005b), p. 10.

[5] On this topic, see for details Jahn M. and Ziemann S. (2014), p. 943.

[6] Lüderssen (2010), p. 373.

[7] Indeed, Kuhlen (2023), p. 143 ff., argues that the Frankfurt School did not exist, both because of the heterogeneity and the aporia of the personal dogmatic solutions to the abovementioned problems.

[8] Naucke (2010), p. 434.

[9] Naucke (2010), pp. 432-433.

1.2. *...And now.*

Debate is exactly what the principles of the *Manifesto* and the related Congress pursue. Indeed, Frankfurt in the early '70s, with its all-peculiar social and political climate[10], was the right time and the right place for the development of ground-breaking ideas on criminal law. Likewise, *now* is the right time and the right place for discussing the *Manifesto* and sharing ideas (and concerns, too!) on the actual state of criminal law among European legal scholars, in the light of the "School's" idea of an "*allgemeines Strafrecht*"[11].

The core similarities between the *Manifesto* and the critical approach of the *Schule*, however, are content-related.

– First off, they share the novel idea of criminal law and criminal punishment as a *power*, as such prone to abuse and in constant need of boundaries[12]. These boundaries, moreover, need to operate on a double level[13]. On the one hand, they serve to legitimise (*i.e.*, democratize) the *allocation* of the punitive power: from this point of view, the *Manifesto* rightly warns against shifts of authority between the Legislative and the Government, as well as between the Legislative and the Judiciary[14]. On the other hand, boundaries guarantee the legitimacy of the *exercise* of said power. This is a key aspect of the so-called *Strafverfassungsrecht*[15], which in Italy was paradigmatically developed by Franco Bricola[16]: namely, the idea that a national Constitution is both a limit and a binding content provider for national criminal law[17]. It is not by chance that Winfried Hassemer, the first criminal lawyer from *Academia* appointed as a judge of the *Bundesverfassungsgericht* (BVerfG), in his dissenting opinion to the decision *Geschwisterinzest* of 2002[18], stated that material criminal law, too, had to comply with the *Grundgesetz*[19].

– Secondly, the *Frankfurter Schule des Strafrechts* and the *Manifesto* share a critical view on the use of criminal law as a panacea, a sort of cure-all-means offered by a good prince for dealing with any worrisome phenomenon affecting society. Highlighting the social and political costs of this dysfunctional use of penal law, the *Manifesto* resonates with the *Schule's* thoughts on the use of criminal law both as a tool and as a symbol for societal problems[20].

– And, thirdly, the *Manifesto* stresses the risk of criminal procedural law being an arena of social regulation and score-settling, instead of a time and space solely aimed at determining the facts and the possible criminal responsibility of the person charged[21]. In this respect, the recent promise of the German Government to make criminal trials "more effective, quicker, more modern and more workable" cannot but raise concern among legal scholars. The criminal procedural law forged by the German Code for criminal procedures (*Strafprozeßordnung* – StPO) actually calls for the opposite approach. It is about time that a *Magna Charta Libertatum* of the accused person is introduced in the StPO, in order to affirm and enshrine the core principles in this matter: the presumption of innocence, the full dignity of the person charged and the right to a fair trial, to begin with[22]. These principles, indeed, are constantly at risk of fading too far into the background.

This is why the *Manifesto* is particularly needed in the European landscape right now, as much as the penal law needed our predecessors' groundwork back in the early days of the *Frankfurter Schule* fifty years ago. Pressure raises counterpressure, one may say.

[10] Jahn M. and Ziemann S. (2014), pp. 944-945.
[11] Hassemer (2005b), p. 11.
[12] Unione delle Camere penali italiane (2019), pp. 8 and 10.
[13] On this topic see the insights by Bartoli (2022), pp. 56-58.
[14] Unione delle Camere penali italiane (2019), p. 3.
[15] See the various contributions to Bäcker M. and Burchard C. (2022).
[16] See Donini (2012), p. 63.
[17] Burchard (2016), p. 28, claims that the Constitution "organizes" and "limits" criminal law, and therefore "ends up legitimizing it".
[18] BVerfG, Beschl. v. 26. Februar 2008 – 2 BvR 392/07 = BVerfGE 120, 224 (255).
[19] See Jahn (2016a), p. 77.
[20] Unione delle Camere penali italiane (2019), pp. 4-5.
[21] Unione delle Camere penali italiane (2019), p. 4.
[22] Jahn (2022d) and Jahn (2022e).

2. The crime of money laundering: a touchstone for the principles of the *Manifesto*.

Unfortunately, the importance of the *Manifesto* can also be confirmed by contrast, *i.e.*, by highlighting the provisions, interpretations and practices that actually *deny* its core statements. In this regard, a comparable key role is played by the crime of money laundering, in Italy as well as in Germany.

As a matter of fact, both article 648-*bis* of the *Codice penale* (art. 648-*bis* c.p.) and § 261 of the German *Strafgesetzbuch* (§ 261 StGB) seem to have undergone a process of expansion and instrumentalization in gross disregard of the principles of liberal penal law. Indeed, the offence of *riciclaggio*/*Geldwäsche* has become a paradigmatic example precisely of the form of criminal law that the *Manifesto* aims to make aware of.

This is particularly true when observing the recent reforms that have occurred in both legal systems in order to comply with EU Directive 2018/1673[23]. Legislative Decree 195/2021 has broadened the scope of art. 648-*bis* c.p. by including in the range of predicate offences all crimes of negligence and certain types of contraventions. In Germany, the Law of 9 March 2021 has gone even further. It has given § 261 StGB the shape of an *all-crimes-Tatbestand* encompassing *every* unlawful fact (*rechtswidrige Tat*) – whereas until that moment the *Geldwäsche* provision was based on a closed list of (mostly serious) predicate crimes. If the broadening of art. 648-*bis* c.p. raises more than a dogmatic perplexity[24], the new shape of § 261 StGB is a veritable change of paradigm[25] – even though this provision seems doomed once again to remain more effective on paper than in reality[26].

For this reason, this paper intends to run a condensed "test" of some of the core statements of the *Manifesto*[27] against both article 648-*bis* c.p. and § 261 StGB.

2.1. *Principle no. 2.*

"*Criminal law is an instrument of social control strongly affecting one's fundamental rights and interests* […]".

The offence of money laundering indeed affects personal liberties and freedoms at more than one level.

Firstly, on a strictly punitive one. As it will be seen in connection with Principle no. 5, the range of behaviours that are criminalised as "money laundering", both in Italy and in Germany, is wide and poorly determined.

But the crime of money laundering represents "*an instrument of social control strongly affecting one's fundamental rights and interests*" also on an administrative-preventive level. The system of anti-money laundering (AML) is a system of integrated control based on crime-prevention[28] via detention and use of financial information; in this context, the repressive moment is conceived as a last resort.

Indeed, the offence of money laundering is *genetically* connected to the information-based AML system: the very decision to criminalise money laundering roots in global economic concerns[29] shaped by the growing interconnectedness of markets and financial systems. As a result, the crime of money laundering – just as the preventive apparatus! – is a means of *control* of illegally obtained assets and financial risks[30]. To the criminal lawyer, this situation recalls the BVerfG's constitutionally grounded *caveat* on the instrumentalization and weaponization of criminal law[31].

[23] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law.
[24] Overview by Melchionda (2022), p. 1 ff.
[25] Gercke *et al.* (2021), p. 330.
[26] Based on an empirical study, Bussmann, K.-D. and Veljovic, M. (2020), p. 420, already observed that, even under the previous version of § 261 StGB, Public Prosecutors very often suspended trials for money laundering (§ 153a StPO) because of the predicate crime being petty.
[27] To this end, we will provide an English translation of the relevant principles of the *Manifesto*.
[28] Stessens (2001), p. 108, qualifies it as "a twin-track fight".
[29] Alldridge (2001), p. 280.
[30] Pieth (1999), p. 543.
[31] BVerfG, Urt. v. 30. Juni 2009 – 2 BvE 2/08, 2 BvE 5/08, 2 BvR 1010/08, 2 BvR 1022/08, 2 BvR 1259/08, 2 BvR 182/09 = BVerfGE 123,

But the crime of money laundering also displays an *operative* connection to the AML system. This raises concerns with respect to *Manifesto's* Principle no. 2 under two different viewpoints, both strictly connected to "*social control*": the obtainment and the exchange of financial information.

Suspicion transaction reports (STR) are the main tool for *obtaining* such information[32]. The trigger for an STR is the (merely factual) suspicion of an ongoing, attempted or achieved operation of "money laundering". Now, whilst in Italy the notion of *riciclaggio* serving to this end is autonomously defined by art. 2, par. 4, of Legislative Decree 231/2007[33], the German legislation (§ 43 *Geldwäschegesetz* – GwG)[34] refers to the *criminal* notion of money laundering, *i.e.*, to § 261 StGB[35]. This reference creates a functional liaison between the repressive and the preventive system[36]: the wider the criminal notion of *Geldwäsche*, the higher the number of STR and the flow of fiscal information[37].

In addition, FIUs are also legitimised to acquire information *motu proprio*, both by consulting obliged entities (even regardless of a previous STR)[38] and by accessing a wide range of public registers and databanks[39].

Also, criminal law becomes an instrument of social control because of the *exchange* of such information among public entities involved in the fight against money laundering. Indeed, according to the relevance of the financial information in their possession, national FIUs have to share said information with the judicial, law enforcement, fiscal, custom or intelligence authorities[40] as well as with FIUs of other Member States[41].

Such a network of information exchange is likely to threaten (among other things) the constitutional right to informational self-determination (*informationelle Selbstbestimmung*), as stated by the BVerfG in the *Antiterrordateigesetz I* decision[42], in that it may determine a *de facto* loss of the pivotal distinction between intelligence activities (aiming at a preventive security-oriented data collection and analysis) and investigation activities (meant to react to suspected committed crime and aiming at acquiring incriminating and also exculpatory evidence). This distinction is indeed the precondition of the principle of separation of police and intelligence data (*informationneller Trennungsprinzip*)[43], whose circumvention may forge intelligence-based rather than suspicion-led police investigations.

267 (410), *Lissabon* ("The core content of criminal law does not serve as a technical instrument for carrying out international cooperation but represents the particularly sensitive democratic decision on a legal ethical minimum standard").

[32] Article 35 of D. Lgs. 231/2007 and § 43 GwG.

[33] Legislative decree of 21 November 2007, *Implementing Directive 2005/60/CE on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and Directive 2006/70/CE laying down implementing measures for Directive 2005/60/EC*, in G.U. Serie generale n. 290 of 14 December 2007.

[34] *Law on the Identification of Profits from Serious Crimes* of 23 October 1993, in BGBl. 1993, I, 1770.

[35] Obliged entities shall file a suspicious transaction report if elements are indicating that a good connected to an economic transaction originates from a criminal behaviour that could be a predicate crime of *Geldwäsche* under § 261 StGB (§ 43, par. 1, GwG).

[36] Findeisen (1997), p. 121.

[37] In 2010, the FATF regretted that "for an economy the size of Germany's […] the level of suspicious transaction reports appears to be unusually low" (although of "very high quality"), because it "denies the FIU and the state law enforcement Authorities important access to a wider intelligence base": Fatf/Gafi (19 February 2010), pp. 170-171, parr. 714 and 719. In 2021, the German FIU observed that one of the causes for the notable increase in STR was the adoption of an all-crimes approach in § 261 StGB: FIU (12 September 2022), pp. 15-16.

[38] Art. 6, par. 6, letter c) of D. Lgs. 231/2007; § 30, subsection 3, GwG. On this subject see the critical remarks by Vogel, B. and Maillart, J.-B. (2020), p. 207.

[39] Art. 6, par. 6, letter e) and art. 9 of D. Lgs. 231/2007; §§ 31 and 23 GwG.

[40] Art. 47 D. Lgs. 231/2007; § 32 GwG.

[41] Art. 53 of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. On this topic, see the highlighted issues by Gianfelici, F. and Siena, F. A. (2021), p. 21 ff.

[42] BVerfG – 1 BvR 1215/07, Urt. v. 24. April 2013 = BVerfGE 133, 277 (316), Rn. 93 ff. The *Antiterrordateigesetz I* decision concerned a joint counter-terrorism database allowing data sharing among a large number of security authorities with very different mandates, especially police authorities and intelligence services, in disregard of the principle of proportionality. The right to informational self-determination originates from Art. 2, par. 1, in conjunction with Art. 1, par. 1, of the German Constitution (*Grundgesetz*, GG); it has recently been reaffirmed in two decisions concerning information exchange between police and intelligence: BVerfG – 1 BvR 1619/17, Urt. v. 26 April 2022, upcoming in BVerfGE 162; BVerfG – 1 BvR 2354/13, Beschl. v. 28. September 2022, upcoming in BVerfGE 163.

[43] Also applying to "extended use" (data mining) of databases set up for police authorities and intelligence services: see BVerfG – 1 BvR 3214/15, Urt. v. 10. November 2020 = BVerfGE 156, 11 (40), Rn. 74 – *Antiterrordateigesetz II*.

2.2. *Principle no. 3.*

"*A penal system is only liberal when the punitive reaction is legitimated. The legitimisation derives from the respect of a strict necessity-rule; from the proportion in respect to the underlying legal interests, and the respect of the person affected*".

The legitimisation of the crime of money laundering in this respect appears to be doubtful because the "underlying legal interest" that the criminal provision is supposed to provide for – the *Rechtsgut* – is difficult to grasp. It has been said by Gunter Arzt that § 261 StGB came into the world "without a brain and without a heart, which means without a *Rechtsgut*"[44]: which is also true for art. 648-*bis* c.p. Or, if ever they have had a *Rechtsgut*, because of their initial connection to organized crime and, since 2001, to the financing of terrorism[45], they now have completely lost it on their way to being the fit-all-crimes for every investigative purpose.

The judicial approach to this topic is rather disappointing: some judges seem to have given up on recovering the legal interest underlying the national offence of money laundering[46]; some others resort to the concept of multi-harmfulness[47] or else talk of a "peculiar *Rechtsgut* not to be further concretised"[48]. For its part, the scholarly debate still revolves around two poles equally unsatisfactory because equally unable to grasp the complexity of the phenomenon of money laundering.

On the one hand, the claim that the offence of money laundering is dangerous for the integrity of the economic and financial legal system – *i.e.*, for competition rules[49] as well as for the collective interest for an equal and correct allocation of monetary resources[50] – does not find an echo in the structure of the criminal provisions, especially after the all-crimes approach[51] has been enlarged (Italy) or newly adopted (Germany). Indeed, the economic quality and/or quantity of the predicate offence has no influence whatsoever on the criminal relevance of the laundering fact, nor does the behaviour criminalised under art. 648-*bis* c.p. and § 261 StGB contain any reference to an economic context[52]. Also, German legal scholars are keen on pointing out that the integrity of the economic and financial legal system is not an appropriate *Rechtsgut* at all, because it has a collective and abstract nature – thus resonating with the *Frankfurter Schule* – and appears to be far too fragile and too fungible at the same time[53]: all the more reason to deny this economic legal interest has an actual hermeneutic and critical function[54].

