Banche dati europee e procedimento penale italiano

MITJA GIALUZ
Ricercatore di Procedura penale
Università di Trieste

Sommario: 1. Introduzione. – 2. I sistemi informativi quali strumenti di trasmissione di provvedimenti giudiziari o di richieste inerenti al procedimento. – 3. Le banche dati europee come contenitori di informazioni utili per l'accertamento dei fatti: il limite territoriale. – 4. (Segue): il limite funzionale. – 5. (Segue): il limite derivante dalla tutela del diritto alla protezione dei dati. – 6. Conclusioni.

1. Introduzione

In termini generali, è possibile individuare due tipologie molto diverse di rapporto tra le banche dati europee e il procedimento penale.

Il primo è quello che vede i sistemi informativi – soprattutto quelli centralizzati – impiegati come strumenti di trasmissione di un provvedimento o di una richiesta emessi nel corso di un procedimento giudiziario. In questi casi, la banca dati è destinataria di "impulsi" che provengono dall'autorità giudiziaria.

La seconda relazione, invece, è quella per cui la banca dati rappresenta un contenitore di informazioni, che possono essere utili per l'accertamento dei fatti e delle responsabilità. In quest'ottica, è il procedimento penale a essere destinatario di dati immagazzinati in archivi informatici.

In questo saggio, si analizzeranno entrambe le prospettive, prendendo in considerazione soltanto il procedimento penale italiano. Come si vedrà, la prima non pone particolari problemi sul piano teorico, mentre con riguardo alla seconda si affronteranno due interrogativi inediti e tra loro connessi. Da un lato, la questione relativa al se e in quale misura le banche dati europee possano divenire fonti di prova, ossia operare come sorgenti di elementi cognitivi utilizzabili nel procedimento penale; dall'altro, la domanda relativa al se e in quale misura il rafforzamento delle banche dati e della cooperazione informativa possa consentire di aggirare gli ostacoli della cooperazione giudiziaria.

2. I sistemi informativi quali strumenti di trasmissione di provvedimenti giudiziari o di richieste inerenti al procedimento

Quanto alla prima tipologia di rapporto tra banche dati e procedimento penale, il sistema informativo che più si presta a veicolare atti pronunciati in sede giudiziaria è senz'altro il SIS.

Va ricordata, anzitutto, la segnalazione ai fini dell'arresto, disciplinata dall'art. 95 CAAS, la quale ha gli stessi effetti della domanda di arresto provvisorio ai fini di estradizione prevista dall'art. 16 della Convenzione europea di estradizione[1]. Si è osservato che il numero di segnalazioni inserite ai sensi dell'art. 95 CAAS ai fini dell'arresto o dell'estradizione non è mai stato particolarmente elevato, soprattutto se paragonato a quello relativo alle segnalazioni degli stranieri ai fini della

1 Su tale sistema, cfr. J. P. Pierini, *Iscrizione della richiesta di arresto provvisorio ai fini estradizionali nel SIS, valutazione dell'urgenza e reiterazione dell'arresto ad opera della polizia giudiziaria*, in "Cassazione penale", 2000, p. 3071; L. Salazar, *L'estradizione nella Convenzione di Schengen*, in "Diritto penale e processo", 1998, p. 1034. In giurisprudenza, riconosce l'equiparazione dell'iscrizione nel SIS alla domanda di arresto provvisorio, Cass., sez. VI, 25 giugno 1999, Tepes, in "Cassazione penale", 2000, p. 3069.

non ammissione, effettuate ai sensi dell'art. 96 CAAS[2]. Nondimeno, va rilevato che proprio tale procedura ha consentito nel passato di procedere a importanti arresti, come a quelli di Cuntrera e Caruana in Spagna, o quelli di Gelli e Ocalan[3].

Com'è noto, tale strumento di diffusione è stato valorizzato dalla decisione quadro 2002/584/GAI in materia di mandato d'arresto europeo, la quale ha previsto la possibilità di dare attuazione al mandato d'arresto europeo proprio attraverso la segnalazione nel Sistema di Informazione Schengen (SIS). L'art. 9, par. 2, della decisione attribuisce all'autorità emittente il mandato d'arresto europeo il potere di disporre la segnalazione «in ogni caso», e, quindi, tanto nell'ipotesi in cui il luogo ove si trova il ricercato sia sconosciuto, quanto nell'evenienza in cui esso sia noto, ma vi sia l'esigenza di accelerare la procedura[4]. Per questo, si è sostenuto che la segnalazione nel SIS sarebbe divenuta la modalità ordinaria di trasmissione del mandato di arresto europeo[5]; e, in effetti, le rilevazioni statistiche sembrano confermare questa previsione[6].

Se effettuata conformemente all'art. 95 CAAS, tale segnalazione *equivale* a un mandato d'arresto europeo. Attualmente, però, poiché il SIS non può contenere tutte le informazioni necessarie, si precisa che l'equiparazione opera anche se non vengono inseriti tutti i dati, i quali vengono poi trasmessi dal SIRENE. Il problema dovrebbe essere risolto con l'avvio – ancora incerto nella data – del SIS II: la decisione del Consiglio dell'Unione 2007/533/GAI sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II)

---

2 È stato rilevato che la segnalazione effettuata *ex* art. 95 CAAS non ha mai raggiunto il due per cento di tutti i dati relativi alle persone: cfr. H. Busch, *The dream of total data collection - status quo and future plans for EU information systems*, <http://www.statewatch.org/analyses/no-61-eu-databases.pdf>, p. 1. Per le statistiche più recenti, cfr. il *Documento SIS Database Statistics dd. 01/01/2008, n. 5441/08*, 30 gennaio 2008, <http://register.consilium.europa.eu/pdf/en/08/st05/st05441.en08.pdf>, p. 2; nonché, il *Documento SIS Database Statistics dd. 01/01/2009, n. 5764/09*, 28 gennaio 2009, <http://register.consilium.europa.eu/pdf/en/09/st05/st05764.en09.pdf>, p. 2.

3 Cfr. A. De Felice, "Intervento", in Corpus iuris, *pubblico ministero europeo e cooperazione internazionale*, a cura di M. Bargis e S. Nosengo, Milano, 2003, p. 36. Per ulteriori casi di applicazione del SIS quale mezzo di trasmissione di richieste di estradizione, M. Pisani, *Domanda di arresto provvisorio a fini estradizionali e Sistema d'Informazione Schengen*, in "Rivista italiana di diritto e procedura penale", 2001, p. 332; Id., *Francia-Germania: il caso Sirven e il Sistema Schengen*, *ibidem*, p. 569.

4 V. M. Bargis, *Il mandato di arresto europeo dalla decisione quadro alle prospettive di attuazione*, in "Politica del diritto", 2004, p. 91.

5 Così, P. Troisi, "L'arresto operato dalla polizia giudiziaria a seguito della segnalazione nel sistema di informazione Schengen", in *Mandato di arresto europeo e procedure di consegna*, a cura di L. Kalb, Milano, Giuffrè, 2005, p. 176, 219 s.

6 V. il *Documento del Consiglio n. 10330/2/08*, 16 settembre 2008, <http://register.consilium.europa.eu/pdf/en/08/st10/st10330-re02.en08.pdf>, p. 3; *Documento del Consiglio n. 11371/2/07*, 27 luglio 2007, <http://register.consilium.europa.eu/pdf/en/07/st11/st11371-re02.en07.pdf>, p. 3. Anche secondo G. De Amicis, "Mandato d'arresto europeo", in *Lezioni di diritto penale europeo*, a cura di G. Grasso e R. Sicurella, Milano, Giuffrè, 2007, p. 568, l'impiego del SIS per la trasmissione del mandato d'arresto ha un'alta incidenza statistica.

prevede, infatti, che, «nel caso di persone ricercate per l'arresto a fini di consegna sulla scorta di un mandato d'arresto europeo, lo Stato membro della segnalazione inserisce nel SIS II una copia del mandato d'arresto europeo originale» (art. 27). Resta, inoltre, salvo lo scambio di ulteriori informazioni mediante gli uffici SIRENE.

La scelta di consentire la diffusione del mandato d'arresto mediante il SIS ha suscitato qualche perplessità da parte della dottrina, la quale ha rilevato che il sistema di informazione Schengen risulta inquinato da dati scorretti o non aggiornati[7]. Non si può negare che la constatazione sia per certi versi corretta: invero, si è lamentata spesso l'inefficienza dei meccanismi volti ad assicurare l'aggiornamento e la cancellazione dei dati inseriti nel SIS o, sul piano soggettivo, il diritto all'autodeterminazione informativa[8].

Ciò induce evidentemente a richiedere che siano migliorati i controlli sul SIS e che siano garantiti in termini effettivi i diritti di accesso, rettifica e cancellazione dei dati inseriti nel SIS. Da questo punto di vista, è fondamentale la piena attuazione della norma dell'art. 111 CAAS (e domani dell'art. 59 decisione 2007/533/GAI), la quale riconosce a chiunque il diritto di adire la giurisdizione o l'autorità competente in base al diritto nazionale con un'azione di rettifica, di cancellazione, di informazione o di indennizzo relativamente ad una segnalazione che lo riguardi[9]. Nondimeno, il funzionamento imperfetto dei meccanismi garantistici – riscontrato, giova specificarlo, soprattutto con riferimento alle segnalazioni effettuate *ex* art. 96 CAAS – non sembra poter condurre addirittura a contestare alla radice la stessa possibilità di impiegare il SIS per diffondere il mandato d'arresto europeo.

Per quel che riguarda specificamente la disciplina nazionale, che ha recepito la decisione quadro, occorre distinguere tra procedura passiva e attiva.

Quanto alla prima, l'art. 11 l. 69 del 2005 prevede che, «nel caso in cui l'autorità competente dello Stato membro ha effettuato la segnalazione nel Sistema di informazione Schengen (SIS) nelle forme richieste, la polizia giudiziaria procede all'arresto della persona ricercata». L'arresto segna l'inizio della procedura passiva: la polizia dovrà, infatti, porre l'interessato immediatamente – e comunque

---

7 Cfr. S. Buzzelli, "Il mandato d'arresto europeo e le garanzie costituzionali sul piano processuale", in *Mandato d'arresto europeo. Dall'estradizione alle procedure di consegna*, a cura di M. Bargis ed E. Selvaggi, Torino, Giappichelli, 2005, p. 101.

