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

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"

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.*

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

http://dpc-rivista-trimestrale.criminaljusticenetwork.eu