On the other hand, the claim that the money laundering offence is a crime against the administration of justice (*Rechtspflege*) reverberates in the structure of both art. 648-*bis* c.p.[55] and § 261 StGB[56]. The modal clause "*in a manner that hampers the identification*" of the illicit provenance and the newly shaped behaviours of § 261 Abs. 1 Nr. 1 and 2 and Abs. 2 (see *infra*) indeed (may) harm the investigation and confiscation activities.

Nevertheless, even if this legal interest is less evanescent than the economic one, a substantial respect for Principle no. 3 of the *Manifesto* does not automatically follow, especially when considering the actual all-crimes pattern. First of all, the punishment established by art. 648-*bis* c.p. (detention from four up to twelve years and fine from 5.000 up to 25.000 Euros) is undeniably not proportionate, considering that money laundering facts can result in a petty

[44] Arzt (1999), p. 758.
[45] Art. 648-*bis* c.p. has been forged by Decree Law no. 59 of 21 March 1978, bearing *Substantial and Procedural Rules for Prevention and Repression of Serious Crimes* (then converted into Law no. 191 of 18 Mai 1978, in G.U. no. 137 of 19 Mai 1978); § 261 StGB has been introduced by the *Law Against Illegal Drug Trafficking and Other Forms of Organized Crime* (1. OrgKG), of 22 July 1992, in BGBl. I, 1992, p. 1032.
[46] As far as concerns the *Isolierungstatbestand* (former § 261 Abs. 2 StGB), see *ex multis* BGH, Urt. v. 4. October 2010 – 1 StR 95/09, *NStZ* 2010, 517 = *NJW* 2010, 370, merely referring to the intention of the legislator when interpreting; BGH, Beschl. v. 23. April 2013 – 2 ARs 91/13; 2 AR 56/13, *NStZ-RR* 2013, 253 = *MMR* 2013, 674; BGH, Beschl. v 6. Juni 2018 – 1 ARs 163/18; 2 AR 106/18, Rn. 5.
[47] C. cost., sent. n. 302/2000.
[48] BVerfG, Urt. v. 30 März 2004 – 2 BvR 1520, 1521 = BVerfGE 110, 226 (251), *Geldwäsche durch Strafverteidiger*.
[49] Manes, Vittorio (2016c), p. 856; Lampe (1994), pp. 125 – 126.
[50] Bricola (1993), p. 38; Pedrazzi (1993), p. 654.
[51] In support of a different view, see Caeiro (2018), p. 282 ff.
[52] Except for the aggravating circumstance under art. 648-*bis*, par. 3, c.p. and for the autonomous provision of § 261 Abs. 4 StGB (*Qualifikationstatbestand*).
[53] Jahn (2020c), p. 663, Rn. 96.
[54] On this function Hassemer (1989a), p. 88).
[55] Dell'Osso (2017), p. 81 ff.
[56] Altenhain (2017), pp. 526 ff. (Rn 8 ff.).

offence or even a mere bagatelle. Secondly, the so-called *Isolierungstatbestand* under § 261 Abs. 1 Nr. 3 and 4 n.F. does not seem to "*respect* […] *a strict necessity-rule*", given that it explicitly criminalises neutral behaviours (obtention, custody and use of a tainted good)[57] in order to overcome evidentiary problems[58].

Lastly, as it will be shortly demonstrated, since the legal interest "administration of justice" may be filled up with several contents, it can foster and nurture the instrumental nature of the crime of money laundering.

2.3. *Principle no. 5.*

"*Every excessive usage of the punitive power goes beyond the principle of the 'bare minimum necessary' and therefore represents an arbitrary act of the State and, in the most serious cases, a crime. Institutions have the precise duty to assure the respect of the criminal offender, who can never be instrumentalized in the name of crime prevention*".

Not only do the criminal provision of *riciclaggio* and *Geldwäsche* allow the obtaining and exchange of financial information, but they also pave the way for the application of far-reaching and intrusive investigative measures, such as undercover investigations (art. 9, co. 1, lett. a Law no. 146 of 16 March 2006; § 110a StPO) telephone wiretapping (art. 266, par. 1, letter a) c.p.p.; § 100a, par. 2, no. 1, letter m StPO) and online searches (100b, par. 2, no. 1, letter l) StPO).

For this reason, as it has been pointed out by scholars in both legal systems, the criminalisation of money laundering displays a procedural instrumental nature[59] that may result in a violation of Principle 5 of the *Manifesto*.

Indeed, the suspect and/or the official charge of money laundering, on the one hand, allows law enforcement authorities to carry out investigations both on (alleged) predicate crimes[60] and on (alleged) laundering activities[61]. On the other hand, it may give rise to investigations that go *beyond* money laundering and its (alleged) predicate crimes, aiming at discovering and dismantling the criminal network possibly having organised the crimes[62].

This instrumentality of the suspect/official charge of money laundering clearly is useful and legit when law enforcement authorities are confronted with serious cases of money laundering, such as the (alleged) laundering of large amounts of money; the laundering of money (allegedly) deriving from serious crimes (both scenarios requiring a solid criminal network); the injection of copious quantities of laundered money in the financial system.

But one should always bear in mind that, nowadays, *any* crime can be a predicate crime of money laundering, not to mention the fact that § 261 subsection 6 StGB punishes negligent money laundering – *i.e.*, the fact of not realizing that a good has an illegal origin due to superficiality or carelessness[63] (a vivid example of an "*excessive usage of the punitive power*", in the words of the *Manifesto*). Therefore, the broadness of the investigative measures that it allows, combined with the system of information exchange, reveals the instrumentality of the money laundering criminal provision as a disproportionate tool for the control and repression of predicate crimes[64].

Indeed, German case law has faced this issue multiple times, due to the previously closed range of predicate crimes in § 261 StGB. In 2003, the *Bundesgerichtshof* (BGH) was confronted with defendants accused of money laundering and criminal conspiracy for smuggling, and thus wiretapped. At that time, however, on the one hand, smuggling was not included in the catalogue of crimes allowing wiretapping pursuant to § 100a StPO a.F. and, on the other hand, the evidentiary framework made it clear that the suspects had participated in the predicate offence and therefore (at that time) could not be charged for (self)money laundering as

[57] Salditt (1992), p. 125; Manes (2004a), p. 55.
[58] Bundesrat, *Draft of a Law Against Illegal Drug Trafficking and Other Forms of Organized Crime*, BT-Drs. 12/989 of 25 July 1991, p. 27.
[59] Jahn, Matthias (2019b), p. 1710, Rn. 5; Manes (2006b), p. 5230.
[60] Bernsmann (2009), p. 328.
[61] Barton (1993), p. 160.
[62] BT-Drs. 12/989 p. 21; Seminara (2000), p. 703.
[63] See for instance BGH, Beschl. v. 11. September 2014 – 4 StR 312/14, *NStZ-RR* 2015, 13. However, ever since BGH, Urt. v. 7. July 1997 – 1 StR 791/96, *JR* 1999, 76, 78 (=BGHSt 43, 158 (168)), when it comes to *Geldwäsche*, case law gives a "willfulness-close" interpretation of negligence.
[64] Brodowski (2021), p. 423.

well[65]. In 2020, the BVerfG affirmed that a domestic search[66] and a search at a lawyer's place[67] can only be justified by a so-called double suspect, which means a suspect concerning the money laundering *and* additionally a suspect concerning its possible predicate offence.

Lastly, the German legislator has acknowledged this problem and the underlying proportionality issues[68]. While transforming § 261 StGB in an all-crimes *Tatbestand*, the 2021 reform has established that law enforcement authorities can only proceed to wiretap in relation to cases of money if its predicate offence belongs to one of the "serious crimes" listed in § 100a Abs. 2 Nr. 1-11 StPO.

2.4. *Principle no. 11.*

"*The legal system has a main duty to clearly define any criminally relevant fact*. […]".

The principle of determinateness of criminal provisions is in danger to be denied when it comes to the crime of money laundering. The "war-against" attitude that led to the introduction and the further implementation of the offence of money laundering, as well as the adaptivity of the underlying criminal phenomenon (see *infra*, 2.5.) seem to legitimise a deliberate denial or an attenuation of the constitutionally relevant principle of determinateness, allowing case law to elastically interpret the constitutive elements of the crime.

As for Italy, the two alternative criminal conducts of "substitution" and "transfer" respect to a certain extent the principle of determinateness. "Substitution", the most ancient form of laundering, consists of the physical replacement of a tainted good with a "clean" one[69]; "transferring" means resorting to legal tools that translate property or possession of a good[70].

However, the third conduct, "perform other operations", somehow nullifies the (already scarce) level of determinateness of "substitution" and "transfer". Because of its broadness, it has been assimilated into a sort of residual general conduct[71] aiming at catching all the behaviours that are not to be subsumed under "substitution" or "transfer": for instance, a material, rather than legal, transfer[72], or even the mere hiding[73] of stolen goods.

Most importantly, all of these behaviours have to be committed "*in a manner that hampers the identification*" of the illicit provenance of the good. The majority of scholars interpret this requirement as an attribute of all three forms of conducts[74] that has to be judicially assessed *in concreto* on an individual base[75]. Nevertheless, case-law is not keen on ascertaining the actual fitness of the conduct to hamper the identification. In particular, *any* cash deposit in a bank is considered a "substitution" *ex se*, given the fungible nature of money[76]; and *any* banking operation aiming at interrupting the paper trail "hampers the identification", even if the operation was actually traceable[77].

As for Germany, one of the ambitions of the 2021 reform was to perform a "rationalisation and restructuring"[78] of the criminal conducts enshrined in § 261 StGB. Indeed, in 2008 the BGH sharply criticised such conducts, accusing them to be "barely understandable", con-

[65] BGH, Beschl. v. 26. Februar 2003 – 5 StR – 423/02, *NJW* 2003, 1880 (= BGHSt 48, 240). A similar case has been faced by OLG Hamburg, Beschl. v. 19 Juni 2002 – 3 Ws 70/02, *StV* 2002, 590.
[66] BVerfG, Beschl. v. 3. März 2021 – 2 BvR 1746/18, *NZWiSt* 2020, 276.
[67] BVerfG, Beschl. v. 31. Januar 2020 – 2 BvR 2992/14, *NStZ* 2020, 559 = *NJW* 2020, 1351.
[68] Ministry for Justice and Consumers' Protection (BMJV), *Draft of a Law for the Improvement of the Fight against Money Laundering via Criminal Law* of 11 August 2020 (BR-Drs. 620/20), p. 16 (Ref-E); Government of the German Federal Republic, *Draft of a Law for the Improvement of the Fight against Money Laundering via Criminal Law* of 9 November 2020 (BT-Drs. 19/24180), p. 17 (Reg-E).
[69] Galli (2019), p. 4727; Castaldo, R. and Naddeo, M. (2010), p. 120.
[70] Mantovani (2021), p. 293; Zanchetti (1997), p. 208.
[71] Cingari (2023), p. 399.
[72] Cass. pen., Sez. II, sent. n. 18577 del 24 gennaio 2003, in *Cass. pen.*, 2004, p. 3642; Cass. pen., Sez. II, sent. n. 11895 del 17 febbraio 2009 (dep. 18 marzo), *Verroggio*.
[73] Cass. pen., Sez. II, sent. n. 46754 del 26 settembre 2018 (dep. 15 ottobre), in *Cass. pen.*, 2018.
[74] Acquaroli (2015), p. 813; Della Ragione (2018), p. 101; Cass. pen., Sez. II, sent. n. 13448 del 13 febbraio 2005, *De Luca*, in *Cass. pen.*, 2006, p. 1822. According to Plantamura (2009), p. 182, however, the modal clause "*in a manner that hampers the identification*" only refers to the conduct of performing "*other operations*".
[75] Manes (2004a), pp. 54-55; Seminara (2000), p. 267.
[76] Cass. pen., sent. del 5 aprile 1986, *Ghezzi*, in *Giur. it.*, 1988; Cass. pen., Sez. II, sent. n. 52549 del 17 novembre 2017; Cass. pen., Sez. VI, sent. n. 13085 del 3 ottobre 2013; Cass. pen., Sez. II, sent. n. 5972 del 22 gennaio 2013 (dep. 7 febbraio), in *St. iuris*, 2013, p. 1047. For recent developments on bitcoins in the Italian case law see Vadalà (2021), p. 2224 ff.
[77] *Ex multis*, Cass. pen., Sez. II, sent. n. 32936 del 13 luglio 2012, *Papale*; Cass. pen., Sez. II, sent. n. 46319 del 21 settembre 2016.
[78] Reg-E, p. 31.

stantly overlapping and so broad that "almost every interaction with an ill-gotten good" had become criminally relevant[79].

Nevertheless, even after 2021, not only does the *Gesetzessystematik* of § 261 StGB remains unaltered, but also the changes that occurred to the conducts are so mild that it can still be said that § 261 StGB is an "open-crime *Tatbestand*"[80] aiming at catching all forms of contact with tainted goods, irrespective precisely of the principle of determinateness of criminal provisions. Indeed, the newly shaped behaviour of *hiding* the ill-gotten good ("*verbergen*", § 261 Abs. 1 Nr. 1), which consists in concealing or displacing the good, subtracting it to the law enforcement radars, may overlap with the newest behaviour of "*substituting, transferring, moving*" ("*umtauschen*, *übertragen*, *verbringen*", § 261 Abs. 1 Nr. 2) of the proceeds in order to avoid their recovery or confiscation. However, these new conducts themselves may overlap with the new Abs. 2 (see *infra*) and/or may result in one of the conducts of the so-called *Isolierungstatbestand*[81].

A further problem in respect of the principle of determinateness under Art. 103 Abs. 2 GG is also the all-new behaviour of § 261 Abs. 2 StGB. Although it criminalises a core-behaviour of laundering, namely concealment and disguise ("*verheimlichen*; *verschleiern*"), this conduct is no longer referred to criminal proceeds and/or their provenance, but to "*elements*" ("*Tatsachen*"), that "*may be useful for the discovery, the confiscation, or the investigations on the paper tail*" of the proceeds themselves[82].

2.5. *Principle no. 15.*

"*Criminal legislation has to be based on criminological data that are reliable and accepted by the scientific community. The worthiness of a more severe punishment has to be grounded in proportionated and criminologically corroborated interests*".

When it comes to money laundering, criminological studies on its empirical dimension appear to be particularly necessary. Indeed, the multi-faceted, adaptive and chameleon-like nature of the criminal phenomenon of money laundering challenges both the ability of the criminal provision to crystallise its actual harmfulness (*Unrecht*) and the aptitude of the preventive regulation to effectively intercept laundering activities.

If the conceptual *description* of money laundering as a three-stage process made of "placement, layering and integration" seems to have achieved a certain level of solidity in the scientific community, the same cannot be said as far as regards its *quantification*.