8 Da ultimo, v. E. Brouwer, *The Other Side of Moon The Schengen Information System and Human Rights: A Task for National Courts*, <http://shop.ceps.eu/BookDetail.php?item__id=1642>, pp. 5 sgg.

9 Come ha rilevato E. Brouwer, *op. cit.*, p. 1, riprendendo quanto affermato dall'autorità di controllo Schengen, «the cornerstone in safeguarding data subjects' rights is the enforcement of final court decisions and data protection authorities by the member state issuing the SIS alert». Peraltro, la stessa Autorità di controllo ha rilevato come l'attuazione dell'art. 111 CAAS sia tutt'altro che soddisfacente (*Rapport de l'Autorité de contrôle commune de Schengen sur une enquête relative à la mise en œuvre de l'article 111 de la Convention d'application de l'Accord de Schengen*, 18 gennaio 2008, <http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/shengen/rapport__schengen__article__111__francais.pdf>, p. 19).

non oltre ventiquattro ore – a disposizione del presidente della corte d'appello e dare immediata comunicazione dell'avvenuto arresto al Ministro della giustizia. Quest'ultima informazione è indispensabile – anche laddove la segnalazione nel SIS sia corredata di tutte le informazioni che lo rendono equivalente al mandato d'arresto europeo – per consentire al Ministro di attivarsi per chiedere l'inoltro del mandato e della documentazione ulteriore richiesta dall'art. 6, comma 4, l. 69 del 2005. La trasmissione del verbale al presidente della corte d'appello nel cui distretto l'arresto è stato eseguito è necessaria invece al fine di porre l'organo monocratico in condizione di decidere sulla convalida del provvedimento restrittivo della libertà personale, entro le successive quarantotto ore[10]. Ove non risulti che l'arresto sia stato eseguito per errore di persona o fuori dei casi previsti dalla legge, il presidente lo convalida con ordinanza, la quale, però, perde efficacia se, entro dieci giorni, non perviene il mandato d'arresto europeo o la segnalazione della persona nel SIS, corredata di tutte le indicazioni previste dall'art. 6 l. 69 del 2005.

Dottrina e giurisprudenza si sono soffermate su diversi i profili della disciplina, ma, per quel che ci riguarda, merita porre in rilievo due snodi problematici.

Il primo concerne la valenza della segnalazione del SIS ai fini dell'arresto: sulla scorta della lettura congiunta dell'art. 11 l. 69 del 2005, dell'art. 9 della decisione quadro e degli artt. 64 e 95 CAAS, la dottrina aveva prospettato il carattere automatico dell'arresto[11]. In effetti, la giurisprudenza ha confermato che, in presenza di una segnalazione nel SIS, l'arresto da parte della polizia giudiziaria si configura come «atto 'dovuto'»: esso è subordinato soltanto alla verifica che la relativa segnalazione sia stata effettuata da una "autorità competente" di uno Stato membro dell'Unione europea e che la stessa sia avvenuta nelle "forme richieste", mentre va esclusa qualsiasi valutazione in ordine all'urgenza dell'arresto[12]. Inoltre, si è precisato che l'obbligo dell'arresto deriva dalla mera segnalazione nel SIS, la quale può anche precedere temporalmente il mandato d'arresto europeo: la segnalazione nel SIS equivale, infatti, a una «richiesta di 'arresto preventivo ai fini della consegna'»[13].

Siffatta disciplina ha suscitato più di qualche perplessità, nella parte in cui configura l'arresto come automatico. Si è sostenuto, invero, che essa non sarebbe pienamente compatibile con l'art. 13, comma 3, Cost., il quale richiede la ricorrenza di «casi eccezionali di necessità e urgenza» affinché l'autorità di pubblica

---

10 Cfr., per tutti, M.R. Marchetti, "Mandato d'arresto europeo", in *Enciclopedia del diritto. Annali*, II.1, Milano, Giuffrè, 2008, p. 548.

11 Cfr. N. Galantini, *L'adattamento del mandato d'arresto europeo nella legge attuativa della decisione quadro*, in "Cassazione penale", 2005, p. 4089; Ead., *Prime osservazioni sul mandato d'arresto europeo*, in "Foro ambrosiano", 2002, p. 267.

12 Così, Cass., sez. VI, 5 giugno 2006, Volanti, in "Diritto e giustizia", 2006, n. 28, p. 56. Analogamente, O. Villoni, "Il mandato d'arresto europeo: autorità competenti e contenuto", in *Mandato d'arresto europeo*, cit., p. 200.

13 Testualmente, Cass., sez. VI, 22 novembre 2005, Calarese, in "Foro italiano", 2006, II, c. 280.

sicurezza possa adottare provvedimenti provvisori di limitazione della libertà personale[14]. Secondo un'interpretazione costituzionalmente orientata sarebbe pertanto necessaria una valutazione sull'urgenza e, pertanto, sull'esistenza di un concreto pericolo di fuga da parte della persona segnalata[15]. In realtà, la Cassazione ha dichiarato manifestamente infondata la questione di legittimità costituzionale sollevata con riferimento all'art. 11 nella parte in cui esclude un tale vaglio: a detta dei giudici di legittimità, infatti, nel caso in questione non può essere invocato l'art. 13, comma 3, Cost., perché non si è in presenza di un arresto eseguito in un caso eccezionale dalla polizia giudiziaria, ma dell'esecuzione di un provvedimento della competente autorità giudiziaria[16].

Il secondo profilo problematico concerne gli atti che debbono essere trasmessi per evitare la caducazione del provvedimento di convalida adottato dal presidente della corte di appello: come si è notato, l'art. 13 l. 69 del 2005 prevede che l'ordinanza di convalida perde efficacia se, nei dieci giorni successivi all'adozione, non perviene il mandato di arresto oppure la segnalazione della persona nel SIS, la quale equivale al mandato d'arresto «purché contenga le indicazioni di cui all'articolo 6». Ora, proprio quest'ultimo richiamo ha suscitato qualche dubbio interpretativo, in quanto l'art. 6 prevede al primo comma una serie di elementi che sono presenti nel mandato d'arresto e, quindi, anche nella segnalazione nel SIS; al comma quarto, invece, contempla la trasmissione di atti ulteriori il cui contenuto non si desume generalmente dalla segnalazione nel SIS. Pertanto, la giurisprudenza è stata chiamata a chiarire se il provvedimento perda efficacia anche nel caso di trasmissione della sola segnalazione non accompagnata da tali atti (in particolare, il problema si è posto con riguardo al mancato invio della relazione sui fatti addebitati alla persona). La Corte di cassazione ha escluso tale eventualità, ritenendo che l'equipollenza della segnalazione rispetto al mandato d'arresto sussiste quando essa presenta i requisiti di cui al comma primo dell'art. 6 l. 69 del 2005: insomma, il richiamo all'art. 6 andrebbe limitato alla sola disposizione del primo comma[17].

---

14 V. M. Tiberi, *Il mandato d'arresto europeo*, Roma, Istituto Poligrafico e Zecca dello Stato, 2006, p. 104; P. Troisi, *op. cit.*, pp. 213 sg.

15 In questi termini, A. Scalfati, *La procedura passiva di consegna*, in "Diritto penale e processo", 2005, p. 950.

16 Così, Cass., sez. VI, 5 giugno 2006, Volanti, cit., p. 56.

17 Cass., sez. VI, 13 dicembre 2005, Cusini, in "Cassazione penale", 2006, p. 3567, la quale ha precisato che «la relazione, al pari degli altri elementi indicati nel comma 4, è necessaria ai fini della decisione sulla richiesta di consegna, ma non costituisce elemento necessario della segnalazione»; analogamente, da ultimo, Cass., sez. VI, 23 aprile 2008, R.P., in "CED Cassazione", n. 239427; Cass., sez. VI, 23 dicembre 2008, P.m. in c. S.B., inedita. In termini critici rispetto a tale soluzione giurisprudenziale, R. Belfiore, *Mandato d'arresto europeo e segnalazione nel SIS: quali atti possono essere richiesti all'autorità di emissione?*, in "Cassazione penale", 2006, pp. 4121 sgg.; D. Servi, *Mandato di cattura europeo: segnalazione nel S.I.S. e requisiti necessari alla misura cautelare*, *ivi*, 2006, pp. 3572 sgg.; nonché, in precedenza, A. Barazzetta-R. Bricchetti, *Misure cautelari: rinvii*

In relazione alla procedura attiva, l'art. 29, comma 2, l. n. 69 del 2005 assegna direttamente all'autorità giudiziaria competente per l'emissione del mandato – ossia al giudice, se si tratta di mandato basato su un provvedimento cautelare e al pubblico ministero, se si è al cospetto di un mandato vòlto a eseguire una sentenza definitiva – il potere di disporre l'inserimento nel SIS della segnalazione della persona. Concretamente, l'autorità giudiziaria, dopo aver adottato il mandato d'arresto secondo un modello corrispondente a quello allegato alla decisione quadro, dovrà predisporre i formulari Schengen A ed M – che contengono le informazioni richieste dall'art. 95, par. 2, CAAS – e trasmetterli alla Divisione SIRENE della Direzione Centrale di Polizia Criminale-Servizio per la Cooperazione Internazionale di Polizia[18]. Peraltro, fintanto che non sarà operativo il SIS-II, al quale aderiranno tutti gli Stati membri dell'Unione, l'autorità emittente dovrà diffondere le ricerche attraverso il Servizio Interpol (per quel che riguarda gli Stati non connessi al SIS). Essa dovrà, inoltre, provvedere, tramite il competente ufficio di polizia, a inserire i dati relativi alla persona ricercata nel Sistema Informatizzato Interforze di polizia[19]. Sempre alla stessa autorità giudiziaria competente ai sensi dell'art. 28 l. 69 del 2005 spetterà chiedere l'eliminazione della segnalazione dal SIS, nel caso di revoca, annullamento o perdita di efficacia del provvedimento restrittivo[20].