The constant asymmetry between the annual number of STRs and the number of convictions for money laundering[83] sheds a light on the seriousness of the dark figure of crime rate. Also, despite the importance of criminological data, as stated by *Manifesto*'s Principle no. 15, the scientific community still lacks a common yardstick and a fully endorsed method for measuring the *quantum* of laundered money on a national and/or international scale[84]. In 1994, the IMF estimated that the global sum of laundered money amounted to between 2 and 5 percentage points of global GDP[85]. Further evaluations do not sensibly differ from this esteem: according to the UNODC, in 2009 the global amount of laundered money was "probably" up to 1,6 trillion US dollars[86]; in 2011, it is said to be between 800 billion and 3 trillion, although "it is difficult to estimate the total amount of money that goes through the

[79] BGH, Urt. v. 24 Juni 2008 – 5 StR 89/08, *JR* 2008, 478 = *NJW* 2008, 2156 (2157).
[80] See Jahn (2019b), p. 1721 Rn. 42.
[81] Altenhain, K. and Fleckenstein, L. (2020), p. 1050. Because of these risks of overlapping, it is preferrable to interpret the new § 261 Abs. 1 Nr. 2 StGB as a crime of concrete, rather than abstract, danger: Gercke *et al.* (2021), p. 337.
[82] In order to counterbalance the vagueness and broadness of this *Tatbestand*, some scholars propose to interpret it as a crime of concrete danger requiring the additional element of the risk for the deviation of investigations, on the model of the crime of false allegations under § 164 StGB: Gercke *et al.* (2021), p. 337.
[83] In its 2022 *Annual Report*, the German FIUs states that, in 2021, the number of STRs concerning money laundering was 295.324 (99% of 298.507 STRs in total), whereas the overall number of convictions amounted to 103. As for Italy, in 2019 the FIU had to deal with 104.933 money laundering-related STR (out of 105.798 STRs) and the number of convictions was 475 (this data is taken from the document "Analysis of Legislative Impact" annexed to the Draft of Legislative Decree no. 159/2021, p. 7-9). In 2021, the FIUs Annual Report states that the number of STRs concerning *riciclaggio* amounted to 138.936 (99, 6% of 139.524); we do not dispose of judiciary statistics concerning 2021.
[84] Van Duyne *et al.* (2018), p. 121 and p. 132.
[85] IMF (1994), as critically reported by Quirk (1996), p. 26.
[86] UNODC (25 October 2011),

laundering cycle"[87].

In this situation, policymakers and stakeholders only seem to be able to conduct *ex-post* identifications of vulnerable businesses, social activities and/or geographical areas[88], with a view to deciphering "typologies" or rather "methods and trends" of money laundering[89].

National legislators, for their part, chase a questionable idea of "effectiveness" and react by increasing the possibilities of crime detection: meaning both the tightening of the business requirements and the broadening of criminal provisions' scope. Whether this also justifies the forging of all-crimes offences, however, is not straightforward: the main consequence of such a normative implementation is that, by sheer mathematics, everybody becomes a money launderer, sooner or later – which means, nobody really is[90].

3. Conclusions.

The crime of money laundering is a perfect example of the modern shift of penal law from a liberal to a security paradigm[91].

Indeed, both *riciclaggio* and *Geldwäsche* were introduced in times of emergency due to the need to counter the newest worrisome criminal phenomenon, *i.e.*, organized crime. This justified the structure of art. 648-*bis* c.p. and § 261 StGB as serious crimes, based on the previous commission of a determined and serious offence.

Despite the official rationale of a campaign (in fact, a war) against economic organized crime and terrorism financing, with the passing of time, the shape of the provisions began to expand and their harmfulness became less and less specific. Simultaneously, the intersections with the administrative-preventive system gained greater importance and the flow of financial information developed into a valuable asset in the fight against all sorts of crimes. To the extent that, bearing in mind the crime of self-laundering too, one may paraphrase what has been said about embezzlement[92] and declare: "*Geldwäsche geht immer*"! Therefore, the crime of money laundering offers a privileged viewpoint to continue watching over and advocating for the precarious relationship between the punitive system, freedom and guarantees.

Look out, closely, for what comes next.

Bibliography

Acquaroli, Roberto (2015): "Il riciclaggio", in Piergallini, Carlo and Viganò, Francesco (a cura di): *Reati contro la persona e contro il patrimonio*, in Palazzo, Francesco and Paliero, Carlo Enrico, *Trattato di diritto penale*, vol. VII (Torino, Giappichelli), pp. 805-835.

Alldridge, Peter (2001): "The Moral Limits of the Crime of Money Laundering", *Buffalo Criminal Law Review*, 5, pp. 279-319.

Altenhain, Karsten (2017): "§ 261 – Geldwäsche; Verschleierung unrechtsmäßig erlangter Vermögenswerte", in: Kindhäuser, Urs, Neumann, Ulfrid, Paeffgen, Hans-Ullrich, and Saliger, Franz (Hrsg.): *Strafgesetzbuch: StGB*, 5. Aufl. (Nomos, Baden-Baden), pp. 516-587.

Altenhain, Karsten and Fleckenstein, Lennart (2020): "Der Gesetzentwurf zur Neufassung des § 261 StGB", *JuristenZeitung*, 21, pp. 1045-1051.

[87] UNODC (2011).
[88] See the study of the German Minster for Finance, *First National Risk Analysis – Fight against Money Laundering and Terrorism Financing*, 10 October 2019, based on the analysis of Bussmann, K.-D. and Vockrodt, M. (2016), p. 138.
[89] Following the creation, in 2016, of a *Working Group on Risks, Trends and Methods* within the FATF, its empirical reports and case studies that used to be called "*Typology Reports*" now go under the name of "*Methods and Trends*".
[90] Fischer (2021), p. 114.
[91] On the topic of security in criminal law from a global perspective see the recent work of Nieto Martín (2022), p. 49.
[92] Ransiek (2004), p. 634.

Arzt, Gunther (1999): "Wissenschaftsbedarf nach dem 6. StrRG", *Zeitschrift für die gesamte Strafrechtswissenschaft,* 4, pp. 757 -784.

Bäcker, Matthias and Burchard, Christoph (Hrsg.) (2022): *Strafverfassungsrecht* (Tübingen, Mohr Siebeck).

Bartoli, Roberto (2022): *Introduzione al diritto penale tra violenza e costituzionalismo* (Torino, Giappichelli).

Barton, Stephan (1993): "Sozial übliche Geschäftstätigkeit und Geldwäsche (§ 261 StGB)", *Strafverteidiger*, 3, pp. 156-163.

Bernsmann, Kai (2009): "Im Zweifel: Geldwäsche?", in Böse, Martin and Sternberg-Lieben, Detlev (Hrsg.): *Grundlagen des Straf- und Verfahrensstrafrecht. Festschrift für Knut Amelung zum 70. Geburtstag* (Berlin, Duncker & Humblot), pp. 318-392.

Bricola, Franco (1993): "Il diritto penale del mercato finanziario", in Aa. Vv.: *Mercato finanziario e disciplina penale* (Milano, Giuffrè), pp. 27-47.

Brodowski, Dominik (2021): "Tue Böses und rede darüber – Geldwäscheverdachtsmeldungen und das Strafrecht", *Zeitschrift für Wirtschafts- und Steuerstrafrecht*, 11, pp. 417-424.

Burchard, Christoph (2016): "Strafverfassungsrecht – Vorüberlegungen zu einem Schlüsselbegriff", in Burchard, Christoph, Tiedemann, Klaus, Sieber, Ulrich, Satzger, Helmut, and Brodowski, Dominik (Hrsg.): *Die Verfassung moderner Strafrechtspflege. Erinnerung an Joachim Vogel* (Baden-Baden, Nomos), pp. 27-61.

Bussmann, Kai-D. and Veljovic, Manuel (2020): "Die hybride strafrechtliche Verfolgung der Geldwäsche – Schlussfolgerungen aus den Ergebnissen einer bundesweiten Studie", *Neue Zeitschrift für Wirtschafts-, Steuer, und Unternehmensstrafrecht*, 11, pp. 417-425.

Bussmann, Kai-D. and Vockrodt, Marcel (2016): "Geldwäsche-Compliance im Nicht-Finanzsektor: Ergebnisse aus einer Dunkelfeldstudie", *Compliance Berater*, 5, pp. 138-143 (also available in English via wcms.itz.uni-halle.de).

Caeiro, Pedro (2018): "Contra uma política criminal "à flor da pele": a autonomia do branqueamento *punível* em face do branqueamento *proibido*", in De Faria Costa, José, Rodrigues, Anabela Miranda, Jolo Antines, Maria, Mónez, Maria, Brandao, Nuno and Fidalgo, Sonia (org.): *Estudios de Homenagem ao Prof. Doutor Manuel da Costa Andrade*, vol. I (Univesidade de Coimbra, Coimbra), pp. 267-301.

Castaldo, Andrea R. – Naddeo, Marco (2010): *Il denaro sporco. Prevenzione e repressione nella lotta al riciclaggio* (Cedam, Padova).

Cingari, Francesco (2023): "I delitti contro la circolazione illecita dei beni", in Cingari, Francesco, Papa, Michele, Vallini, Antonio: *Lezioni di diritto penale, parte speciale. Delitti contro il patrimonio*, pp. 385-413.

Galli, Martina (2019): "Art. 648-*bis*", in Padovani, Tullio (a cura di): *Codice penale* (Milano, Giuffrè), tomo I, pp. 4724-4738.

Dell'Osso, Alain Maria (2017): *Riciclaggio di proventi illeciti e sistema penale* (Giappichelli, Torino).

Della Ragione, Luca (2018): "La struttura della fattispecie", in Della Ragione, Luca and Maiello, Vincenzo (a cura di): *Riciclaggio e reati nella gestione dei flussi di denaro sporco* (Giuffrè, Milano), pp. 56-199.

Donini, Massimo (2012): "L'eredità di Bricola e il costituzionalismo penale come metodo. Radici nazionali e sviluppi sovranazionali", *Diritto penale contemporaneo – Rivista trimestrale*, 2, pp. 51-74.

Fatf/Gafi (19 February 2010): "Mutual Evaluation Report – Anti-Money Laundering and Combating the Financing of Terrorism: Germany", in www.fatf-gafi.org (Paris).

Findeisen, Michael (1997): "Der Präventionsgedanke im Geldwäschegesetz", *Zeitschrift für Wirtschafts- und Steuerstrafrecht*, 4, pp. 121-128.

Fischer, Thomas (2021): "Ein Volk von Geldwäschern", *Journal der Juristischen Zeitgeschichte*, pp. 114-116.

FIU (12 September 2022): "Jahresbericht 2021", in www.zoll.de (Bonn).

Gianfelici, Folco and Siena, Fabio Antonio (2021), "Il *legal framework* europeo di contrasto al riciclaggio verso una svolta? Problemi attuali e prospettive di una revisione organica", 2, *Giurisprudenza penale web*, pp. 1-30.

Gercke, Björn, Jahn, Matthias and Paul, Theresa (2021): "Sorgenkind außer Kontrolle: Paradigmenwechsel der Geldwäsche Bekämpfung mit der Neufassung des § 261 StGB", *Strafverteidiger*, 5, pp. 330-340.

Hassemer, Winfried (1989a): "Grundlinien einer personalen Rechtsgutslehre", in: Philipps, Lothar, and Scholler, Heinrich (Hrsg.): *Jenseits des Funktionalismus. Arthur Kaufmann zum 65. Geburtstag* (Heidelberg, Decker & Müller), pp. 85-94.

Hassemer, Winfried (2005b): "Frankfurter Profile", *Kritische Justiz*, pp. 2-16.

Hassemer, Winfried, Lüderssen, Klaus and Naucke, Wolfgang (Hrsg.) (1979a): *Hauptprobleme der Generalprävention* (Frankfurt am Main, Metzner Verlag).

Hassemer, Winfried, Lüderssen, Klaus and Naucke, Wolfgang (Hrsg.) (1983b): *Fortschritte im Strafrecht durch die Sozialwissenschaften?* (Heidelberg, C.F. Müller).

Hecker, Bernd (2019): "Geldwäsche; Verschleierung unrechtsmäßig erlangter Vermögenswerte (§ 261)", in Schönke, Adolf and Schröder, Horst (Hrsg.): *Strafgesetzbuch. Kommentar*, 30. Aufl. (München, C.H. Beck), pp. 2563-2577.

Institut für Kriminalwissenschaften Frankfurt (1995a): *Vom unmöglichen Zustand des Strafrechts* (Berlin, Peter Lang Verlag).

Institut für Kriminalwissenschaften Frankfurt (1999b): *Irrwege der Strafgesetzgebung*, (Berlin, Peter Lang Verlag).

Institut für Kriminalwissenschaften Frankfurt (2007c): *Jenseits des rechtsstaatlichen Strafrechts* (Berlin, Peter Lang Verlag).

International Monetary Fund (1994), "International Monetary Statistics".

Jahn, Matthias (2016a): "Strafverfassungsrecht: Das Grundgesetz als Herausforderung für die Dogmatik des Straf- und Strafverfahrensrechts", in Burchard, Christoph, Tiedemann, Klaus, Sieber, Ulrich, Satzger, Helmut, and Brodowski, Dominik (Hrsg.): *Die Verfassung moderner Strafrechtsplege. Erinnerung an Joachim Vogel* (Baden-Baden, Nomos), pp. 63-86.

Jahn, Matthias (2019b): "Geldwäsche; Verschleierung unrechtsmäßig erlangter Vermögenswerte (§ 261)", in Satzger, Helmut, Schluckebier, Wilhelm, and Widmaier, Gunter (Hrsg.): *StGB – Strafgesetzbuchkommentar*, 5. Aufl., (Köln, Carl Heymanns Verlag), pp. 1702-1735.

Jahn, Matthias (2020c): "§ 39 Geldwäsche", in Hilgendorf, Erich, Kudlich, Hans and Valerius, Brian (Hrsg.): *Handbuch des Strafrechts – Besonderer Teil II*, Bd. 5 (Heidelberg, C. F. Müller), pp. 663-726.

Jahn, Matthias (2022d): *Diskussion um Reform der Strafprozessordnung*: *Magna Charta statt "Pizza mit Allem"*, in www.lto.de.

Jahn, Matthias (2022e): "Die Gesamtreform des deutschen Strafverfahrens – Bedeutung, Bedingungen, Befunde", *Strafverteidiger*, 9, pp. 594-600.

Jahn, Matthias and Ziemann, Sascha (2014): "Die Frankfurter Schule des Strafrechts: Versuch einer Zwischenbilanz", *JuristenZeitung,* 19, pp. 943-947.

Kuhlen, Lothar (2023): "Gibt es eine Frankfurter Schule der Strafrechtswissenschaft?", in Brunhöber, Beatrice, Burchard, Christoph, Günther, Klaus, Jahn, Matthias, Jasch, Michael, Silva-Sánchez, Jesús-Maria and Singelstein, Tobias (Hrsg.): *Risikostrafrecht und Strafrecht als Risiko. Festschrift für Cornelius Prittwitz zum 70. Geburtstag* (Baden-Baden, Nomos Verlag), pp. 131-147.

Lampe, Ernst-Joachim (1994): "Der neue Tatbestand der Geldwäsche (§ 261 StGB)", *JuristenZeitung*, 3, pp. 123-132.

Lüderssen, Klaus (2010), in Hilgendorf, Eric (Hrsg.): *Die deutschsprachige Strafrechtswissenschaft in Selbstdarstellungen* (Berlin, De Gruyter), pp. 349-387.

Manes, Vittorio (2004a): "Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale", *Rivista trimestrale di diritto penale dell'economia*, 1-2, pp. 35-80.

Manes, Vittorio (2006b): "voce Riciclaggio e reimpiego dei proventi illeciti", in: Cassese, Sabino (a cura di): *Dizionario di diritto pubblico* (Milano, Giuffrè), pp. 5226-5237.

Manes, Vittorio (2016c): "Riciclaggio (art. 648-*bis* c.p)" in Canestrari, Stefano, Cornacchia, Luigi, Gamberini, Alessandro, Manes, Vittorio, Mantovani, Marco, Mazzacuva, Nicola, Sgubbi, Filippo, Stortoni, Luigi, and Tagliarini, Francesco (a cura di): *Diritto penale. Lineamenti di parte speciale*, (Bologna, Monduzzi Editoriale), pp. 852-867.

Mantovani, Ferrando (2021): *Diritto penale. Parte speciale II: delitti contro il patrimonio* (Milano, Wolters Kluwer), pp. 272-306.

Melchionda, Alessando (2022), "Il nuovo assetto normativo per la "lotta al riciclaggio mediante il diritto penale"", *Archivio penale*, 2, pp. 1-33.

Naucke, Wolfgang (2010), in Hilgendorf, Eric (Hrsg.): *Die deutschsprachige Strafrechtswissenschaft in Selbstdarstellungen* (Berlin, De Gruyter), pp. 417-446.

Nieto Martín, Adán (2022): *Global Criminal Law: Postnational Criminal Justice in the Twenty-First Century* (London, Palgrave Macmillan).

Pedrazzi, Cesare (1993): "voce Mercati finanziari (disciplina penale)", *Digesto delle discipline penalistiche*, (Utet, Torino), vol. VII, pp. 652-665.

Pieth, Mark (1999): "The Harmonization of Law against Economic Crime", *European Journal of Law Reform*, 4, pp. 527-545.

Plantamura, Vito (2009): "Tipo d'autore o bene giuridico per l'interpretazione, e la riforma, del delitto di riciclaggio?", *Rivista trimestrale di diritto penale dell'economia*, 1-2, p. 161-192.

Quirk, Peter J. (1996): "Macroeconomic Implications of Money Laundering", *International Monetary Fund Working Paper*, 66, pp. 1-42.

Ransiek, Andrea (2004): "Risiko, Pflichtwidrigkeit und Vermögensnachteil bei der Untreue", *Zeitschrift für die gesamte Strafrechtswissenschaft,* 116, pp. 634-679.

Salditt, Franz (1992): "Der Tatbestand der Geldwäsche", *Strafverteidiger-Forum*, pp. 121-136.

Seminara, Sergio (2000): "L'impresa e il mercato", in Pedrazzi, Cesare, Alessandri, Alberto, Foffani, Luigi, Seminara, Sergio, Spagnolo, Giuseppe (a cura di): *Manuale di diritto penale dell'impresa* (Bologna, Monduzzi Editoriale), pp. 702-714.

Stessens, Guy (2001): *Money Laundering: A New International Law Enforcement Model* (Cambridge, Cambridge University Press).

Unione delle Camere penali italiane (2019): "Manifesto del diritto penale e del giusto processo", in www.camerepenali.it.

United Nations, Office on Drugs and Crime (25 October 2011): "Press Release".

United Nations, Office on Drugs and Crime (2011): "Money Laundering Overview", in www.unodc.org.

VAdalà, Rosa Maria (2021), "La dimensione finanziaria delle valute virtuali. Profili assiologici di tutela penale", *Giurisprudenza italiana*, 10, pp. 2225-2231.

Van Duyne, Petrus C., Harvey, Jackie H., Gelemerova, Liliya Y. (2018): *The Critical Handbook on Money Laundering. Policy, Analysis and Myths* (London, Palgrave McMillan).

Vogel, Benjamin and Maillart, Jean-Baptiste (Eds.) (2020): *National and International Anti-Money Laundering. Law. Developing the Architecture of Criminal Justice, Regulation and Data Protection* (Cambridge, Intersentia).

Zanchetti, Mario (1997): *Il riciclaggio di denaro proveniente da reato* (Milano, Giuffrè).

"Gimme Shelter": The Right to Silence for Silenced Migrant Victims*

"Gimme Shelter": il diritto al silenzio per le vittime migranti silenziate

"Gimme Shelter": el derecho al silencio por las víctimas migrantes silenciadas

Sara Bianca Taverriti
Assegnista di ricerca in diritto penale presso l'Università degli Studi di Milano
sara.taverriti@unimi.it

Immigration, Privilege against Self-Incrimination and Right to Silence, Fundamental Rights

Immigrazione, Diritto a non autoincriminarsi e diritto al silenzio, Diritti fondamentali

Inmigración, Derecho a no autoincriminarse y derecho a guardar silencio, Derechos fundamentales

Abstracts

This paper aims at addressing the issue of access to justice for victims of crimes with an irregular migration status. One of the prominent side effects of punishing irregular migration is the substantial exclusion of these individuals from the circuit of the criminal justice system, as they fear being tried or ordered to leave the country after approaching the police. The article draws on the similarities between the condition of victims with an irregular migration status and the "cruel trilemma" of the defendant forced to choose between maintaining his silence and being held in contempt of court; lying and thereby perjuring, or incriminating himself. Thus, the paper questions whether the *nemo tenetur se detegere* principle can be used to protect these victims. After reviewing a series of remedies and reliefs that somehow protect the right to silence of the migrant victim, the paper shows discriminations that are still affecting these individuals and it proposes to extend the scope of application of this guarantee, originally conceived for the defendant.

L'articolo affronta il tema dell'accesso alla giustizia penale per le vittime di reato con status migratorio irregolare. Uno dei prominenti effetti collaterali derivanti dalla criminalizzazione dell'immigrazione irregolare è la sostanziale esclusione di questi individui dal circuito del sistema giudiziario penale, dal momento che gli stessi temono di essere sottoposti a processo o comunque espulsi dal territorio statale a seguito del contatto con le forze di polizia. Il lavoro prende le mosse dalle somiglianze tra la condizione della vittima migrante irregolare e il c.d. *"cruel trilemma"* che avvince l'indagato/imputato nell'ardua scelta tra tacere, dichiarare il falso alle autorità o autoincriminarsi. L'A. si domanda quindi se sia possibile che il principio del *nemo tenetur se detegere* possa essere utilizzato per fornire protezione a queste vittime. Dopo aver preso in considerazione una serie di strumenti (domestici e non) che offrono protezione e rimedio a queste situazioni, anche attraverso la tutela del diritto al silenzio delle vittime, l'articolo propone l'estensione del campo di applicazione di questa garanzia (originariamente concepita in favore dell'indagato/imputato) anche a questi soggetti, in ragione dell'insufficienza dei meccanismi di tutela e delle perduranti discriminazioni gravanti sulle vittime migranti irregolari.

El artìculo tiene por objeto la cuestión del acceso a la justicia de las víctimas extranjeras en situación irregular. Uno de los principales efectos colateral de castigar la inmigración irregular es la exclusión sustancial de estas personas del circuito del sistema de justicia penal, ya que temen ser procesadas o expulsadas del territorio tras el contacto con la policía. El artìculo se basa en las similitudes entre la condición de las víctimas extranjeras irregulares y el *"cruel trilemma"* del acusado obligado a elegir entre mantener su silencio, cometer perjurio, o declarar contra sí mismo. Se analiza entonces si el principio *nemo tenetur se detegere* puede usarse para proteger a estas víctimas. Después de revisar una serie de instrumentos juridicos y mecanismos que, de una u otra forma, protegen el derecho al silencio de la víctima migrante, el artículo muestra discriminaciones que aún afectan a estas personas y propone ampliar el ámbito de aplicación de esta garantía, originalmente concebido para el acusado.

[*] This paper constitutes the extended version of the presentation given at the *X AIDP International Symposium for Young Penalists – Criminal Justice in the Prism of Human Rights*, held at the University of Bologna on 27-28 October 2022, and it builds on previous research conducted within the scope of the international project *"Safe reporting" of crime for victims and witnesses with irregular migration status in the USA and Europe* (August 2018 – October 2019), funded by the University of Oxford and coordinated by the Center on Migration, Policy and Society. Further research on the topic is currently ongoing within the framework of the project *VISA RoC - Victims with Irregular migration Status' sAfe Reporting of Crimes* (JUST-2021-JACC) co-funded by the EU Commission.

Sommario

1. Introduction.

Over the last decades, the distance between criminal law and immigration law is somehow blurring as in most countries violations of immigration law are criminally prosecuted or, however, subject to administrative procedures of removal. One of the prominent side effects of punishing irregular migration is the substantial exclusion of these individuals from the circuit of the criminal justice system. In fact, as irregular migrants could be tried or ordered to leave the country after their identification, they are often disinclined to report crimes they have suffered or witnessed because they fear approaching the police. Therefore, part of the population is left not only unprotected but also more exposed to victimisation as these people become the favourite prey of offenders who can rely on the silence of these victims.

This paper addresses the issue of these migrant victims left unprotected taking into consideration the Italian legal system as the main field of observation, and drawing on human rights – and, in particular, the right to access justice for victims of crimes and the 'right to silence' and its derivative guarantees – as tools of a possible solution to it.

The paper is articulated as follows. First, it will reframe the issue of migrant victimization (and related crime underreporting) from a criminological and victimological perspective. Subsequently, it will delve into the legislation and practice of the Italian Legal system, analysing rules governing crime reporting and immigration enforcement processes, and their interlinks. Then, we will move to the main suggestion of the article which is the possibility of recognizing protection for victims with an irregular migration status building on the *nemo tenetur se detegere principle*, which is originally conceived to protect the defendant within the scope of the criminal proceeding. Then we will analyse a series of remedies and reliefs provided to this kind of victims that evoke the same *rationale* of the right to remain silent, taking into account not only the Italian legal system but also solutions offered in other countries. Subsequently, we will identify obstacles and limits that made these measures insufficient to protect victims' right to access the criminal justice system and we will propose a different approach to the problem that suggests further solutions.

2. Silenced migrant victims.

With migration flows becoming an ever-more topical issue in the Western world, irregular migration has significantly drawn the attention of criminal lawyers and criminologists in Europe and North America. Several studies looked at irregular migration under the lens of criminal law, including "crimmigration"[1] studies analyzing irregular migration as a crime in itself (in those countries, as in Italy, where irregular entry or stay is penalized), and the countless studies that tried to confirm or bust the myth that depicts migrants (and particularly those with irregular status[2]) as more prone than natives to carry out a crime[3]. In return, the same

[1] Term coined by Juliet P. Stumpf (2006), p. 367 ff.; Sklansky (2012), pp. 157 ff.; Garcìa Hernàndez (2017). On the roots of this tendency see also Garland (2001); Simon (2007). The phenomenon of Crimmigration is also extending to other collateral political strategies, like the provision of immigration law consequences for criminal convictions, and the deprivation or limitation of personal freedom in immigration law enforcement, the criminalisation of rescue operation by NGOs; for a wide perspective on the European state of the art see, Gatta *et al.* (2021), Curi *et al.* (2020).

[2] Including individuals who have either entered the country without proper authorization, breaching immigration rules (irregular entrants), or who entered in compliance with such laws, but subsequently did not comply with the conditions of their stay (i.e. overstayers: migrants who have stayed in the country beyond the expiration of their visas 'overstayers'; migrants who have lost their regular status following other events, like divorce, the refusal of an asylum application, the loss of regular employment).

[3] On the nexus between immigration and crime rates see Bernat (2017); Jacob I. Stowell *et al.* (2009), p. 889; Martinez *et al.* (2010), 797;

level of attention has not been given to the other side of the medal, the one that sees migrants as victims (or witnesses) rather than authors of crimes.

This article aims to fill this gap by focusing on irregular migrants as victims of crime, to analyze how the law may offer victims with irregular migration status an opportunity to report a crime or, conversely, get in these victims' way to interact with law enforcement authorities. In fact, among the various factors that may discourage migrants from reporting crime, criminal and immigration legislation play a determinant role in establishing a nexus between one's immigration status, victimization and inclination to report the crime. Irregular migrant victims' interactions with law enforcement authorities to seek protection may *de facto* be prevented by legislation that prioritizes sanctioning them with deportation (or even criminal charges) over the need of ensuring their protection and access to justice.

2.1. *From 'crimmigration' to 'victimigration'.*

Understanding how being a migrant can itself be a source of vulnerability – and, in particular, how having irregular status increases the level of vulnerability – remains largely unexamined. Studies analyzing migrants' victimization tend to be limited to specific national contexts or specific criminal activities, such as trafficking and smuggling of human beings or labour exploitation[4]. Yet, as we shall see, some studies did flag that there is a clear correlation between one's condition as a migrant, particularly if irregular, and an increased vulnerability to victimization to (any kind of) crime. Some studies in victimology gave this issue greater attention and explored the factors making migrants more exposed to crime than nationals.

Ezzat Fattah (1991) sketched a profile of typical migrant victims: often male, young, unmarried, unemployed or day workers; easily recognizable as belonging to a certain minority based on ethnicity; and usually living in suburbs or 'skid-rows'.[5] In this scenario, migrants are depicted as 'convenient scapegoat[s]'[6] for society, which does not perceive them as fully-fledged members of the community, with the public being more insensitive and less indignant when the victim is a foreigner, due to lack of empathy[7]. As a result, there are several factors influencing migrants' victimization, including: language and cultural barriers; migrants lacking time and economic support to invest in criminal proceedings; migrants lacking experience and, as minorities, suffering discrimination; lack of knowledge of the legislation of the host country, social isolation, and psychological and cultural barriers which contribute to discouraging interactions with the police[8] .

Irregular migrants may be even more prone to victimization than other foreign nationals. It has been long shown that irregular migrants are strongly deterred from seeking services or reporting crime due to the fear that contacting the authorities would inevitably lead to the detection of their irregular status and, subsequently, their deportation.[9] Irregular status and the related reluctance to report crimes exacerbate migrants' vulnerability, enhancing the chances that criminals will perpetrate offences against them. Studies in the US found, for example, that Latino migrants have been targeted by robbers because their ethnicity made them 'visually identifiable' to criminals who assumed Latinos would have irregular status, and therefore would not report crimes.[10] According to a study conducted in Italy[11] focused on immigrant victims of ordinary crimes, in addition to common factors influencing migrants' victimisation, there are several factors that may further enhance their vulnerability, like: recent

Crocitti (2014). See Sampson (2008), p. 28 ff.; Rumbaut and Ewing (2007). A recent synthesis of the empirical facts on immigration and crime, with a special focus on incarceration Fasani *et al.* (2019).