A parte la segnalazione effettuata per consentire l'esecuzione di un mandato d'arresto europeo – che, ove non si applichi la decisione quadro avrà l'efficacia della richiesta di arresto per fini di estradizione –, la Convenzione di applicazione dell'accordo di Schengen contempla altre segnalazioni che sono volte a consentire l'esecuzione – in luoghi non predefinibili – di atti rilevanti per il procedimento penale.

Giova ricordare, anzitutto, la segnalazione prevista dall'art. 98 CAAS. Siffatta disposizione consente di inserire nel sistema, su richiesta dell'autorità giudiziaria, i dati «relativi ai testimoni, alle persone citate a comparire dinanzi all'autorità giudiziaria nell'ambito di un procedimento penale per rispondere di fatti che sono stati loro ascritti, o relativi alle persone alle quali deve essere notificata una sentenza penale o una richiesta»: la segnalazione viene introdotta ai fini della co-

---

al rito da decifrare, in "Guida al diritto", 2005, n. 19, pp. 85-86; A. Scalfati, *La procedura passiva di consegna*, cit., p. 949. Nella giurisprudenza di merito, va segnalata anche Corte App. Bologna, 21 giugno 2005, Guillemin, in "Foro italiano", 2005, II, c. 522, la quale ha riconosciuto che il giudice può decidere anche sulla richiesta di esecuzione sulla base degli atti trasmessi attraverso il SIS e alla documentazione inviata tramite il SIRENE.

18 Cfr. la *Circolare ministeriale n. 1-1489/05/U del 24 giugno 2005*, in "Rivista italiana di diritto e procedura penale", 2006, p. 389; nonché, G. Iuzzolino, *L'emissione del mandato d'arresto europeo tra ermeneutica e prassi*, in "Cassazione penale", 2008, p. 2126.

19 V. ancora G. Iuzzolino, *L'emissione del mandato d'arresto europeo*, cit., p. 2127.

20 Cfr. F. Siracusano, "Il procedimento di emissione del mandato d'arresto europeo", in *Mandato d'arresto europeo*, cit., p. 406.

municazione del luogo di soggiorno o del domicilio dei soggetti. Nella decisione 2007/533/GAI tale segnalazione viene implementata: il capo VII è dedicato proprio alla «segnalazione di persone ricercate per presenziare ad un procedimento giudiziario» e l'art. 35 prevede che le informazioni richieste vengano comunicate allo Stato membro richiedente «tramite scambio di informazioni supplementari», laddove oggi la trasmissione avviene conformemente alla disciplina nazionale e alle vigenti convenzioni relative all'assistenza giudiziaria (art. 98, par. 2, CAAS). Negli anni, il numero di soggetti segnalati per fini giudiziari è progressivamente cresciuto – si è passati dalle 35.317 segnalazioni *ex* art. 98 CAAS presenti nel 2005, alle 64.684 del 2008, e, infine, alle 72.958 segnalazioni presenti nel 2009[21] –, ma siffatta opportunità non è ancora sufficientemente praticata, nonostante la sua indubbia utilità anche al fine di ridurre il numero degli irreperibili.

Altrettanto significativa nell'ottica della ricerca di un oggetto rilevante ai fini dell'accertamento penale è la segnalazione prevista dall'art. 100 CAAS. Tale norma consente, infatti, di inserire nel SIS i «dati relativi agli oggetti ricercati a scopo di sequestro o di prova in un procedimento penale». Per la verità, non può trattarsi di qualsiasi bene, ma soltanto degli oggetti rubati, altrimenti sottratti o smarriti, indicati dalla stessa statuizione. Si tratta di veicoli a motore di una certa cilindrata, di rimorchi e roulotte, di armi da fuoco, di documenti intatti o di documenti d'identità rilasciati (passaporti, carte d'identità, patenti di guida) oppure, infine, di banconote registrate.

In effetti, questa forma di segnalazione è ben più utilizzata, tant'è che la decisione SIS II – nell'apposito capo intitolato «segnalazione di oggetti a fini di sequestro o di prova in un procedimento penale» – ha esteso il novero degli oggetti che possono essere segnalati, ricomprendendovi natanti e aeromobili, certificati di immatricolazione per veicoli e targhe di veicoli, nonché valori mobiliari e mezzi di pagamento, quali assegni, carte di credito, obbligazioni, titoli e azioni, rubati, altrimenti sottratti, smarriti o falsificati (art. 38). Anche per queste segnalazioni, la decisione SIS II ha previsto che, qualora dall'interrogazione emerga l'esistenza di una segnalazione per un oggetto rinvenuto, l'autorità che la constata si mette in contatto con l'autorità che ha effettuato la segnalazione per concordare le misure necessarie e che le indicazioni relative vengano trasmesse tramite il veicolo delle informazioni supplementari.

Come si vede, il sistema informativo Schengen presenta molteplici possibilità di impiego in relazione al procedimento penale (inteso in senso lato). A seconda delle scelte del legislatore europeo, esso potrà fungere da vero e proprio canale di trasmissione di quella che è stata suggestivamente definita eurordinan-

---

21 Cfr. *Documento SIS Database Statistics dd. 01/01/2005*, 2 giugno 2005, <http://register.consilium.europa.eu/pdf/en/05/st08/st08621.en05.pdf>, p. 2; *Documento SIS Database Statistics dd. 01/01/2008*, cit., p. 2; nonché, il *Documento SIS Database Statistics dd. 01/01/2009*, cit., p. 2.

za[22] – come accade nel caso del mandato d'arresto europeo – oppure potrà funzionare come mezzo di ricerca preliminare che rende possibile l'innesco di una cooperazione giudiziaria: la scoperta della persona o dell'oggetto aprirà infatti un procedimento di cooperazione, che varia a seconda degli strumenti giuridici disponibili.

Nell'ipotesi in cui il bene individuato tramite il SIS vada sottoposto a sequestro o confisca, potrà essere adottato un provvedimento di blocco o di sequestro ai sensi della decisione quadro 2003/577/GAI[23]. Per la verità, in tal caso, il sistema SIS potrebbe forse essere utilizzato anche come strumento indiretto di esecuzione di un provvedimento già adottato in relazione a un bene la cui localizzazione non sia nota: in tale evenienza, la segnalazione nel SIS potrebbe essere volta a localizzare il bene e, quindi, in ultima analisi, a eseguire il provvedimento. Non si ha invece la possibilità di una vera e propria trasmissione dell'eurordinanza tramite il SIS, in quanto l'art. 4 della decisione quadro ne prevede in ogni caso l'invio diretto all'autorità giudiziaria competente per l'esecuzione. Qualora questa non sia nota, si prescrive che l'autorità giudiziaria dello Stato di emissione si attivi attraverso tramite i punti di contatto della Rete giudiziaria europea.

Nel caso in cui la segnalazione si riferisca a un bene ai fini di prova, la sua scoperta potrà condurre oggi all'emissione di un mandato europeo di ricerca della prova volto ad acquisire l'oggetto: dopo un *iter* preparatorio piuttosto travagliato è giunta in porto la decisione quadro relativa al mandato europeo di ricerca delle prove (2008/978/GAI)[24]. Il problema è che questa non contempla il SIS quale pos

---

22 Cfr. G. Iuzzolino, "La decisione sull'esecuzione del mandato d'arresto europeo", in *Mandato d'arresto europeo*, cit., p. 274.

23 In *GUUE*, L 196, 2 agosto 2003, p. 45.

24 In *GUUE*, L 350, 30 dicembre 2008, p. 72. Sul mandato europeo di ricerca della prova, cfr., tra i tanti, S. Allegrezza, "Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello spazio giudiziario europeo", in *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia*, a cura di T. Rafaraci, Milano, Giuffrè, 2007, p. 691; R. Belfiore, *Il mandato europeo di ricerca delle prove e l'assistenza giudiziaria nell'Unione europea*, in "Cassazione penale", 2008, p. 3894; G. De Amicis, *Cooperazione giudiziaria e corruzione internazionale*, Milano, Giuffrè, 2007, pp. 156 sgg.; Id., *Il mandato europeo di ricerca delle prove: un'introduzione*, in "Cassazione penale", 2008, p. 3033; A. IJzerman, "From the CATS Portfolio: The European evidence warrant", in *European evidence warrant. Transnational Judicial Inquiries in the EU*, a cura di J.A.E. Vervaele, Antwerpen, Intersentia, 2005, pp. 5 sgg.; N. La Rocca, "Prova (prospettive europee)", in *Digesto delle discipline penalistiche*, IV Agg., Torino, Utet, 2008, pp. 840 sgg.; G. Melillo, "Il mutuo riconoscimento e la circolazione della prova", in *L'area di libertà sicurezza e giustizia*, cit., p. 465; J.R. Spencer, "The problems of trans-border evidence and European initiatives to resolve them", in *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, a cura di G. Grasso e R. Sicurella, Milano, Giuffrè, 2008, p. 477; C. Williams, "Overview of the Commission's proposal for a Framework Decision on the European evidence warrant", in *European evidence warrant*, cit., pp. 69 sgg. Da ultimo, si veda la *Relazione sulla proposta di decisione quadro del Consiglio relativa al mandato europeo di ricerca delle prove diretto all'acquisizione di oggetti, documenti e dati da utilizzare nei procedimenti penali*

sibile veicolo di trasmissione del mandato europeo: l'art. 8 prevede, infatti, che il MER (mandato europeo di ricerca delle prove) possa essere trasmesso direttamente «all'autorità competente di uno Stato membro in cui l'autorità competente dello Stato di emissione abbia motivi legittimi per ritenere che si trovino o, nel caso di dati elettronici, che siano direttamente accessibili in base alla legislazione dello Stato di esecuzione oggetti, documenti o dati pertinenti». Anche in tal caso, come in quello della decisione n. 577 del 2003, l'alternativa è la trasmissione mediante il sistema di telecomunicazione protetto della Rete giudiziaria europea (art. 8, par. 3).

La scelta compiuta dal legislatore europeo dipende probabilmente dalla circostanza che l'emissione del mandato di ricerca della prova presuppone generalmente la previa identificazione dell'oggetto e quindi dello Stato in cui si trova il bene. Il sistema che ne deriva è tale per cui, per ricercare un bene da acquisire a fini di prova, si può utilizzare il SIS: solo una volta che tale bene sia individuato, si potrà emettere il MER e trasmetterlo direttamente all'autorità dello Stato competente. Siffatta opzione appare limitativa, soprattutto se la si confronta con quella effettuata in tema di mandato d'arresto, ove pure viene in gioco il bene essenziale della libertà personale. In particolare, appare irragionevole che l'inserimento nel SIS a fini di ricerca dell'oggetto di prova possa riguardare soltanto determinati beni (come si è visto, solo quelli indicati nell'art. 100 e nell'art. 38 decisione SISII).

3. Le banche dati europee come contenitori di informazioni utili per l'accertamento dei fatti: il limite territoriale

Ancor più interessante e problematica si presenta la prospettiva *lato sensu* probatoria, che vede i soggetti coinvolti nel procedimento penale come fruitori delle informazioni *contenute nelle* o *prodotte dalle* banche dati europee.

Da questo punto di vista, la domanda centrale è se, e in quale misura, le banche dati europee possono operare come fonti di prova in senso tecnico, ossia come sorgenti di elementi cognitivi utilizzabili nel procedimento penale. La risposta a tale interrogativo passa attraverso una precisazione preliminare e l'analisi di tre profili problematici strettamente connessi tra di loro.

La precisazione riguarda la nozione di banche dati europee, la quale va intesa in senso molto ampio. In essa vanno ricompresi, tanto gli archivi centrali dell'Unione – quali SIS, SID, TECS di Europol, EPOC-II di Eurojust, Eurodac, VIS –, quanto le banche dati istituite a fini preventivi e repressivi dai singoli Stati membri, quali in particolare le banche dati di polizia[25], gli archivi contenenti in-

---

(13076/2007 – C6-0293/2008 – 2003/0270(CNS), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2008-0408+0+DOC+PDF+V0//IT>, pp. 1 sgg.

25 Si allude ad archivi corrispondenti a quello che è il Centro elaborazione dati del Dipartimento

formazioni dattiloscopiche[26] e le banche dati genetiche[27]. Proprio l'attuazione del principio di disponibilità ha portato anzitutto all'introduzione di legami più o meno stretti tra queste diverse basi di dati nazionali, secondo il modello dell'in-

---

della pubblica sicurezza, istituito presso il Ministero dell'Interno (Ufficio per il coordinamento e la pianificazione), con l'art. 8 l. 1 aprile 1981, n. 121: al riguardo, per tutti, M. Bonetti, *Riservatezza e processo penale*, Milano, Giuffrè, 2003, pp. 288 sgg.; G. Buttarelli, *Banche dati e tutela della riservatezza*, Milano, Giuffrè, 1997, pp. 565 sgg.; A.A. Dalia, sub *artt. 7-11*, in "Legislazione penale", 1982, pp. 50 sgg.; P. Gallerini Monaci, *Il Centro elaborazione dati presso il Ministero dell'interno. Problemi e prospettive*, in "Rivista trimestrale di diritto e procedura civile", 1984, pp. 540 sgg.; A. Intini – A.R. Casto – D.A. Scali, *Investigazione di polizia giudiziaria*, Roma, Laurus Robuffo, 2006[7], pp. 91 sgg.; L. Mone, *L'amministrazione della pubblica sicurezza e l'ordinamento del personale*, Roma, Laurus Robuffo, 2007[15], p. 62; M. Pisani, *Criminalità organizzata e cooperazione internazionale*, in "Rivista italiana di diritto e procedura penale", 1998, p. 711. Solo per citarne alcune, si pensi al *Police National Computer*, operante presso l'*Home Office* della Gran Bretagna (cfr. *Database State*, <http://www.jrrt.org.uk/uploads/database-state.pdf>, pp. 21 sg.; T. Thomas, *Criminal Records. A Database for Criminal Justice System and Beyond*, New York, Palgrave Macmillan, 2007, pp. 27 sgg.), o all'INPOL, utilizzato dal *Bundeskriminalamt* tedesco (cfr. *The Bundeskriminalamt Facts and Figures 2008*, <http://www.bka.de/profil/broschueren/facts2008.pdf>, p. 10), oppure, ancora, al *Système de circulation hiérarchisée des enregistrements opérationnels de la police sécurisés* (CHEOPS), impiegato dalla polizia francese (cfr. A. Bauer - C. Soullez, *Fichiers de police et de gendarmerie. Comment améliorer leur contrôle et leur gestion?*, Parigi, La Documentation française, 2007, pp. 15 sgg.).

26 Il riferimento è alle banche dati corrispondenti a quella del Casellario Centrale d'Identità, istituito presso il servizio polizia scientifica della direzione centrale anticrimine della polizia di Stato, che utilizza il sistema automatizzato AFIS e contiene i cartellini segnaletici di circa quattro milioni di persone (così, A. Spinela – G. Solla, *L'identificazione personale nell'investigazione scientifica: DNA e impronte*, in "Cassazione penale", 2009, p. 433; nonché, A. Intini – A.R. Casto – D.A. Scali, *op. cit.*, p. 138). Si pensi, ad esempio, al *National Fingerprint Database* (IDENT1), che consente alle forze di polizia di Inghilterra, Scozia e Galles, di confrontare più di sedici milioni di «sets of ten-prints» (cfr. <http://www.npia.police.uk/en/10504.htm>; nonché, *Database State*, cit., p. 23), oppure al sistema identificativo utilizzato dal *Bundeskriminalamt* tedesco, che conserva i dati relativi a più di tre milioni di persone (v. *The Bundeskriminalamt*, cit., p. 8), o, ancora, al *Fichier automatisé des empreintes digitales* (FAED), istituito nel 1987 e comune a polizia e *gendarmerie* (v. A. Bauer - C. Soullez, *op. cit.*, pp. 44 sgg.).

27 Al riguardo, si leggano, anche per ulteriori indicazioni bibliografiche, G. Capoccia, *Istituzione di una banca dati del DNA a fini identificativi e di giustizia*, in "Rassegna penitenziaria e criminologica", 2007, pp. 47 sg.; C. Fanuele, *Un archivio centrale per i profili del DNA nella prospettiva di un "diritto comune" europeo*, in "Diritto penale e processo", 2007, pp. 386 sgg.; P. Felicioni, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Milano, Ipsoa, 2007, pp. 193 sgg.; C. McCartney, *Forensic Identification and Criminal Justice. Forensic science, justice and risk*, Portland, Willan Publishing, 2006, pp. 159 sgg.; P.D. Martin – H. Schmitter – P.M. Schneider, *A brief history of the formation of DNA databases in forensic science within Europe*, in "Forensic Science International", 2001, pp. 225 sgg.; A. Moustiers, "Preuve et biotecnologies: l'utilisation des empreintes génétiques à des fins judiciaires", in *La preuve pénale. Internationalisation et nouvelles technologies*, a cura di O. de Frouville, Parigi, La Documentation française, 2007, pp. 177 sgg.; L. Picotti, *Trattamento dei dati genetici, violazioni della* privacy *e tutela dei diritti fondamentali nel processo penale*, in "Il diritto dell'informazione e dell'informatica", 2003, pp. 722 sgg.; L. Scaffardi, *Le Banche dati genetiche per fini giudiziari e i diritti della persona*, <http://www.forumcostituzionale.it/site/images/stories/pdf/documenti__forum/paper/0114__scaffardi.pdf>; P.M. Schneider – P.D. Martin, *Criminal DNA databases: the European situation*, in "Forensic Science International", 2001, pp. 232 sgg.

terconnessione (dei casellari giudiziari) ovvero dell'accesso on-line indiretto o diretto (previsto dal trattato di Prüm e dalla decisione 2008/615/GAI con riguardo rispettivamente ai dati indicizzati contenuti negli schedari di analisi del DNA e ai sistemi automatizzati d'identificazione dattiloscopica). In secondo luogo, ha condotto al rafforzamento dell'obbligo di trasmissione dei dati contenuti in archivi nazionali secondo quanto previsto dalla decisione 2009/315/GAI, in materia di casellario giudiziario e dalla decisione quadro 2006/960/GAI per le banche dati gestite direttamente dalle autorità di *law enforcement* oppure per quelle alle quali siffatte autorità hanno accesso diretto[28].

I tre profili problematici che andranno affrontati coincidono con tre possibili limiti all'utilizzo delle banche dati europee quali fonti di prova. Il primo ha natura spaziale e dipende dalla circostanza che le banche dati europee contengono informazioni raccolte al di fuori del territorio nazionale. Il secondo limite ha natura funzionale ed è legato all'individuazione dei canali attraverso i quali i dati possono essere immessi nel procedimento penale, dal momento che si tratta spesso di informazioni raccolte nel corso di indagini amministrative. Il terzo limite si ricollega direttamente alla tutela del diritto alla protezione dei dati personali.