[4] FRA, *Severe labour exploitation – Workers moving within or into the European Union* (Publications Office of the EU 2015), in fra.europa.eu, accessed 31 march 2023; FRA, *Protecting migrants in an irregular situation from labour exploitation – Role of the Employers Sanctions Directive* (Publications Office of the EU 2021), in fra.europa.eu, accessed 31 march 2023; Chudžíková and Bargerová (2018).

[5] Fattah (1991).

[6] Kelsey (1926), pp. 165 ff.

[7] Von Hentig (1948), pp. 414 f.

[8] See Capuano (2011); Reina *et al.*, (2014), pp. 593 ff.; Messing *et al.* (2015), pp. 328 ff.

[9] Kittrie (2006), pp. 1449 ff.; Rodrigues *et al* (2018); Reina *et al.* (2014), pp. 593–615; Messing *et al.* (2015), pp. 328–340; Gleeson (2018), pp. 561 ff.; PICUM, *Guide to the EU victims' directive: advancing access to protection, services and justice for undocumented migrants*, (Brussels 2015) <picum.org/wp-content/uploads/2017/11/VictimsDirectiveGuide_Justice_EN.pdf>.

[10] See Delvino and González Beilfuss (2021), pp. 1 ss.; Barranco and Shihadeh (2015), pp. 440.

[11] See Capuano (2011).

arrival; being undocumented; being unemployed; being single; being a person of colour; being female (possibly); coming from Sub-Saharan Africa; living in degraded areas, and having poor knowledge of the language.

2.2. *Underreporting and the dark figure of crime against migrants.*

Moreover, crime against migrants with irregular status is difficult to measure for a number of reasons: measuring crime rates, in general, is a difficult task and commonly presents challenges in criminology, due both to limitations in research methods and to the general difficulty of capturing the reality of social phenomena like criminality.[12] For irregular migrants, this task is even harder, as estimating accurately their actual number is particularly challenging, due to this group's 'invisibility' to public administrations.

The dark figure of crime against irregular migrants is likely higher than any known figure since a significant number of crimes go unreported (and thus undetected) due to irregular migrants' fear of self-incrimination and deportation.[13] In addition, cultural gaps might lead foreign victims to disregard criminal action, when they see this as a natural behaviour within their cultural background despite it being a punishable offence in the country where they live. Migrants might also be reluctant to report crimes when the offender is a member of the family or if he/she comes from the same ethnic or national background.[14]

Concerning the situation in Italy, the Italian National Institute of Statistics (ISTAT) produced data on crimes against all foreign nationals, including those regularly or irregularly present in the national territory. According to a 2017 ISTAT report on Criminality, victims were foreign citizens (including non-residents) in one-fifth of crimes reported in Italy, but the percentage was dramatically higher for violent offences than offences against property. Proportionally, foreigners were more exposed to criminal offences than Italians.[15] Previous studies had shown that immigrants are more likely to suffer crimes committed by nationals of their own countries of origin rather than by Italian nationals and that crimes are more frequent within the same national group than between different groups[16]. According to ISTAT, in Italy, foreign nationals are victims of :20% of voluntary manslaughters/murders, 30% of attempted murders, 30% of sexual assaults, 14% of incidences of stalking, 23% of criminal injuries, 14% of threats, 12% of insults, 18% of thefts, 16% of muggings, and 20% of robberies.[17] In addition to common crimes, migrants tend to be victims of specific crimes like hate crimes, xenophobic assault, smuggling, trafficking of human beings and organs, modern slavery, debt bondage, exploitation of begging, and exploitation to commit other crimes.[18]

[12] Constant variations in criminal legislation; the discretion retained by police officers in recording crimes; the disinclination of some victims to report crimes; and the interest of criminal organizations in covering up illegal trafficking, are just some of the factors leading to misrepresentations in statistics based on crime reporting data. The problem is so structurally embedded that criminologists developed the concept of a 'dark figure of crime' in an effort to identify the scope of undiscovered and unreported crimes that do not feed back into official data. See the almost equivalent notion of 'secret deviance' in Becker (1963); Bureau of Social Science Research (Washington, D.C.) *Report on a Pilot Study in the District of Columbia on Victimization and Attitudes Toward Law Enforcement* (Washington, DC: President's Commission on Law Enforcement and Administration of Justice 1967).

[13] Gutierrez and Kirk (2017), p. 926; Reina *et al.* (2014); Messing *et al* (2015); Bucher *et al.* (2010), pp. 159 ff.; Comino *et al.* (2020), pp. 1214 ff.; Fussell (2011), pp. 593 ff.

[14] In situations involving human trafficking and smuggling of migrants, victims are often afraid to contact authorities because of the relationship with traffickers, which can vary from complete subjection due to fear of retaliation to gratitude for the help provided in the migration journey. UNHCR, (2017) *L'identificazione delle vittime di tratta tra i richiedenti protezione internazionale e procedure di referral. Linee guida per le Commissioni Territoriali per il riconoscimento della protezione internazionale*, available at www.unhcr.org, p. 9.

[15] ISTAT, (2017) Delitti, imputati e vittime. Una lettura integrata delle fonti su criminalità e giustizia, available at www.istat.it.

[16] Barbagli and Colombo (2009).

[17] ISTAT, (2017) (n 15).

[18] See FRA, Encouraging hate crime reporting. The role of law enforcement and other authorities (Report) 2021; FRA, Protecting migrants in an irregular situation from labour exploitation. Role of the Employers Sanctions Directive (Report) 2021. Amongst EU and international legislation, see Directive 2009/52/EC of the European Parliament and of the Council of 18 June 2009 providing for minimum standards on sanctions and measures against employers of illegally staying third-country nationals; Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA; Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA; ILO Convention concerning Migrations in Abusive Conditions and the Promotion of Equality of Opportunity and Treatment of Migrant Workers (Entry into force: 09 Dec 1978).

3. Going around a minefield: in search of a safe path for irregular migrants to report a crime.

Now that we have reframed the topic from a criminological and victimological perspective, we have to analyse the issue in practice, considering the Italian legal system as a point of observation.

To get into the topic in practice, it might be useful to question which are the paths for crime reporting available in Italy, for a victim with an irregular migration status seeking to access the criminal justice system, knowing that in the Italian legal system, irregular entry and stay is provided not only as an administrative offence but also as a criminal offence[19]. In fact, Italian legislation establishes four different misconducts related to irregular migration punished as criminal offences. The main offences criminalising irregular migrants are detailed in the Consolidated Law on Immigration [20]. These are 'irregular entry and stay' in the State's territory [21]; the infringement of an order to leave the State's territory [22]; the re-entry into the State's territory after an administrative expulsion [23]; and the re-entry into the State's territory after a border rejection or expulsion[24]. In practice, some of these criminal offences coincide with having an irregular migration status as such – this being particularly true for the crime of irregular entry or stay which sanctions people who irregularly entered the territory or overstayed in Italy after their residence permit expired. [25]

Moreover, all these crimes are prosecutable *ex officio*, and the Italian criminal justice system places a duty to report crimes prosecutable *ex officio* upon all police officers, public officials, and, under certain conditions, doctors. Meaning that every public official (including police officers) has the duty to report crimes they gained knowledge of in the exercise of their function. The violation of the duty to report a crime for public officials is punished by art. 361 and 362 of the Italian Penal Code.

In short, the combined effect of the criminalisation of migrants with an irregular *status* and the duty to report irregular migrants for public officials, including police officers, makes the interaction between migrants and public authority problematic.

Concerning the paths for crime reporting, the victim can report directly to public authorities or through the support of another person (usually a lawyer). Reports by private parties (denuncia) can be submitted by whoever has knowledge of an offence (when prosecutable *ex officio*). The report shall be submitted orally or in writing, personally or by means of a proxy, to a Public Prosecutor or a criminal police official. When submitted in writing the report shall be signed by its author or their proxy (Art. 333 CPP[26]). Conversely, minor crimes, and some

[19] See Di Martino *et al.* (2013); Mentasti (2022), p. 502 ff.

[20] Decreto legislativo 25 luglio1998, n 286, Testo Unico sull'immigrazione (also Consolidated Law on Immigration, or CLI).

[21] CLI, Art. 10-bis, punished with a fine ranging from 5.000 euros to 10.000 euros.

[22] CLI, Art. 14 (5-ter) punished with a fine ranging from 10.000 to 20.000 euros and (5-quater) punished with a fine ranging from 15.000 to 30.000 euros. In both of these cases, the Italian legislation provides for administrative detention pending expulsion. It is important to note that this article provides for a safeguard clause, which refers to a justified reason that exempts the person from his/her criminal liability. The Constitutional Court (Corte cost., sentenza 13 gennaio 2004, n. 5) affirmed that the justified reason does not require situations as severe as State of Necessity or coercion. Moreover, the Court stated the justified reason which legitimates the infringement of the order to leave consists in objective conditions or in subjective and personal situations of serious and pressing psychological conditioning that make compliance with the order extremely difficult. Nevertheless, the Court of Cassation also specified that the migrant condition as such and other derived situations such as the lack of a regular job or an unstable financial situation are not considerable justified reasons (Cass. Pen., Sez. I, 19 febbraio 2018 n. 7915).

[23] CLI, Art. 13 (13) and (13-bis) Once the foreigner received an expulsion measure, he/she cannot re-enter the State's territory without a special authorization issued by the Ministry of Interior. In case of transgression, the foreigner is punished with imprisonment for a period of one to four years, and is newly expelled with immediate removal." Nevertheless, the provision does not apply to foreigners already expelled, for whom entry was authorized for family reunification (pursuant to CLI, art. 29). The same punishment is applicable for transgression of the prohibition to re-enter, in case of expulsion ordered by the judge. By contrast, when the foreigner has been already reported for irregular re-entry in the State's territory and re-expelled, his/her re-entry in the national territory is subject to imprisonment for a period of one to five years.

[24] CLI, Art. 10 (2-ter) punished with dention ranging from one to four years and expulsion and (2-quarter) punished with detention ranging from one to five years. These two offences have been recently introduced by the the Decreto Legislativo 4 ottobre 2018, n 113 (also 'Salvini Decree'), for a comment see Aimi (2019), pp. 137 ff.; Masera (2019).

[25] According to many Italian scholars, Art. 10-bis of the CLI would violate the harm principle (*nullum crimen sine iniuria*) to the extent that it criminalises a human condition (rather than a human behaviour) which does not produce any harm. The lack of a clause that envisages a 'justified reason' excluding the criminal liability and other circumstances which do not depend on the migrant would violate the culpability principle. Most of these criticisms were ummarized in the constitutional reviews analysed by the Constitutional Court in the judgment Corte cost., sentenza 5 Luglio 2010, n 250; for comments on this judgement see Caputo (2010), pp. 1187 ff.; Masera (2010), p. 1373; Viganò (2010), pp. 13; Cavaliere (2013), pp. 32 f.; Ferrajoli (2009), p. 9 ff.; Gatta (2009), p. 1323 ff.

[26] Codice di Procedura Penale, DPR 22 Settembre 1988, n 447 (hereafter CCP).

major offences (for instance, sexual assault or stalking), require a 'complaint' (querela) by the victim for the prosecution to be initiated[27]. The complaint shall be submitted in the same way as the report by private parties (orally or in writing, personally or by means of a proxy). Moreover, if it bears an authenticated signature, the statement may also be delivered by an appointed person or sent by mail in a registered envelope.

When the victim approaches a police station he/she is immediately identified by police officers – either through ID documents or through database checks. At this moment, the migrant victim is immediately detected as irregularly present on the Italian territory and the criminal proceeding against him/her must start. In a different scenario, he/she could report the crime in writing, through a proxy (for example, a report drafted by a lawyer) preventing direct contact between the migrant with irregular status and public officials. Nevertheless, the identification of the victim and his/her participation in the trial is almost always necessary to continue the investigations and the trial. Moreover, it cannot be ruled out that this way of reporting may disclose (and bring evidence of) the irregular presence of the complainant, or clues of his/her irregular migration status.

With all this in mind, it is easy to understand that irregular migrants' approaching public authorities in Italy are effectively exposed to the risk of being detected, prosecuted and deported.[28]

In this scenario, migrant victims are trapped in a deadlock: reporting the crime they have suffered, thus revealing (sooner or later) their condition of irregularity; or keeping silence on the crime suffered and remaining unprotected and exposed to the risk of further victimization.

4. A right to silence for silenced victims?

The situation we have just sketched sounds familiar to criminal lawyers as it reminds us of the so-called "cruel trilemma" of the defendant forced to choose between maintaining silence and being held in contempt of court; lying and thereby perjuring, or incriminating himself[29]. In that situation, the *nemo tenetur se detegere* principle – no one is bound to incriminate himself – offers a way out of this impossible decision: the defendant can remain silent without fearing contempt or other negative consequences.

4.1. *The right to remain silent: essential features.*

The right to silence has distant roots that are impossible to summarize in a few lines[30] and even though it is not always expressly provided, most criminal justice systems rely on it. An explicit recognition of the right to not be a witness against oneself lies in the Fifth amendment of the US Constitution of 1791[31], in the International Covenant on Civil and Political Rights, which also provide the right not to be compelled to confession[32], in the Inter-American Convention on Human Rights[33] and the Rome Statute of the International Criminal Court[34].

The European Court of Human Rights recognised the right to remain silent and the

[27] See Pecorella, (2016); Vitarelli (2020), pp. 474 ff.; Taverriti (2017), pp. 503 ff.

[28] Just to name two episodes that took place in Italy, see "*Chiami l'ambulanza? Arriva la polizia. Dei migranti chiamano il 118, ma con l'ambulanza arriva la polizia: 18 fogli di via, un rimpatrio*", in www.osservatoriodiritti.it; "*Irregolare vittima di reato? Ti arrangi. Giovane immigrato senza permesso di soggiorno denuncia l'aggressore e riceve il foglio di via*", in www.osservatoriodiritti.it

[29] Term used by the United State Supreme Court in Murphy v. Waterfront Comm'n., 378 U.S. 52, 55 (1964), Greenawalt (1981), pp. 39 ff.; for a critical review of the argument see Dolinko (1986), pp. 1090-1107.

[30] See Alschuler (1996), pp. 2625 ff.; Dolinko (1986), pp. 1063; Helmholz (1990), pp. 962; Levy (1968); Redmayne (2007), pp. 209 ff.; Catalano (2011), pp. 4020 ff.

[31] «No person […] shall be compelled in any criminal case to be a witness against himself».