---

28 Riprendendo implicitamente la distinzione – operata da G. Vermeulen - T. Vander Beken - L. Van Puyenbroeck - S. Van Malderen, *Availability of law enforcement information in the European Union. Between mutual recognition and equivalent right of access*, Antwerp-Apeldoorn, Maklu, 2005, p. 15 – tra le informazioni alle quali le autorità di *law enforcement* hanno accesso autonomamente e quelle per le quali è necessaria un'autorizzazione dell'autorità giudiziaria, la decisione quadro 960 del 2006 attua il canone di disponibilità solo rispetto alle prime. Tra esse vengono annoverate però tre categorie di dati. Anzitutto, quelli detenuti direttamente da autorità incaricate dell'applicazione della legge (art. 2, lett. c). In secondo luogo, le informazioni «conservate in una banca dati alla quale un'autorità incaricata dell'applicazione della legge può accedere direttamente» (art. 4, par. 1): si pensi, solo per fare un esempio, agli elenchi di tutti i propri abbonati e di tutti gli acquirenti del traffico prepagato della telefonia mobile, che le imprese sono tenute a rendere disponibili, anche per via telematica, al centro di elaborazione dati del Ministero dell'interno (ai sensi dell'art. 55, comma 7, d.lgs. 1 agosto 2003, n. 259) (per un panorama comparato delle informazioni alle quali le autorità di *law enforcement* hanno accesso, cfr. ancora G. Vermeulen - T. Vander Beken - L. Van Puyenbroeck - S. Van Malderen, *op. cit.*, p. 15). Infine, la decisione prende in considerazione anche «qualsiasi tipo di informazioni o dati detenuti da autorità pubbliche o da enti privati che siano accessibili alle autorità incaricate dell'applicazione della legge *senza il ricorso a mezzi coercitivi*»; in tal caso, si può trattare di qualsiasi informazione, anche non contenuta in una banca dati, che l'autorità di *law enforcement* può conseguire senza la necessità dell'autorizzazione dell'autorità giudiziaria. Per quel che riguarda i dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, dipenderà dai singoli ordinamenti: com'è noto, la direttiva 2006/24/CE ne prescrive la conservazione per un periodo non inferiore a sei mesi e non superiore a due anni dalla data della comunicazione (art. 6), ma rinvia agli ordinamenti nazionali la disciplina relativa all'accesso (cfr. il considerando n. 25), prevedendo soltanto che esso sia consentito solo alle «autorità nazionali competenti»: è possibile che, in alcuni ordinamenti, queste siano le stesse autorità di *law enforcement* e, in tal caso, si potrà ritenere attuato appieno anche per questi dati il canone di disponibilità (cfr. *supra*, M. Gialuz, "La cooperazione informativa quale motore del sistema europeo di sicurezza", § 5).

Prendendo le mosse dal primo aspetto, si tratta di capire se e in che misura le banche dati europee e gli strumenti giuridici che prevedono lo scambio di informazioni tra di esse possono garantire la libera circolazione dei dati anche nell'ottica del procedimento penale. È evidente che tutti i modelli di collegamento delle banche dati nazionali e, a maggior ragione, le banche dell'Unione garantiscono una rapida circolazione delle informazioni sul *piano operativo*: il punto è verificare se queste informazioni sono utilizzabili anche in un contesto ad alto tasso di formalizzazione, qual è il procedimento penale.

A tal fine, può essere ragionevole partire proprio dal canone di disponibilità, il quale ha come ambito naturale la cooperazione di polizia – tanto che il Programma dell'Aia lo enuncia esplicitamente nella parte dedicata al rafforzamento della sicurezza (§ 2)[29] –, ma finisce per estendersi anche al procedimento penale. Lo stesso documento ribadisce l'auspicio per una migliore circolazione dei dati anche nella parte relativa al rafforzamento della giustizia con riguardo alle informazioni desumibili dai casellari giudiziali nazionali (§ 3.3.1). Ma la diffusività del principio è stata soprattutto riaffermata, non a caso, con riferimento alla cooperazione in materia di terrorismo, dal considerando n. 4 della decisione 2005/671/GAI, concernente lo scambio di informazioni relative alla lotta contro tale forma di criminalità: vi si afferma, infatti, che «il campo d'applicazione degli scambi di informazioni deve essere esteso a tutte le fasi dei procedimenti penali, comprese le condanne e a tutte le persone, gruppi o entità oggetto di un'indagine, di un'azione penale o di una condanna per reati di terrorismo»[30].

Ciò premesso, ci si deve evidentemente soffermare sui principali strumenti normativi che hanno dato attuazione al canone di disponibilità. Il primo è costituito dalla decisione quadro n. 960 del 2006[31].

Se sotto il profilo dell'ambito soggettivo, non vi è dubbio che la decisione si riferisca alle sole autorità di polizia (con esclusione dell'autorità giudiziaria), con riguardo all'ambito oggettivo di operatività, è altrettanto sicuro che essa si applica anche all'attività di polizia giudiziaria successiva all'acquisizione di una *notitia criminis*[32]. Ciò emerge chiaramente dal fatto che la decisione quadro attiene sia allo scambio di informazioni relative alle operazioni di *intelligence* criminale, sia a quelle relative all'indagine penale (art. 1, par. 1). La prima (ossia la *criminal intelligence operation*) viene definita come «una fase procedurale nella quale, in una fase precedente all'indagine penale, un'autorità competente incaricata dell'applicazione della legge, ai sensi della legislazione nazionale, ha facoltà di raccogliere,

---

29 Cfr. *Programma dell'Aia: rafforzamento della libertà, della sicurezza e della giustizia nell'Unione europea*, in *GUUE*, C 53, 3 marzo 2005, p. 7.

30 In *GUUE*, L 253, 29 settembre 2005, p. 22.

31 In *GUUE*, L 386, 29 dicembre 2006, p. 89.

32 Cfr. *supra*, S. Ciampi, "Principio di disponibilità e protezione dei dati personali nel 'terzo pilastro' dell'Unione europea", § 9.

elaborare e analizzare informazioni su reati o attività criminali al fine di stabilire se sono stati commessi o possono essere commessi in futuro atti criminali concreti» (art. 2, lett. *c*); l'indagine penale (ossia la *criminal investigation*) viene invece indicata come «una fase procedurale nella quale le autorità incaricate dell'applicazione della legge o le autorità giudiziarie competenti, compresi i pubblici ministeri, adottano misure per individuare e accertare i fatti, le persone sospette, e le circostanze in ordine a uno o più atti criminali accertati» (art. 2 lett. *b*).

Pertanto, se nel corso di un'indagine penale, in uno Stato membro è necessario ottenere un'informazione detenuta da un'autorità di polizia di un altro Stato in una propria banca dati oppure in una banca dati – pubblica (ad es. registro anagrafico) o privata (ad es. gestore di telefonia) – alla quale la polizia ha accesso diretto, la polizia che indaga può chiedere la trasmissione del dato e lo Stato estero dovrà trasmettere l'informazione – salvi casi tassativi di rifiuto – entro i termini brevi indicati dall'art. 4. Si badi, tale trasmissione avverrà al di fuori delle vie della cooperazione giudiziaria: potranno essere utilizzati i canali – assai agili – della cooperazione di polizia (art. 6).

La decisione fornisce un'ulteriore indicazione sul proprio ambito di applicazione: l'art. 1, par. 4, precisa, infatti, che essa non impone alcun obbligo per gli Stati membri di fornire informazioni e *intelligence* da utilizzare «come prove dinanzi ad un'autorità giudiziaria» («as evidence before a judicial authority»), né conferisce il diritto a utilizzarle a tal fine. Laddove lo Stato ricevente voglia impiegare le informazioni a tale scopo, deve ottenere il consenso dello Stato che le ha fornite, se è necessario, in virtù della legislazione nazionale di quest'ultimo e facendo ricorso agli strumenti di cooperazione giudiziaria vigenti tra gli Stati membri.

L'ambito di operatività dei meccanismi semplificati di trasmissione dei dati risulta pertanto delimitato – ai nostri fini – da un confine di ordine (per così dire) spaziale e da uno di natura funzionale: il primo deriva dal riferimento all'indagine penale, mentre il secondo si desume dall'esclusione della possibilità di utilizzare le informazioni come prove dinnanzi a un'autorità giudiziaria. Spetterà, dunque, al legislatore nazionale, in sede di attuazione della decisione quadro, adeguare tali limiti di ordine generale al contesto processuale italiano.

Con riguardo al concetto di "indagine penale", sembra che esso possa coincidere con quello di indagine preliminare: si tratta, infatti, dello spazio procedimentale che precede l'elevazione di un'accusa. Sarà quindi esclusa la possibilità di utilizzare i dati ottenuti in forza della decisione n. 960 nella fase strettamente processuale. Qualche problema in più potrebbe sorgere, invece, per l'altro limite. Nel nostro ordinamento, si potrebbe essere indotti a pensare che il secondo vincolo si limiti a specificare il primo. In quest'ottica, il divieto di utilizzo delle informazioni davanti all'autorità giudiziaria a fini probatori potrebbe essere concepito come divieto di impiegare i dati nel processo: nel corso delle indagini, invece, i dati trasmessi in attuazione del canone di disponibilità potrebbero essere sempre utilizzati. In tal senso, peraltro, potrebbe deporre l'orientamento giu-

risprudenziale che si è sviluppato in ordine all'istituto dello scambio spontaneo di informazioni previsto dall'art. 10 della Convenzione del Consiglio d'Europa sul riciclaggio (del 1990), dall'art. 46 della CAAS e ora anche dall'art. 7 della Convenzione dell'Unione europea sull'assistenza giudiziaria[33]: si è, infatti, stabilito che la documentazione acquisita per i canali di polizia è equivalente a quella acquisita mediante rogatoria[34] oppure che è estranea alla disciplina delle rogatorie[35] e se n'è ammesso l'utilizzo in indagini preliminari, in udienza preliminare e ai fini dell'adozione di misure cautelari, fermo in ogni caso il limite del rispetto dei diritti fondamentali garantiti dall'ordinamento giuridico nazionale[36].

Ebbene, una lettura che conduca a sovrapporre il limite funzionale a quello spaziale non può essere accolta. Non pare potersi escludere che un "utilizzo come prova dinanzi a un'autorità giudiziaria" si può avere anche nel corso delle indagini preliminari. Naturalmente, viene in mente l'impiego di un elemento di prova ai fini dell'adozione di una misura cautelare: in tal caso, invero, vi è un giudizio sulla probabile responsabilità. Al contrario, non sembra potersi parlare di "utilizzo come prova dinanzi a un'autorità giudiziaria" nel caso di provvedimento che autorizza un mezzo di ricerca della prova invasivo: in tale ipotesi, non vi è un accertamento – sia pure provvisorio – sulla responsabilità di un soggetto, ma tutt'al più (nel solo caso delle intercettazioni di comunicazioni) un vaglio relativo alla sussistenza di un fatto di reato. Insomma, la motivazione del provvedimento autorizzatorio è incentrata piuttosto sull'utilità dell'atto invasivo nell'individuazione di elementi conoscitivi che sulla ricostruzione del passato. In sede di attuazione della decisione occorrerà, allora, chiarire che i dati trasmessi in forma semplificata potranno essere utilizzati dalla polizia o dal pubblico ministero, sia per fini strettamente investigativi, sia per giustificare l'adozione di atti volti a

---

33 Al riguardo, cfr. E. Calvanese, *Cooperazione giudiziaria tra Stati e trasmissione spontanea di informazioni: condizioni e limiti di utilizzabilità*, in "Cassazione penale", 2003, pp. 458 sgg.; A. Ciampi, *L'assunzione di prove all'estero in materia penale*, Padova, Cedam, 2003, pp. 357 sgg.; G. De Amicis, *Cooperazione giudiziaria e corruzione internazionale. Verso un sistema integrato di forme e strumenti di collaborazione tra le autorità giudiziarie*, Milano, Giuffrè, 2007, pp. 329 sgg.; M.R. Marchetti, *L'assistenza giudiziaria internazionale*, Milano, Giuffrè, 2005, pp. 245 sgg.

34 Così, Cass., sez. I, 31 ottobre 2002, Moio, in "Archivio della nuova procedura penale", 2003, p. 132.

35 In tal senso, Cass., sez. III, 6 novembre 2002, Pils, in "Archivio della nuova procedura penale", 2003, p. 508, la quale si riferiva però a documentazione acquisita prima dell'accertamento della *notitia criminis*, ossia in una fase in cui non trovano ancora spazio le garanzie previste dagli artt. 727 ss.

36 Questo questo senso, Cass., sez. II, 8 marzo 2002, Pozzi, in "Cassazione penale", 2003, p. 449; Cass., sez. I, 1° dicembre 2000, Rondinella e altro, in "Centro elaborazione dati della Cassazione", n. 218214; Cass., Sez. I, 9 maggio 2000, Franzoni, *ivi*, n. 216737; Cass., sez. I, 10 luglio 1997, Ibba, in "Archivio della nuova procedura penale", 1997, p. 432; Cass., sez. I, 25 giugno 1991, Ferrante, in "Cassazione penale", 1991, II, p. 260. A tale riguardo, cfr. R. Vanni, *Spunti sul crimine transnazionale: utilizzabilità nel corso delle indagini preliminari di rogatorie passive, spazio investigativo e spazio cautelare, moderna cooperazione internazionale*, in "Il foro ambrosiano", 2003, pp. 88 sgg.

ricercare altri elementi conoscitivi necessari ad accertare il fatto criminoso: non potranno, invece, essere impiegati dal giudice per la decisione cautelare.

Il secondo strumento che ha dato attuazione al canone di disponibilità è senza dubbio la decisione 2008/615/GAI sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera[37]. Essa ha recepito il Trattato di Prüm nell'ordinamento comunitario e ha fissato, almeno per quanto concerne la circolazione delle informazioni personali relative ai profili DNA e ai dati dattiloscopici, un limite ancora più stringente. Infatti, è previsto – ai fini di indagine penale – un accesso diretto ai dati di indice; ma per la trasmissione dei dati personali che si riferiscono ai dati di indice rispetto ai quali è emersa una concordanza, gli artt. 5 e 10 della decisione stabiliscono un rinvio al diritto nazionale dello Stato richiesto. Il che significa che, di regola, essa dovrà seguire le procedure dell'assistenza giudiziaria: nondimeno, a rendere più agevole la trasmissione delle informazioni potrebbero intervenire proprio le norme della decisione n. 960 del 2006 e delle leggi nazionali che vi daranno attuazione[38], nonché quelle della decisione quadro sul mandato europeo di ricerca della prova. Diverso, invece, il discorso in ordine ai dati di immatricolazione dei veicoli, per i quali è previsto un accesso effettivamente diretto (art. 12 decisione n. 615 del 2008): pertanto, sembra potersi concludere che l'autorità dello Stato membro la quale effettua la consultazione e ottiene l'informazione relativa ai proprietari o agli utenti di un veicolo o al veicolo stesso potrà utilizzarlo nel procedimento penale senza che sia necessario un passaggio attraverso i meccanismi dell'assistenza giudiziaria.

L'ultimo filone da prendere in considerazione è quello relativo all'attuazione del canone di disponibilità nell'ambito delle informazioni relative a precedenti condanne dell'imputato[39]. Al riguardo, la decisione n. 876 del 2005 si limita a intervenire sullo strumento tradizionale di cooperazione previsto dagli artt. 13 e 22 della Convenzione di assistenza giudiziaria del 1959, prevedendo l'obbligo, per lo Stato richiesto, di trasmettere la risposta con il modulo standardizzato, immediatamente e comunque in un termine non superiore a dieci giorni (art. 3). Diverso, invece, l'impianto sotteso al sistema costituito dalla decisione quadro sull'organizzazione e il contenuto degli scambi sulle informazioni estratte dal casellario giudiziario (2009/315/GAI) e dalla decisione che istituisce il sistema europeo di informazione sui casellari giudiziari (2009/316/GAI). Sulla base di tale pacchetto normativo, le informazioni relative alla storia penale dell'imputato ottenute attraverso il sistema informatizzato potranno essere utilizzate nel corso del

37 In *GUUE*, L 210, 6 agosto 2008, p. 1. V. *supra*, A. Marandola, "*Information sharing* nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione".

38 Cfr. *supra*, S. Ciampi, *op. cit.*, § 10.

39 V. *supra*, M. Gialuz, "Il casellario giudiziario europeo: una frontiera dell'integrazione in materia penale".

procedimento penale (art. 9 della decisione n. 315), inteso in senso ampio come comprendente «la fase precedente al processo penale, la fase del processo penale stesso e l'esecuzione della condanna» (art. 1, lett. *b*, della decisione n. 315).

Per la verità, gli ostacoli all'impiego delle informazioni in parola nel procedimento penale italiano – ai fini dell'applicazione dei diversi istituti basati sulla "memoria"[40] – sembrano venire dalla disciplina interna. Dalla lettura congiunta dell'art. 730 c.p.p. e dell'art. 3 comma 1 lett. a del Testo unico in materia di casellario giudiziale (d.P.R. 14 novembre 2002, n. 313), si evince come le sentenze straniere acquisiscano rilevanza – anche soltanto come meri fatti storico giuridici – solo con il riconoscimento[41]. Si badi, però, che il legislatore italiano sarà chiamato a superare siffatta scelta: dovrà, infatti, dare attuazione alla decisione quadro sulla considerazione delle decisioni di condanna tra Stati membri dell'Unione europea in occasione di un nuovo procedimento penale (2008/675/GAI)[42], la quale prescrive proprio di equiparare la sentenza emessa in altro Stato dell'Unione a quella interna (art. 3, par. 1). Probabilmente, tale risultato può essere conseguito già a livello interpretativo – in applicazione del canone dell'interpretazione conforme alla decisione quadro[43] – valorizzando la norma dell'art. 696 c.p.p.

In conclusione, pertanto, si può affermare che il quadro che emerge dagli strumenti normativi che danno attuazione al canone di disponibilità è piuttosto composito. Vi è un primo livello che riguarda le informazioni più sensibili – quali quelle relative ai profili DNA o alle impronte digitali –, per le quali si prevede che debbano essere utilizzati i canali tradizionali dell'assistenza giudiziaria. Vi è poi un livello intermedio, relativo ai dati trattati da autorità di *law enforcement* (ossia di fonte poliziesca), con riguardo ai quali si consente una trasmissione diretta e deformalizzata ai soli fini investigativi. Infine, vi è un terzo livello, che concerne i dati giudiziari attinenti ai precedenti penali e ai dati meno sensibili (quali quelli relativi agli autoveicoli), nel quale si assiste effettivamente al superamento dell'ostacolo territoriale. Sicché, le informazioni contenute in una base dati nazionale possono essere trasmesse all'autorità di *law enforcement* o all'auto-

---

40 Cfr., per una puntuale ricognizione, D. Negri, "La circolazione del '*curriculum* criminale' tra i procedimenti penali", in *Contrasto al terrorismo interno e internazionale*, a cura di R. Kostoris e R. Orlandi, Torino, Giappichelli, 2006, p. 319.

41 Cfr. *supra*, M. Gialuz, "Il casellario giudiziario europeo", cit., § 4, nota 63.

42 In *GUUE*, L 220, 15 agosto 2008, p. 32.

43 Cfr., per tutti, A. Ciampi, "L'ordinamento italiano e le decisioni quadro quale strumento di cooperazione di polizia e giudiziaria", in *Equo processo: normativa italiana ed europea a confronto*, a cura di L. Filippi, Padova, Cedam, 2006, pp. 89 sgg.; *L'interpretazione conforme al diritto comunitario in materia penale*, a cura di F. Sgubbi e V. Manes, Bologna, Bononia University Press, 2007, pp. 53 sgg.; M. Marchegiani, *L'obbligo di interpretazione conforme alle decisioni quadro: considerazioni in margine alla sentenza Pupino*, in "Diritto dell'Unione Europea", 2006, p. 563; A. Weyembergh, "L'effectivité du troisième pilier de l'Union Européenne et l'exigence de l'interprétation conforme: la Cour de Justice pose ses jalons (note sur l'arrêt Pupino, du 16 juin 2005, de la Cour de Justice des Communautés européennes)", in *Per un rilancio del progetto europeo*, cit., pp. 353 sgg.

rità giudiziaria di altro Stato membro e utilizzate nell'ambito del procedimento penale (inteso in senso lato).

4. (Segue): il limite funzionale

Nell'ottica del legislatore europeo, si dovrebbero distinguere tre categorie di elementi conoscitivi, che assumono rilievo nell'attività di prevenzione e repressione dei reati: l'"*intelligence*", l'"*information*" e l'"*evidence*". Delle prime due si è detto: esse vengono definite dall'art. 2, lett. d, della decisione n. 960 del 2006 come «qualsiasi tipo di informazioni o dati detenuti da autorità incaricate dell'applicazione della legge» oppure «da autorità pubbliche o da enti privati che siano accessibili alle autorità incaricate dell'applicazione della legge senza il ricorso a mezzi coercitivi». La differenza tra esse risiede nella circostanza che l'*intelligence* non è connessa a una specifica indagine penale, mentre di *information* si parla con riferimento a elementi conoscitivi che si ricollegano a un'indagine volta alla ricostruzione di un fatto di reato[44]. La definizione di *evidence* si desume invece dalla decisione quadro sul mandato europeo di ricerca della prova: si tratta degli «oggetti, documenti e dati» da utilizzare nei procedimenti penali avviati da un'autorità giudiziaria (artt. 1, parr. 1 e 5).