[32] See Art. 14, para 3, (g) providing «In the determination of any criminal charge against him, everyone shall be entitled to the following minimum guarantees, in full equality: […] Not to be compelled to testify against himself or to confess guilt.».

[33] See Art. 8, para 2 (g) «Every person accused of a criminal offense has the right to be presumed innocent so long as his guilt has not been proven according to law. During the proceedings, every person is entitled, with full equality, to the following minimum guarantees: […] g. the right not to be compelled to be a witness against himself or to plead guilty».

[34] See Art. 67, para 1(g) «In the determination of any charge, the accused shall be entitled to a public hearing, having regard to the provisions of this Statute, to a fair hearing conducted impartially, and to the following minimum guarantees, in full equality: […] Not to be compelled to testify or to confess guilt and to remain silent, without such silence being a consideration in the determination of guilt or innocence»

privilege against self-incrimination within the scope of art. 6 of the Convention[35], although not specifically mentioned as these are «generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6»[36]. The *rationale* is to fulfil the requirements of a fair trial and to assure the presumption of innocence preventing improper compulsion by the authorities and miscarriages of justice.

EU Law also recognized this right in art. 47 and 48 of the EU Charter of fundamental rights, which together provide for the right to a fair trial, the presumption of innocence and the right of defence[37]. As usual, in accordance with art. 52 (3) of the EUCHR, these standards are recognized the same meaning and scope as the corresponding guarantees provided by the ECHR, and they are thus interpreted taking into account art. 6 of the ECHR and the related case law. Also, the EU Court of Justice has recently recognised that the right operates even in administrative proceedings which fall within the scope of the *matière pénale*[38] when individuals are required to answer questions which might establish their liability for an offence that is punishable by administrative sanctions of a criminal nature, or their criminal liability[39]. EU also took significative steps to further enhance the protection of the presumption of innocence with the 2016/343 Directive[40] explicitly providing the right to remain silent and not to incriminate oneself at art. 7[41].

Even though the right to remain silent seems to enjoy a good reputation in most legal experiences around the globe, there are some points to outline about its objective and subjective scope of protection and range of application.

First, the right to remain silent is usually recognised as a guarantee for individuals that are already accused or at least suspected of committing a crime, and it generally applies to criminal proceedings starting from the point at which the suspect is questioned by the police[42]. So, it basically does not apply before the beginning of the police investigation. Moreover, the right to remain silent is not absolute. In fact, the scope of the guarantee does not protect against the making of self-incriminating statements *per se*, but against the risk of obtaining evidence through moral or physical coercion in defiance of the will of the accused[43]. This situation recurs when the accused person is obliged to testify under the threat of sanctions[44]; when he/she is under physical or psychological pressure to obtain evidence or statements[45]; when authorities try to elicit information using subterfuge even though the accused chose to remain silent[46].

Moreover, the ECtHR considers the right to remain silent a relative one[47]. So, even though it is not possible to extinguish the very essence of this right, public interest concerns (i.e. in investigation and punishment) can justify – to some extent – a limitation of the right to silence[48].

All this considered, the victim with irregular migration status approaching authorities to report a crime he/she has suffered is not yet accused or suspected of a crime, but the mere discovery of his/her name might disclose his/her condition, thus incriminating oneself. Nevertheless, he/she could not enjoy the right to silence which is exclusively recognized for the accused/suspected person.

In Italy, the right to silence is recognized as an articulation of the fundamental right of

[35] See Ashworth (2008), pp. 751 ff.; Lamberigts (2016), pp. 418 ff.; Veas (2022), pp. 869 ff.; See Funke v France (1993) 16 EHRR 297, para 44; Saunders v United Kingdom (1996) 23 EHRR 313, para 68; Murray v United Kingdom (1996) 22 EHRR 29, para 45; O'Halloran and Francis v United Kingdom (2007) 46 EHRR 21, para 45; Bykov v Russia App no 4378/02 (EctHR Grand Chamber, 10 March 2009), para 92; Ibrahim and Others v the United Kingdom App nos 50541/08, 50571/08, 50573/08 and 40351/09 (EctHR 13 September 2016), para 272).

[36] Murray v United Kingdom (1996) 22 EHRR 29, para 45.

[37] Hancox (2021), p. 231.

[38] See for all Mazzacuva (2017).

[39] Case C-481/19, DB vs Consob (GC, 2 February 2021) commented by Basile (2021); Aranci (2021). See also the request for a preliminary ruling deriving from the Italian constitutional Court, Corte Cost., 10 maggio 2019, Ord. n. 117 commented by Confalonieri (2020); Caneschi (2020), pp. 579 ff.; Fares (2020), p. 57; Lasagni (2020), p. 135.

[40] Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11 March 2016

[41] See Pivaty *et al.* (2021), p. 328; Pivaty (2021), p. 427.

[42] Murray v United Kingdom (1996) 22 EHRR 29, para 45.

[43] Ibrahim and Others v the United Kingdom App nos 50541/08, 50571/08, 50573/08 and 40351/09 (ECtHR 13 September 2016), para 267.

[44] Saunders v United Kingdom (1996) 23 EHRR 313, para 68-70.

[45] Jalloh v. Germany [GC], 2006-IX; Gäfgen v. Germany [GC], 2010-IV.

[46] Allan v. the United Kingdom, 2002-IX; contrast with Bykov v. Russia [GC], 2009, para 101-102).

[47] Ashworth (2008), pp. 760-762; Murray v United Kingdom (1996) 22 EHRR 29, para 47; Ibrahim and Others v the United Kingdom App nos 50541/08, 50571/08, 50573/08 and 40351/09 (ECtHR 13 September 2016), para 269.

[48] Saunders v United Kingdom (1996) 23 EHRR 313, para 67; Heaney and McGuinness v Ireland (2000) 33 EHRR 12, para 57.

defence, provided in art. 24 of the Italian Constitution, but it is also connected to art. 27, c. 2 affirming the presumption of innocence, and art. 111 Cost. which sets the standards for due process in the Italian legal system, and art. 13 Cost which enshrined personal liberty is inviolable[49].

4.2. *Mixed signals from the Italian case law.*

In Italy, after the introduction (2009) of art. 10-bis of CLI – which criminalised illegal entry and stay, some of the numerous constitutional reviews submitted to the Constitutional Court regarded the possible conflict between art. 10-bis CLI (and other norms of the CLI) and the fundamental right not to self-incriminate.

To our ends, the most important case[50] referred to a woman who was required to testify in the trial against her abusive husband, but she refused to attend the examination because she was afraid that the Judge would have denounced her, due to her irregular condition (art. 10-bis), based on the duty to report (art. 331 CP). According to the Judge who submitted the question to the Constitutional Court, the risk of being detected as irregular migrants undermined the right to justice and to a fair trial, as laid down in art. 24 (right of defence) and in art 47 of the EUCFR[51], given the lack of exemptions from the duty to report irregular migrants. The Constitutional Court declared the question inadmissible[52], but the ruling is noticeable because the Court indirectly claimed two important arguments. On the one hand, the Court reaffirmed that there is no obligation to report a crime when it is already known to the Public Prosecutor. On the other hand, the Court states that the migrant eligible for one of the permits related to victims protection or that is potentially allowed to remain in Italian territory has the right to legally reside in Italy even before the issuance of the permit by the Questore.

In another case[53], a migrant with irregular status was seeking to receive the payment of his salary and compensation due to an accident at work. The migrant did not appear at the hearing in front of the Labour Court, and his attorney referred that the man feared he would have been denounced by the Judge. The Judge submitted the question to the Constitutional Court in similar terms to those mentioned above. One important difference, in this case, was that the migrant could not have access to the special permit for victims of crimes, because his situation did not meet their requirements. Astonishingly, the question has never been decided (or maybe received) from the Constitutional Court.

5. Seeking some shelter: safe reporting mechanisms between 'firewalls' and special resident permits.

With all this in mind, we can now consider some measures that have been actually taken in different legal systems[54] to mitigate victimization and underreporting of people with irregular migration status, which could also be considered as an articulation of the *nemo tenetur se detegere* as there could be: (i) 'firewalls' shielding victims from being identified as "irregular" by authorities responsible for deportation/prosecution, thus protecting their silence; (ii) remedies that provide a regular migration status after crime reporting, thus encouraging victims to speak up.

[49] For an overview of the right to remain silence in Italy see Grevi (1972); Amodio (1974), pp. 408 ff.; Luparia (2006); Mazza (2004); Patanè (2006); Tassinari (2012); Marchesi and Panzavolta (2021), pp. 365.
[50] Trib. Min. Roma, Ord. N. 84/2010, 30.09.2010, in G.U. n. 21 del 18.5.2011.
[51] Art. 47 EUCFR - *Right to an effective remedy and to a fair trial*: Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.
[52] Corte Cost., 11 novembre 2011, Ord. n. 306.
[53] Trib. Voghera, 20 november 2009, R.G. 91/09 commented by Bozano and Guariso (2009), p. 1077.
[54] See the comparative research conducted with regard to Belgium, Netherlands, Spain, USA and Italy under the guide of the University of Oxford available at https://www.compas.ox.ac.uk/project/safe-reporting-of-crime-for-victims-and-witnesses-with-irregular-migration-status-in-the-usa-and-europe/

5.1. *Firewall measures: keeping silence.*

Firewalls are measures that aim at keeping separated immigration enforcement activities from public service provision, criminal justice or labour law enforcement, to ensure that migrants with an irregular migration status are not discouraged from accessing essential services and/or reporting crime[55]. Also known as non-cooperation policies, firewalls in the area of crime reporting would prevent the detection of the victim as an irregular migrant or the communication of his/her personal details to other authorities responsible for immigration enforcement. Such firewalls generally operate according to a *'don't ask'* model, when they prohibit or limit the possibility of crime enforcement officers inquiring about the immigration status of the person they are interacting with; a *'don't tell'* model, when they proscribe communicating information about someone's immigration status to immigration enforcement authorities; and/or *'don't enforce'* model, when they prevent the arrest or detention of individuals by criminal enforcement actors solely for a violation of immigration law[56]. The rationale of these measures is to reassure migrants by encouraging them to report crimes they have suffered but also to build trust among police and communities in order to promote the cooperation of civilians in crime prevention.

Non-cooperation policies include a wide range of combinations of practices, encompassing one or more of the components cited above (*don't ask*, *don't tell*, *don't enforce*) and are pretty common in the United States, where they are often adopted at the local level (counties, cities and – at times – states) to prevent local police officers from getting involved in immigration law enforcement, which is the responsibility of the federal government (US Department of Homeland security) [57].

This is also the case of the Netherlands which implemented the 'free in, free out' policy, which allows irregular migrants freely to enter a police station to report a crime and be guaranteed to be able to leave freely, without being arrested or detained[58]. The policy started as a pilot project in Amsterdam, and it was progressively extended to further municipalities (Utrecht and Eindhoven) and finally recognised at the national level as an implementation of the EU Victims' Directive requirements in the Netherlands[59].

Local initiatives undertaken by some municipalities envisage the issuance of identity documents that do not show the immigration status of the holder. This is the case of San Francisco, New Heaven and New York City's status-blind municipal ID card: a broadly accepted government-issued photo identification, recognized for interacting with the New York Police Department (NYPD)[60].

Taking a closer look at the Italian legal system, it is evident that it is not possible to replicate firewall measures deployed at the local level. The lack of distinction between immigration enforcement and police forces, and the duty to report irregular migrants, which binds both police officers and public servants make it particularly difficult to replicate in Italy firewall practices structured like those developed in Sanctuary cities in the USA[61].

Something similar to a non-cooperation policy is provided about the obligation to report irregular migrants in the scope of the right to health. In fact, the duty to present a report does not apply to medical doctors when there is a risk of exposing the patient to criminal proceedings (Art. 365, para. 2 IPC). In addition, Art. 35, para. 5 CLI explicitly states that access to healthcare facilities cannot mandate any kind of reporting of migrants. This provision is aimed at reassuring migrants in need of healthcare, so they do not fear being reported or deported for accessing healthcare. The same exemption is not provided for migrants seeking to access the criminal justice system to report a crime they have suffered. Therefore, while healthcare facilities are conceived as safe harbours for migrants with irregular status, the same cannot be said for police stations and other public facilities migrants may need to access to exercise their rights.

[55] Crépeau and Hastie (2015), p. 165.
[56] See extensively Delvino (2019), pp. 28 ff.; Kittrie (2006), pp. 1449.
[57] Meissner *et al.* (2013).
[58] Timmerman *et al.* (2020), p. 427.
[59] Timmerman *et al.* (2020), p. 438.
[60] See de Graauw (2014), p. 309.
[61] See Taverriti (2019), pp. 32 f.

5.2. *Special resident permits: protecting words.*

Another way to defuse the deportation threat dynamic that discourages irregular migrants from reporting crime is providing migrant victims or witnesses with authorization to regularly reside in the state territory after crime reporting. These measures include special visas or residence permits, or the suspension of immigration enforcement. Unlike firewalls, these measures do not ensure the right to remain silent, but instead, provide protection to individuals releasing self-incriminating statements concerning their irregular status.

Italian legislation has introduced special resident permit for victims of certain crimes, showing both legislators' interest in addressing crime underreporting and in filling the justice gap for irregular migrant victims. These special permits offer protection by adopting a multi-agency approach, allowing victims to stay in the country, but also to obtain public support to reintegrate into Italian society. They are usually renewable and/or convertible into permits for work or study reasons, so they offer an encouraging horizon of stabilization. In Italy, special residence permits are provided for: (a) victims of serious crime released for social protection reasons; (b) victims of domestic violence; (c) victims of severe labour exploitation; (d) persons who cooperate in the prevention of terrorist attacks.

Art. 18 of CLI provides a *special permit issued for reasons of social protection to people who have suffered a serious crime perpetrated by a criminal organisation*. This permit is one of the most inspiring examples of tools offered by Italian legislation for the integration and protection of migrant victims, it can be issued for victims of offences within the area of sexual exploitation, including sexual exploitation as such, recruitment for prostitution, and sex trafficking committed both at national and international level. But the permit also applies to a wide range of other serious offences that have in common the provision of mandatory arrest *in flagrante delicto*[62]. Three requirements define the scope of application of the special permit for social protection reasons: 1) the victim must have suffered one of the criminal offences listed in Art. 18 CLI; 2) the situation of violence against a foreigner or his/her serious exploitation has to be ascertained (either during police/judicial operations, or during intervention carried out by the social services); 3) the presence of an actual threat to the migrant's safety consequent to his/her attempts to escape the pressure of a criminal organisation perpetrating the crime[63], or in retaliation for the statements given during preliminary investigations or trial.

Art. 18-bis CLI provides a *special permit for victims of domestic violence*. This special permit was introduced in compliance with the Istanbul Convention, with the aim of combating gender-based violence and protecting victims.[64] The aim of this tool is to protect victims of domestic violence irrespective of their contribution to criminal proceedings. Accordingly, its issuance does not require victims to report the crime. It applies to crimes related to domestic violence[65], thus including crimes perpetrated even by a single offender. There must be a real and actual danger for the foreigner's safety as a consequence of escaping the violence or due to statements provided during preliminary investigations or trials.

These two special permits show a multi-agency approach focusing on victims' protection and encouragement: in both cases, the victim is also included in a social program of assistance and social integration[66]. Moreover, both permits are accessible through a *judicial path* or a *social path*. The *judicial path* takes place when the criminal offence is known in the context of a criminal proceeding, but it does not require that the migrant submit a report or a complaint for

[62] Just to name a few of them, the permit can be issued to victims of: modern slavery, crimes related to child prostitution and pornography; tourist initiatives aimed at exploiting child prostitution; illegal labour intermediation and labour exploitation; sexual offences and grooming of minors; crimes of aggravated theft and robbery and serious crimes against the property; crimes concerning weapons, narcotic drugs, mafia-type association aiming at committing other crimes; trafficking of migrants, domestic abuse and stalking, and other. For the full list of crimes, see CPP, Art. 380.

[63] It is important to notice that a special permit for social protection reasons does not apply to cases in which the crime is perpetrated by one single person, being necessarily the activity of a criminal organisation. This might significantly limit the application of this measure of protection.

[64] Council of Europe Convention on preventing and combating violence against women and domestic violence, made in Istanbul, 11.V.2011.

[65] Namely, art. 572 IPC (abuses in the family), artt. 582, 583, 583-bis CP (providing different kind of personal injuries), art. 605 CP (kidnapping), art. 609-bis CP (sexual violence), art. 612-bis (stalking) or one of the crime listed in art. 380 CPP.

[66] Social services usually take away the victim from his/her environment and prevent him/her to keep in touch with the persons who caused the situation of violence or exploitation. This is often not easy since relatives and friends are often involved. The programme involves arranging for an accommodation, initial reception, and classes of Italian.

the permit to be released. The *social path* arises from aid interventions carried out by the social services highlighting a situation of violence or severe exploitation against the migrant. Social services, associations and other entities entitled to offer assistance to migrants can promote the issuance of these special permits, and even in this case, the victim is not required to report the crime or to cooperate in the criminal proceeding to receive it. This confirms these permits are conceived as tools of protection rather than as a reward for victims' cooperation.

in compliance with Directive 2009/52/EC[67], Italy introduced a *special permit for victims of severe labour exploitation*[68]. The main purpose of such permits is to allow the criminal justice system to benefit from the victim's cooperation in the fight against illegal employment and exploitation of migrants with irregular status. There are three basic conditions required for the permit to be issued: 1) a situation of severe labour exploitation; 2) a report submitted by the foreigner; 3) and that he/she takes part in the proceedings against the employer. Unlike the two other special permits analysed above, the permit for severe labour exploitation is at least partially intended to act as a reward as it requires the active cooperation of the victim with prosecutors. Indeed, to obtain the permit a victim must report the crime and cooperate in the trial against the exploiters.

The special permit for investigative reasons was introduced in 2005 as a tool for counteracting terrorism[69]. In this situation, the person who reports a crime is not a victim of crime, but an informant who is encouraged to report to public authorities as a witness of the activities of a terrorist organisation. It is possible to issue this special residence permit when, during police operations, investigations or criminal proceedings for crimes of terrorism, the permanence in the State's territory of the person who cooperated becomes necessary.

Despite being considered 'best-practices', these special permits also suffered from limitations and shortcomings. On the one hand, special permits do not cover the whole spectrum of crimes that migrants with irregular status suffer the most (i.e. immigration frauds related to their irregular condition, street crimes perpetrated by one single offender or outside the scope of domestic violence). On the other hand, the successful use of these measures depends on victims' awareness about the existence and the functioning of special permits; but also on the actual presence, within a certain territory, of associations authorized to carry out these initiatives.[70] In addition, the release of special permits is never automatic, as the public authorities who are responsible for their issuance (the Public Prosecutor and the Police Commissioner) retain wide discretion about it.

6. Concluding remarks and future directions.

At the end of our analysis, we can now draw some conclusions on the state of the art of the protection of victims with an irregular migration status and suggest some proposals to enhance equal and effective access to justice for this kind of individuals.

This article outlined the condition of vulnerability affecting victims with an irregular migration status that makes them more exposed to victimization and demonstrated that the fear of being detected as 'irregular' and thus being subject to criminal or administrative proceedings that culminate in deportation plays an important role in discouraging crime reporting for these people. Thus, there are victims – with special needs of protection – who are discriminated and substantially denied justice, as they are not able to access the criminal justice system in practice. We have then verified that in Italy there is an actual risk of deportation or prosecution discouraging irregular migrants from reporting crime, precisely deriving from the conjunction of the criminalization of irregular entry or stay, the need for identification of the victim during reporting procedures which easily reveal their condition, and the duty to report irregular migrants with no exceptions for public authorities.

As immigration and public security issues are the monopoly of the central state and are both the responsibility of the same police forces, firewall practices seem unlikely to take place

[67] Directive 2009/52/EC of the European Parliament and of the Council of 18 June 2009 providing for minimum standards on sanctions and measures against employers of illegally staying third-country nationals.
[68] D. lgs. 16 july 2012, n. 109, 'Attuazione della direttiva 2009/52/CE che introduce norme minime relative a sanzioni e a provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare'.
[69] D. L. 27 july 2005, n. 144, Misure urgenti per il contrasto del terrorismo internazionale.
[70] See Delvino and Spencer (2014).

in Italy. Thus, the most suitable action for enhancing equal protection for victims with an irregular status would be a legislative reform at the national level. To this end, comparing the right to healthcare and the right to access justice for the victims, it would be reasonable to introduce a special exemption to the obligation to report irregular migrants applicable to judicial authorities and police forces receiving a criminal report from a migrant seeking protection, irrespective of the crime suffered. Likewise, the potential extension of the scope of application of special permits for victims of crimes ought to be conceived at the national level, considering the wide range of criminal cases whose victims are typically irregular migrants that are still not covered by this form of relief.

Alternatively to legislative reforms, which might be difficult to achieve, there may be some room for the judicial affirmation of the right to remain silent for victims with irregular migration status in order to prevent discrimination in their access to justice.

As we have seen, the condition of migrant victims compelled to reveal their irregular migration status resembles very much to the condition of the defendant at risk of self-incriminating oneself, but limitations in the scope of application (the suspect or the accused person, after the beginning of the proceeding) and in the relativity of the right to remain silent suggest that the *nemo tenetur se detegere* is not *per se* a way out of the issue. The protective measures we have analysed show several similarities with the right to silence and its corollaries, suggesting that the right to remain silent and not incriminate oneself could be a suitable tool of protection. So, it remains to verify if there are other possible way to affirm a general right not to incriminate oneself for the migrant victim when reporting a crime. Hereafter we will sketch some proposal to achieve this objective at different levels, challenging the duty to report irregular migrant for public authorities.

First, according to the principle of primacy of the EU law, it could be argued that public authorities getting in touch with an irregular migrant in the scope of a reporting procedure can disapply on their own motion, and thus infringe the norm providing a duty to report, as it would be in contrast with EU law with direct effect[71]. To this end, it is worth noticing that victims' protection has gained greater attention from the EU over the last decade, especially with the adoption of the so-called 'victims directive' Dir. 29/2012[72], which emphasized the need for victims' protection inside and outside the criminal proceeding, clearly establishing that victims' rights should apply to all victims without discrimination with respect to residence status (Art. 1) and Member States should "take the necessary measures" to ensure that the rights set out in the Directive are not made conditional on the victim's residence status (Recital 10)[73]. Indeed, obstacles in crime reporting for irregular migrants violate several provisions of the victims' directive regarding information and support, the rights related to the participation of the victim in the proceeding, and the right to receive adequate protection. Thus, combining the right to remain silent deriving from EU legal sources mentioned above, and the victims right laid down in the victims' directive, we can derive the possibility of disapplying the duty to report irregular migrants approaching public authorities to report a crime. Nevertheless, this solution shows some risk of arbitrariness and uneven application when left to the discretion of each public authority involved, thus it could be useful to request a preliminary ruling from the Court of Justice of the EU.

Further perspectives of protection could be achieved through a judicial review of the duty to report irregular migrants deferred to the Constitutional Court. As we have seen, precedent case law did not expressly address the issue of victims' right to silence concerning their irregular status when reporting a crime. So, as the range of applications of the right to remain silent is recently expanding in the view of the Italian constitutional Court[74], it could be interesting to raise the question in front of the Court to verify if the reasons supporting the right of de-

[71] See essentially the seminal case law Case 106/77, Simmenthal, EU:C:1978:49, Case 103/88, Costanzo, EU:C:1989:256 and subsequent jurisprudence of ECJ. In the Italian doctrine, for all, Manes (2019), pp. 26 ff..; Viganò (2019), p. 481.

[72] Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, see Bargis and Belluta (2017); Luparia (2015).

[73] Equal access to justice is functional to the full implementation of the EU Victims Directive in line with the aims and recommendations recently stated in the EU's "Strategy on the rights of victims of crime" (2020-2025), which include a European Commission's commitment to "assess legal and practical tools at EU level to improve reporting of crime and access to support services for migrant victims, independently of their residence status", and recommendations to EU countries to "take actions to ensure that all victims, including migrant victims have access to justice independently of their residence status".

[74] See, just recently, Corte cost., sent. 6 aprile 2023 (dep. 5 giugno 2023), n. 111, pres. Sciarra, rel. Viganò.

fence of the victim (articulated in the right to report crimes suffered) could be used as a driver of the expansion of the right not to incriminate oneself to any individual (irrespective of his formal condition of accused/suspected of having committed a crime) even before the formal beginning of the proceeding against him/her (thus, in any form of approach of the individual to public authorities).

Finally, the case law of the ECtHR gives some food for thought to suggest wider protection in these situations. As we have seen, if we consider the right to remain silent and not to incriminate oneself taken alone, as recognised according to the interpretation of art. 6 provided by the ECtHR, there is no way to cover the situation of migrant victims of crime with irregular status. Nevertheless, if we consider the whole picture, one could argue that the duty to report irregular migrants even when they are approaching public authorities to report a crime gives rise to serious discrimination in the effective access to justice and related protection for victims of crimes, which make these individuals disinclined to report, and thus more exposed to suffer crimes in the territory of the State. Looking at the issue from this perspective, the duty to report irregular migrants seeking to report a crime, would not only infringe on victims' right of defence (the right of access to a court according to art. 6 of the ECHR), but also the positive obligation (derived from art. 1 of the ECHR) to protect his/her life, physical and psychological well being, and private life (i.e. artt. 2, 3, 8 of the ECHR), which requires domestic authorities to display due diligence in protecting individuals whose life is at risk and take preventive measures[75]. The same considerations apply when we consider that the substantial deprivation of accessing the criminal justice system to report a crime results in the breach of the duty to put in place and apply an adequate legal framework affording protection against acts of violence by private individuals[76]. Besides all, we should consider that the denial of justice deriving from the situation analysed affects only migrants with an irregular status, precisely because of their migration status, resulting in clear contradiction with the prohibition of discrimination established by art. 14 of the Convention.

In the end, the road towards the affirmation of the right to silence for victims of crimes is long and winding, but when we consider reshaping the *nemo tenetur se detegere* to adjust it to this situation, we should also consider balancing the extension of the guarantee with the public interest of the State. Well, on a closer inspection, keeping the duty to report irregular migrants grants the enforcement of immigration law (including its criminal limb), whereas the silence of victims with an irregular status carries the weight of the public interest to protect that single victim, but also to detect and prosecute all the crimes committed on its territory, without exceptions. We should probably reflect on what is our priority and if this can be considered a fair and proportionate balance of interests[77].

References.

Aimi, Alberto (2019): "Il "Decreto Sicurezza" 2018: i profili penalistici", *Rivista italiana di diritto e procedura penale*, pp. 135-194.

Alschuler, Albert W. (1996): "A Peculiar Privilege in Historical Perspective: The Right to Remain Silent", *Michigan Law Review*, 94, pp. 2625-2672.

Amodio, Ennio (1974): "Diritto al silenzio o dovere di collaborazione? A proposito dell'interrogatorio dell'imputato in un libro recente", *Rivista italiana di diritto e procedura penale*, pp. 408-419.

Aranci, Matteo (2021): "Diritto al silenzio e illecito amministrativo punitivo: la risposta della Corte di giustizia", *Sistema Penale*, 2, pp. 73-98.

[75] See Sudre, (1995), pp. 363 ff.; Mowbray (2004); Schabas (2016), pp. 90 ff. and *passim*; in the Italian doctrine see Nicosia (2006), pp. 255 ff.; Paonessa (2009); Viganò (2011), pp. 2645 ff.; Manes (2013), pp. 106 ff.; Bernardi (2020), pp. 129 f.;
[76] See, for example, *Osman v UK* ECHR 1998-VIII; *L.C.B. v. the United Kingdom*, 9 June 1998, para. 36, Judgments and Decisions 1998-III; *Opuz v. Turkey*, 2009-III, para 128; *Makaratzis v. Greece* [GC], no. 50385/99, para. 57, ECHR 2004-XI; *Paul and Audrey Edwards v. the United Kingdom*, no. 46477/99, § 71, ECHR 2002-II. *Beganović v. Croatia*, no. 46423/06, §§ 85–86, 25 June 2009.
[77] See, for all, Recchia (2020).

Ashworth, Andrew (2008): "Self-Incrimination in European Human Rights Law – a Pregnant Pragmatism?", *Cardozo Law Review*, 30, pp. 751-774.

Barbagli, Marzio and Asher, Colombo (2009): "Immigrants as authors and victims of crimes: the Italian experience", in McDonald William F. (ed): *Immigration, Crime and Justice* (Emerald JAI, North America), pp. 69-94.

Bargis, Marta and Belluta, Hervé (2017) (eds): *Vittime di reato e sistema penale. La ricerca di nuovi equilibri*, (Torino, Giappichelli).

Basile, Enrico (2021): "La Corte di giustizia riconosce il diritto al silenzio nell'ambito dei procedimenti amministrativi "punitivi"", *Sistema Penale*, 3 febbraio 2023.

Barranco, Raymond E. and Shihadeh Edward S. (2015): "Walking ATMs and the immigration spillover effect: the link between Latino immigration and robbery victimization", *Social Science Research*, 52, pp. 440-450.

Becker, Howard S. (1963): *Outsiders: Studies in the Sociology of Deviance* (New York, Free Press of Glencoe).

Bernardi, Alessandro (2020): "Il diritto penale tra sovranità nazionale e fonti europee: il caso del Consiglio d'Europa", in Grasso, Giovanni, Maugeri, Anna Maria and Sicurella, Rosaria, (eds.): *Tra diritti fondamentali e principi generali della materia penale la crescente influenza della giurisprudenza delle corti europee sull'ordinamento penale italiano*, (Pisa, Pisa University Press), pp. 97-201.