Ebbene, mentre con riguardo alla categoria delle *pre-evidence*[45] – che ricomprende *intelligence* e *information*, che si collocano in uno stadio preliminare a quello relativo all'esercizio dell'azione penale – lo scambio è governato sempre e comunque dal principio di disponibilità, con riferimento all'*evidence* il quadro è più variegato: se in passato si doveva ricorrere agli strumenti di assistenza giudiziaria tradizionali[46], dopo l'adozione della decisione 2008/978/GAI e la sua attuazione, si potrà impiegare lo strumento riconducibile al canone del reciproco

---

44 Cfr. E. De Busser, *The architecture of data exchange*, in "International Review of Penal Law", 2007, p. 37, la quale precisa come l'*intelligence* sia qualificata talora «as 'soft' data – as opposed to 'hard' data – which stands for information, indicating the fact whether data can be endorsed by documents (f.e. sentences, witness statements, etc.) and is therefore reliable or not». Cfr. anche *supra*, § 3. Va notato che la nozione di *intelligence*, che emerge a livello europeo appare assai più ampia rispetto a quella fatta propria dalla dottrina italiana: al riguardo, cfr. *supra*, S. Ciampi, *op. cit.*, § 7.

45 La locuzione "pre-evidence phase" è utilizzata da G. Vermeulen - T. Vander Beken - L. Van Puyenbroeck - S. Van Malderen, *op. cit.*, p. 26.

46 In tal senso, G. Vermeulen - T. Vander Beken - L. Van Puyenbroeck - S. Van Malderen, *op. cit.*, p. 27, che escludono che l'attuazione del canone di disponibilità possa riguardare la cooperazione giudiziaria; nonché, E. De Busser, *op. cit.*, p. 38, la quale sottolinea la necessità che gli ambiti rimangano distinti utilizzando un'immagine efficace: «the notions of pre-evidence and evidence can be described as two storeys in the house of EU exchange of data. The ground floor represents all information and intelligence that will be able to be exchanged according to the principle of availability»; «the top floor represents all evidence to be exchanged in accordance with bi- and multilateral mutual legal assistance instruments».

riconoscimento, ossia il mandato europeo di ricerca della prova. Un problema potrebbe sorgere per il fatto che il MER ha un ambito di applicazione ristretto, in quanto non si applica ad esempio ai dati sulle comunicazioni conservati dai fornitori di servizi di comunicazioni elettroniche accessibili al pubblico o di una rete pubblica di comunicazione (art. 4, par. 2, lett. *e*).

Ad ogni modo, quale che sia il canale attraverso il quale l'elemento conoscitivo proveniente da archivi europei è trasmesso all'autorità (di polizia o giudiziaria) italiana, viene in rilievo un secondo possibile limite al suo utilizzo nel procedimento penale. Anche per i dati in relazione ai quali può essere superato l'ostacolo territoriale si pone, infatti, un problema di ordine funzionale: il procedimento penale dovrebbe essere impermeabile ai risultati dell'attività di *intelligence* o di indagine amministrativa. Tale sbarramento è tradizionalmente volto a garantire il rispetto del canone di separazione dei poteri dello Stato e a salvaguardare i diritti della persona sottoposta al procedimento penale.

Ebbene, non è un mistero che i confini tra attività di *intelligence* e di indagine penale si vanno facendo sempre più blandi e che si registra un tendenziale aumento dell'osmosi tra l'ambito della prevenzione e quello della repressione. Già negli anni novanta, la dottrina italiana lo aveva ben messo in luce, soprattutto con riferimento ai procedimenti relativi alla criminalità organizzata: si era parlato di inchieste preparatorie, prodromiche alle vere e proprie indagini penali[47]. Successivamente, il fenomeno dell'allentamento della separazione tra attività di *intelligence* e attività di polizia si è consolidato soprattutto con riguardo ai reati terroristici e nel contesto del *security paradigm*[48].

A favorire l'interconnessione tra i due momenti è stata anche la diffusione dell'*intelligence led policing*[49], ossia di quel paradigma investigativo che si fonda sull'impiego di tutte le informazioni disponibili, sulle tecniche di analisi criminale (come ad esempio il *profiling*), e, in definitiva, proprio sulla stretta cooperazione tra autorità di *law enforcement* e servizi di *intelligence*. Tale modello è stato recepito

---

47 Il riferimento è a R. Orlandi, *Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell'*inquisitio generalis*?*, in "Rivista italiana di diritto e procedura penale", 1996, pp. 283 sgg.

48 Cfr., in particolare, D. Derenčinović - A.M. Getoš, *Cooperation of law enforcement and intelligence agencies in prevention and suppression of terrorism – european perspective*, in "International Review of Penal Law", 2007, pp. 82 sg.; G. Marullo, "Il ruolo e le attività di intelligence e delle forze di polizia nella lotta alla criminalità organizzata ed al terrorismo nei paesi dell'Unione europea, nel rispetto della Convenzione del Consiglio d'Europa per la protezione dei dati personali e la Convenzione europea sui diritti dell'uomo", in *La cooperazione internazionale per la prevenzione e la repressione della criminalità organizzata e del terrorismo*, a cura di M. Cherif Bassiouni, Milano, Giuffrè, 2005, p. 187; J.A.E. Vervaele, "Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?", in *L'area di libertà sicurezza e giustizia*, cit., pp. 485-486.

49 Sul quale, cfr., per tutti, J. Ratcliffe, *Intelligence-Led Policing*, Cullompton, Willan Publishing, 2008, p. 6.

nel Programma dell'Aia – ove si parla di *intelligence-led law enforcement* o, nella versione italiana, di «metodologia di contrasto basata sull'intelligence» (§ 2.3) – e ad esso è in qualche misura riferibile la stessa configurazione dell'Europol.

Non sfuggirà che in tale modello, che si è sviluppato soprattutto con riguardo alla lotta al terrorismo e ai reati di criminalità organizzata[50], assumono un ruolo essenziale proprio le banche dati di polizia e, in certa misura, il collegamento tra le queste e quelle dei servizi segreti[51]: basti pensare al sistema di informazione e, soprattutto, agli archivi di analisi dell'Europol, che sono costituiti per la raccolta, il trattamento o l'utilizzazione di dati con «lo scopo di venire in aiuto all'indagine criminale» (art. 10, par. 2, Convenzione Europol). Ora, le informazioni contenute nel sistema informativo vanno comunicate dall'Europol alle unità nazionali interessate (art. 13 Convenzione Europol) e potranno essere utilizzate dai servizi competenti degli Stati membri «per prevenire e combattere la criminalità che rientra nella competenza dell'Europol e le altre forme gravi di criminalità» (art. 17 Convenzione Europol)[52]. Pertanto, tali informazioni potrebbero anche avere ingresso nel procedimento penale, magari indirettamente, ossia attraverso le relazioni di servizio, che possono avere un impiego probatorio nel corso delle indagini preliminari o nei riti premiali[53].

Parallelamente a quella tra attività di *intelligence* e attività di indagine penale, si è andata affievolendo la linea di separazione tra ispezione amministrativa e indagine penale: ciò riguarda i poteri di accertamento della Commissione[54], ma soprattutto le indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF). Com'è noto, il regolamento (CE) n. 1073/1999[55] riconosce all'OLAF il potere di svolgere indagini – espressamente qualificate "amministrative" dall'art. 2 – esterne o interne (artt. 3 e 4), ossia rispettivamente rivolte nei confronti di soggetti

---

50 Cfr., con riguardo all'esperienza inglese, Ö. Ülgen, *The UK's new serious organized crime agency (SOCA): combining intelligence and law enforcement*, in "International Review of Penal Law", 2007, p. 153.

51 V., in termini critici, P. De Hert - S. Gutwirth, *Interoperability of police databases within the EU: an accountable political choice?*, <http://papers.ssrn.com/sol3/papers.cfm?abstract__id=971855>, p. 9.

52 A tali disposizioni corrispondono gli artt. 17 e 19 della Decisione del Consiglio che istituisce l'Ufficio europeo di polizia: cfr. *Documento del Consiglio n. 8706/3/08*, 9 ottobre 2008, <http://register.consilium.europa.eu/pdf/it/08/st08/st08706-re03.it08.pdf>.

53 Cfr., con riguardo all'attività di *intelligence*, M.L. Di Bitonto, "Raccolta di informazioni e attività di *intelligence*", in *Contrasto al terrorismo interno e internazionale*, cit., p. 261. Sull'«ingresso privilegiato che avranno nei procedimenti penali le informazioni fornite da Europol», v. F.M. De Martino, "Europol: flusso transnazionale dei dati personali e loro utilizzazione nel processo penale italiano fra immunità degli agenti e cultura del sospetto», in *Nuove strategie per la lotta al crimine organizzato transnazionale*, a cura di V. Patalano, Torino, Giappichelli, 2003, p. 146.

54 In tal senso, J.A.E. Vervaele, *L'europeizzazione del diritto penale e la dimensione penale dell'integrazione europea*, trad. it. di R. D'Antoni, in "Rivista trimestrale di diritto penale dell'economia", 2005, pp. 137 sg.

55 In *GUCE*, L 136, 31 maggio 1999, p. 1.

non appartenenti alle istituzioni comunitarie o a soggetti che ne fanno parte. Entrambe si concludono con relazioni sui fatti accertati, che, ai sensi dell'art. 9, par. 2, del regolamento (CE) n. 1073/1999, «costituiscono elementi di prova nei procedimenti amministrativi o giudiziari dello Stato membro nel quale risulti necessario avvalersene al medesimo titolo e alle medesime condizioni delle relazioni amministrative redatte dagli ispettori amministrativi nazionali». È stato rilevato come tale norma – che ricalca quella dell'art. 8, par. 3, del regolamento EURATOM n. 2185/1996[56] – stabilisca «il generale principio di non separatezza, ed anzi di circolazione, degli elementi di prova dall'ambito amministrativo comunitario al circuito giudiziario nazionale»[57].