Bernat, Frances (2017): 'Immigration and crime', in Pontell, Henry N. (editor): *Oxford research encyclopedias: Criminology and criminal justice* (New York, Oxford University Press).

Bozano, Luce, Guariso, Alberto, (2009): "Reato di immigrazione clandestina e diritto di difesa", *D&L: Rivista critica di diritto del lavoro*, pp. 1077-1081.

Bucher, Jacob, Manasse Michelle, Tarasawa Beth (2010): "Undocumented Victims: An Examination of Crimes Against Undocumented Male Migrant Workers", *The Southwestern Journal of Criminal Justice*, 7 (2), pp. 159-179.

Caneschi, Gaia (2020): "*Nemo tenetur se detegere* anche nei procedimenti amministrativi sanzionatori? La parola alla Corte di giustizia", *Cassazione penale*, 2, pp. 579-587.

Capuano, Romolo G. (2011), *Immigrants as victims of crime in Italy: an exploratory study* (Saarbrücken, Lambert).

Caputo, Angelo (2010): "La contravvenzione di ingresso e soggiorno illegale davanti alla Corte Costituzionale", *Diritto Penale e Processo*, 16 (10), pp. 1187-1204.

Catalano, Elena M. (2011): "Diritto al silenzio, *right not to be questioned* e tutela della autoincriminazione. Note storico-comparative", *Cassazione Penale*, 11, pp. 4018-4033.

Cavaliere, Antonio(2013): "Diritto penale e politica dell'immigrazione", *Critica del diritto*, 1, pp. 17-43.

Chudžíková, Alena H. and Bargerová, Zuzana (2018): "Victims of labour exploitation or "illegal" migrants? Ukrainian workers' labour rights protection in Slovakia", ec.europa.eu, pp. 1-36.

Comino, Stefano, Mastrobuoni, Giovanni, Nicolò, Antonio (2020): "Silence of the Innocents: Undocumented Immigrants' Underreporting of Crime and their Victimization", *Journal of Policy Analysis and Management*, 39, 4, pp. 1214-1245.

Confalonieri, Sofia (2020): "Il *nemo tenetur se detegere* nel labirinto delle fonti. Riflessioni a margine di Corte cost., ord. n. 117 del 2019", *Diritto Penale Contemporaneo – Rivista Trimestrale*, 1, pp. 108-140.

Crépeau, François and Hastie Bethany (2015): "The case for 'firewall' protections for irregular migrants: safeguarding fundamental rights", *European Journal of Migration Law*, 17, pp. 157-183.

Crocitti, Stefania (2014): "Immigration, Crime, and Criminalization in Italy" in Bucerius, Sandra and Tonry Michael (eds.), *The Oxford Handbook of Ethnicity, Crime, and Immigration* (New York, Oxford University Press), pp. 791-833

Curi, Francesca, Martelloni, Federico, Sbraccia, Alvise, Valentini, Elena (2020), *I migranti sui sentieri del diritto. Profili socio-criminologici, giuslavoristici, penali e processual-penalistici*, (Torino, Giappichelli).

de Graauw, Els (2014): "Municipal ID Cards for Undocumented Immigrants: Local Bureaucratic Membership in a Federal System", *Politics and Society*, 42 (3), pp. 309-330.

Delvino, Nicola (2019): "Safe Reporting of crime for Victims and Witnesses with Irregular Migration Status in the United States", www.compas.ox.ac.uk, pp. 1-44.

Delvino, Nicola, González Beilfuss, Markus (2021): "Latino Migrant Victims of Crime: Safe Reporting for Victims With Irregular Status in the United States and Spain", *American Behavioral Scientist*, 65, pp. 1193-1205.

Delvino, Nicola, Spencer, Sarah (2014): "Irregular Migrants in Italy: Law and Policy on Entitlements to Services", ESRC (COMPAS), University of Oxford, www.compas.ox.ac.uk, pp. 1-38.

Dolinko, David (1986): "Is there a rationale for the privilege against self-incrimination?" *UCLA Law Review*, 33, pp. 1063-1148

Di Martino, Alberto, Biondi Dal Monte, Francesca, Boiano, Ilaria, Raffaelli, Rosa (2013) *The criminalization of irregular migration: law and practice in Italy* (Pisa, PisaUniversity Press).

Escobar Veas, Javier (2022): "A Comparative Analysis of the Case Law of the European Court of Human Rights on the Right against Self-Incrimination", (2022) *Revista Brasileira de Dereito Processual Penal*, 8 (2), pp. 869-901.

Fasani, Francesco, Mastrobuoni, Giovanni, Owens, Emily G., Pinotti, Paolo (2019): *Does Immigration Increase Crime?: Migration Policy and the Creation of the Criminal Immigrant*, (Cambridge, Cambridge University Press).

Fattah, Ezzat A. (1991): *Understanding Criminal Victimization: an introduction to theoretical victimology*, (Scarborough, Prentice-Hall Canada)

Fares, Guerino (2020): "Diritto al silenzio, soluzioni interpretative e controlimiti: la Corte costituzionale chiama in causa la Corte di giustizia", *www.dirittifondamentali.it*, 1, pp. 57-90.

Ferrajoli, Luigi (2009): "La criminalizzazione degli immigrati (Note a margine della l. n. 94/2009)" *Questione Giustizia*, 5, pp. 9-18.

Fussell, Elizabeth (2011): "The deportation threat dynamic and victimization of Latino migrants: Wage theft and robbery", *The Sociological Quarterly*, 52, pp. 593-615.

Gatta, Gian Luigi, Mitsilegas Valsamis and Zirulia Stefano, (eds) (2021): *Controlling Immigration Through Criminal Law. European and Comparative Perspectives on "Crimmigration"* (Oxford, Hart Publishing).

Gatta, Gian Luigi (2009): "Il "reato di clandestinità" e la riformata disciplina penale dell'immigrazione", *Diritto Penale Processo*, pp. 1323-1339.

Garcìa Hernàndez, Cesar C. (2017): *Crimmigration Law*, (Chicago, American Bar Association)

Garland, David (2001), *The Culture of Control: Crime and Social Order in Contemporary Society* (Oxford, Oxford University Press)

Gleeson, Shannon (2018): "Labor rights for all? The role of undocumented immigrant status for worker claims making", *Law & Social Inquiry*, 35, pp. 561-602.

Greenawalt, Kent (1981): "Silence as a Moral and Constitutional Right", *William and Mary Law Review*, , 23, pp. 15-71.

Grevi, Vittorio (1972): "*'Nemo tenetur se detergere'*: Interrogatorio dell'imputato e diritto al silenzio nel processo penale italiano (Milano, Giuffrè).

Gutierrez, Carmen M. and Kirk, David S. (2017): "Silence speaks: The relationship between immigration and the underreporting of crime", *Crime and Delinquency*, 63, pp. 926-950.

Helmholz, Richard H. (1990): "Origins of the Privilege against Self-Incrimination: The Role of the European Ius Commune", *NYU Law Review*, 65, pp. 962-991.

Kelsey, Carl (1926): "Immigration and Crime", *the Annals of the American Academy of Political and Social Sciences*, 125, pp. 165-174

Kittrie, Orde F. (2006): "Federalism, Deportation and Crime Victims Afraid to Call the Police" *Iowa Law Review*, 91, pp. 1449-1508.

Lamberigts, Stijn (2016): "The Privilege against Self-Incrimination: A Chameleon of Criminal Procedure", *New Journal European Criminal Law*, 7(4), pp. 418-438.

Lasagni, Giulia (2020): "Prendendo sul serio il diritto al silenzio: commento a Corte cost., ord. 10 maggio 2019, n. 117", *Diritto Penale Contemporaneo – Rivista Trimestrale* 2, pp. 135-162.

Levy, Leonard W. (1968): *Origins of the Fifth Amendment* (New York, Oxford University Press).

Luparia, Luca (2006), *La confessione dell'imputato nel sistema processuale penale* (Milano Giuffrè).

Luparia, Luca (editor) (2015): *Victims and Criminal Justice. European Standards and National Good Practices*, (Milano, Wolters Kluwer).

McDonald, William F. (editor) (2009): *Immigration, Crime and Justice* (Bingley, Emerald Group Publishing).

Marchesi, Diletta and Panzavolta, Michele (2021): "Keep silence for yourself: The protection of the right to silence in the Italian criminal justice system" *New Journal of European Criminal Law*, 12(3), pp. 365-388.

Martinez, Ramiro, Stowell, Jacob I., Lee, Matthew T. (2010): "Immigration and crime in an era of transformation: A longitudinal analysis of homicides in San Diego neighborhoods, 1980–2000", *Criminology*, 48(3), pp. 797-829.

Masera, Luca (2010): "Corte Costituzionale e immigrazione: le ragioni di una scelta compromissoria", *Rivista Italiana di Diritto e Procedura Penale*, 4, pp. 1373-1395.

Masera Luca (2019): "La *crimmigration* nel decreto Salvini'", *La legislazione penale*, pp. 1-46.

Mazza, Oliviero (2004): *L'interrogatorio e l'esame dell'imputato nel suo procedimento* (Milano, Giuffrè).

Mazzacuva, Francesco (2017): *Le pene nascoste. Topografia delle sanzioni punitive e modulazione dello statuto garantistico* (Torino, Giappichelli).

Messing, Jill T., Becerra, David, Ward-Lasher Allison and Androff, David K. (2015): "'Latinas' perceptions of law enforcement: Fear of deportation, crime reporting, and trust in the system'" *Affilia*, 30 (3), pp. 328-340.

Mentasti, Giulia (2022): 'The criminalisation of migration in Italy: current tendencies in the light of EU law', *New Journal of European Criminal Law,* 13(4), pp. 502-525.

Mowbray, Alastair (2004): *The development of positive obligations under the European Convention on Human Rights by the European Court of Human Rights* (Oxford, Hart Publishing).

Nicosia, Emanuele (2006): *Convenzione europea dei diritti dell'uomo e diritto* penale, (Torino, Giappichelli).

Paonessa, Caterina (2009): *Gli obblighi di tutela penale. La discrezionalità legislativa nella cornice dei vincoli costituzionali e comunitari* (Pisa, ETS)

Patanè, Vania (2006): *Il diritto al silenzio dell'imputato* (Torino, Giappichelli).

Pecorella, Claudia (2016): "'Sicurezza vs. libertà? La risposta penale alle violenze sulle donne nel difficile equilibrio tra istanze repressive e interessi della vittima'", *Diritto Penale Contemporaneo*, p. 1-16.

Pivaty, Anna, Beazley, Ashlee, Daly, Yvonne M., Beckers, Laura, de Vocht, Dorris, ter Vrugt, Peggy (2021): "'Opening Pandora's box: The right to silence in police interrogations and the Directive 2016/343/EU'" *New Journal of European Criminal Law*, 12(3), pp. 328-346.

Pivaty, Anna, Beazley, Ashlee, Daly, Yvonne M., de Vocht, Dorris, ter Vrugt Peggy (2021): "Strengthening the protection of the right to remain silent at the investigative stage: what role for the EU legislator?" *New Journal of European Criminal Law*, 12(3), pp. 427-448.

Recchia Nicola (2020): *Il principio di proporzionalità nel diritto penale. Scelte di criminalizzazione e ingerenza nei diritti fondamentali* (Torino, Giappichelli).

Redmayne, Mike (2007): "'Rethinking the Privilege against Self-Incrimination'", *Oxford Journal of Legal Studies*, 27, pp. 209-232.

Reina, Angelica S., Lohman, Brenda J., Maldonado, Marta M. (2014): ""He said they'd deport me": Factors influencing domestic violence help-seeking practices among Latina immigrants" *Journal of Interpersonal Violence*, 29(4), pp. 593-615.

Rumbaut, Ruben G. and Ewing, Walter A. (2007): "The Myth of Immigrant Criminality and the Paradox of Assimilation: Incarceration Rates among Native and Foreign-Born Men" (Washington, DC, Immigration Policy Center) pp. 1-16.

Sampson, Robert J. (2008): "Rethinking crime and immigration", *Contexts*, 7(1), pp. 28-33.

Schabas, William A. (2016): *The European Convention on Human Rights* (Oxford University Press).

Simon, Jonathan (2007): *Governing Through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear* (Oxford University Press)

Sklansky, David Alan (2012): "Crime, Immigration, and *ad hoc* Instrumentalism", *New Criminal Law Review*, 15(2), pp. 157-223.

Sudre, François (1995): "*Les obligations positives dans la jurisprudence européenne des droits de l'homme*", *Revue Trimestriell des Droits de l'Homme*, pp. 363-384.

Stowell, Jacob.I., Messner, Steven F., McGeever, Kelly F., Raffalovich, Lawrence E. (2009): "Immigration and the recent violent crime drop in the United States: A pooled, cross-sectional time-series analysis of metropolitan areas", *Criminology*, 47(3), pp. 889-928.

Stumpf, Juliet P. (2006): "The Crimmigration Crisis: Immigrants, Crime, and Sovereign Power", *American University Law Review*, 56, pp. 367-419.

Tassinari, Davide (2012): *Nemo tenetur se detegere. La libertà dalle autoincriminazioni nella struttura del reato* (Bologna, Bononia University Press).

Taverriti, Sara Bianca (2017): "La tutela della vittima tra procedibilità a querela e procedibilità d'ufficio", in Bargis Marta and Belluta Hervè, *Vittime di reato e sistema penale. La ricerca di nuovi equilibri* (Torino, Giappichelli), pp. 503-526.

Taverriti, Sara Bianca (2019): "Safe reporting of crime for victims and witnesses with irregular migration status in Italy", COMPAS, University of Oxford, www.compas.ox.ac.uk.

Timmerman, Ruben I., Leerkes, Arjen, Staring, Richard, Delvino, Nicola (2020): "'Free In, Free Out': Exploring Dutch Firewall Protections for Irregular Migrant Victims of Crime", *European Journal of Migration and Law*, 22(3), pp. 427-455.

Viganò, Francesco (2010): "Diritto penale e immigrazione: qualche riflessione sui limiti alla discrezionalità del legislatore", *Questione Giustizia*, 3, pp. 13-36.

Viganò, Francesco (2019): "La tutela dei diritti fondamentali della persona tra corti europee e giudici nazionali" *Quaderni Costituzionali*, pp. 481-502.

Viganò, Francesco (2011): "L'arbitrio del non punire. Sugli obblighi di tutela penale dei diritti fondamentali", in Bertolino Marta, Eusebi Luciano and Forti Gabrio (eds), *Studi in onore di Mario Romano* (Napoli, Jovene), pp. 2645-2704

Vitarelli, Tiziana (2020): "Violenza contro le donne e bulimia repressiva", *Diritto Penale Contemporaneo – Rivista Trimestrale*, 3, pp. 461-484.

Von Hentig, Hans (1948): *The Criminal and his Victim. Studies in the Sociobiology of Crime*, (New Heaven, Yale University Press).

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

http://dpc-rivista-trimestrale.criminaljusticenetwork.eu