Per quel che riguarda specificamente l'ordinamento italiano, in dottrina si tende ad ammettere l'utilizzo delle relazioni nell'ambito delle indagini preliminari, ma la giurisprudenza è andata ben più in là, ritenendo che gli atti compiuti dall'Uclaf (ossia il diretto predecessore dell'OLAF) possano essere utilizzati anche in dibattimento: trattandosi di «atti promananti da un organo pubblico di controllo», essi possiederebbero «tutti i requisiti prescritti dall'art. 234 c.p.p. per l'inserimento nel fascicolo per il dibattimento»[58].

Come si intenderà, anche per i dati contenuti nei sistemi informativi potrebbe essere impiegata la categoria dei documenti: in effetti, una volta riprodotto il contenuto dichiarativo o rappresentativo su un supporto tradizionale, essi potrebbero essere ricondotti all'ampia nozione dell'art. 234 c.p.p.; oppure, anche a prescindere dalla riproduzione, potrebbero essere sussunti nella definizione di documento informatico, inteso come «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»[59].

---

56 In *GUCE*, L 292, 15 novembre 1996, p. 2.

57 Così, A. Perduca – F. Prato, *Le indagini dell'ufficio europeo per la lotta antifrode (Olaf) ed i rapporti con le autorità giudiziarie*, in "Cassazione penale", 2006, p. 4248. Sul rapporto tra indagine dell'OLAF e procedimento successivo, cfr. O. Broutin, "L'Office de lute antifraud", in *La preuve pénale*, cit., p. 41; S. de Moor, "Transnational investigations and the judicial follow-up to the OLAF inspection reports under the existing cooperation instruments", in *European Evidence Warrant*, cit., pp. 49 sgg.; D. Merckx, "The judicial follow-up of OLAF cases – A national perspective", *ibidem*, pp. 53 sgg.

58 In tal senso, Trib. Marsala, 17 dicembre 1998, XY, in "Cassazione penale", 1999, p. 2687. In termini favorevoli, V. Pacileo, *I rapporti dell'Olaf con le autorità giudiziarie nazionali: forme e modalità di assistenza*, <www.csm.it>, p. 8. In termini critici, invece, A. Perduca-F. Prato, *op. cit.*, p. 4250, secondo il quale in tale pronuncia si è andati oltre a quanto previsto dalla giurisprudenza di legittimità con riferimento ai verbali di constatazione della polizia giudiziaria e dei servizi ispettivi amministrativi nazionali; nonché, C. Bovio, *Le indagini interne ed esterne dell'Olaf: garanzie difensive ed effetti processuali*, <http://appinter.csm.it/internat/relaz/oL13698.pdf>, p. 4, che distingue tra atti effettivamente amministrativi dell'OLAF e atti compiuti durante la vera e propria indagine, i quali, avendo come presupposto gli indizi di illecito, dovrebbero essere svolti con il rispetto delle garanzie previste dal codice di rito penale.

59 Si tratta, come noto, della definizione posta dall'art. 1, lett. *p*), d.lgs. 7 marzo 2005, n. 82, che riprende quella dell'art. 1, lett. *a*, d.P.R. 10 novembre 1997, n. 513: a seguito della soppressione

La questione centrale, allora, è capire se, una volta superato l'ostacolo territoriale – mediante il ricorso alla rogatoria o al mandato europeo di ricerca della prova – essi possano per ciò solo essere acquisiti – laddove possibile – mediante l'inserimento nel fascicolo per il dibattimento ai sensi dell'art. 431 lett. *d* c.p.p. oppure direttamente acquisiti in dibattimento come tali.

Evidentemente, il problema deriva dal fatto che le banche dati considerate sono istituite proprio per finalità di sicurezza e di giustizia: sicché, esse forniranno documenti o informazioni che hanno un qualche legame, più o meno stretto, con l'accertamento penale. E, allora, il rischio è quello di utilizzare tale canale per far refluire in giudizio prove "documentali" che sono formate al di fuori del procedimento penale e da soggetti estranei al procedimento penale italiano, ma che sono *ab origine* destinate a tale contesto.

Occorre peraltro prendere atto che non si può fornire una risposta generalizzata, con riferimento a ciascuna banca dati: se vi sono banche dati tendenzialmente giudiziarie (come quella di Eurojust) oppure di *intelligence* (come quella di Europol) o di polizia (come la banca dati interforze, istituita presso il Ministero dell'Interno) vi sono archivi misti (come il SIS). Si dovrà, dunque, di volta in volta avere riguardo alla singola *res* individuata attraverso la banca dati e acquisita, per qualificarla a seconda dei casi come atto compiuto in un procedimento penale straniero, oppure come atto posto in essere nel corso di attività di *intelligence* criminale preventiva o di un'indagine di polizia amministrativa. Il primo potrà essere acquisito a norma dell'art. 238 c.p.p. e, se si tratti di atto non ripetibile della polizia giudiziaria, potrà essere inserito nel fascicolo per il dibattimento solo se le parti vi consentono oppure dopo l'esame testimoniale dell'autore, compiuto anche mediante rogatoria (art. 78 disp. att. c.p.p.)[60]. Laddove si tratti di dati provenienti da inchieste di *intelligence* o da attività di polizia amministrativa, potranno essere acquisiti come documenti solo se costituiscono veicolo di conoscenze non altrimenti acquisibili al processo per l'impossibilità di assumere oralmente in dibattimento l'atto probatorio[61].

Certo, vista la tendenza permissiva della giurisprudenza, non sarà facile garantire il rispetto del limite funzionale nella prassi: è accaduto, per esempio, che

---

– da parte dell'art. 3 l. 18 marzo 2008, n. 48 – della seconda parte dell'art. 491-*bis* c.p., occorre infatti riferirsi alla nozione generale del codice dell'amministrazione digitale (cfr. G. Amato, *Incerta l'efficacia probatoria del documento*, in "Guida al diritto", 2008, n. 16, p. 55; L. Picotti, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale*, in "Diritto penale e processo", 2008, p. 703; M. Scoletta, "Il nuovo regime penale delle falsità informatiche", in *Sistema penale e criminalità informatica*, a cura di L. Lupária, Milano, Giuffrè, 2009, pp. 8 sgg.).

60 Al riguardo, si legga C. Valentini, *L'acquisizione della prova tra limiti territoriali e cooperazione con autorità straniere*, Padova, Cedam, 1998, pp. 212 sg.

61 In tal senso, con riguardo al documento amministrativo atipico, R. Orlandi, *Atti e informazioni della autorità amministrativa nel processo penale*, Milano, Giuffrè, 1992, p. 146.

la qualifica come documenti di atti compiuti dall'ufficio SIRENE abbia consentito di aggirare, tanto il limite funzionale, quanto quello territoriale [62]; in palese violazione del canone di legalità della prova.

5. (Segue): il limite derivante dalla tutela del diritto alla protezione dei dati

Accanto al limite territoriale e a quello funzionale, si pone per i dati contenuti negli archivi informatici – sia quelli europei, che quelli nazionali – un ulteriore vincolo di utilizzazione, derivante dall'esigenza di tutelare quel diritto alla protezione del dato di carattere personale, che trova espresso e autonomo riconoscimento nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea[63].

L'analisi di questo terzo limite non può che prendere le mosse dalla constatazione di una differenza fondamentale nelle banche dati. Esse possono operare come depositi statici di informazioni preesistenti, nei quali la tecnologia informatica consente soltanto di identificare il dato utile, oppure, come contenitori "dinamici" di produzione di informazioni, nei quali la tecnologia informatica consente – si pensi ai sistemi informativi di Eurojust, agli archivi di analisi di Europol, oppure al sistema di indagine del CED interforze[64] – di *elaborare* i dati mettendoli in relazione e dando quindi loro un senso, che non avevano se presi singolarmente. Occorre, allora, distinguere: l'elemento cognitivo fornito al procedimento dalla banca dati può essere – come accade per altre prove: prima tra tutte, la testimonianza – originario oppure derivato. Sarà originario nel caso della banca dati tecnico-scientifica (l'impronta digitale; il profilo genetico; il dato

---

62 Ci si riferisce, in particolare, a una vicenda processuale per molti versi paradigmatica verificatasi davanti al Tribunale di Trieste. Era accaduto che la polizia di frontiera – del valico con la Slovenia – avesse accertato l'esistenza di una segnalazione nel SIS di un veicolo; richiesta la trasmissione di ulteriori informazioni tramite SIRENE tedesco, era risultato che il veicolo era stato oggetto di un'appropriazione indebita. Si è così aperto un procedimento penale per ricettazione e il pubblico ministero ha chiesto – e il tribunale ha concesso – l'acquisizione nel fascicolo per il dibattimento dei formulari SIRENE (A ed M) che contenevano i dati del veicolo e soprattutto il tipo di reato contestato, il luogo e la data dell'appropriazione indebita, l'autorità giudiziaria procedente e altri dati accessori. In tal modo, invece di acquisire con rogatoria gli atti del procedimento penale tedesco, si è qualificato come documento un qualcosa che difficilmente poteva avere tale caratteristica, perché o si trattava di attività di cooperazione di polizia giudiziaria oppure di attività di indagine preventiva.

63 Sull'importanza di tenere distinte la privacy, che costituisce un «tool of opacity» e il *right to data protection*, che configura un «tool of transparency», cfr. P. De Hert – S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in *Privacy and the Criminal Law*, a cura di E. Claes, A. Duff e S. Gutwirth, Anversa-Oxford, Intersentia, 2006, pp. 62 sgg., 103.

64 V. A. Intini – A.R. Casto – D.A. Scali, *op. cit.*, p. 95; A. Manganelli - F. Gabrielli, *Investigare. Manuale pratico delle tecniche di indagine*, Padova, Cedam, 2007, p. 20.

attinente alla comunicazione elettronica)[65]; sarà invece indiretto o derivato, tanto laddove esso derivi dalla rielaborazione dei dati singoli, quanto nel caso in cui coincida con una rappresentazione di un elemento cognitivo esterno inserito nell'archivio non nella sua integralità ma – come normalmente accade – attraverso riferimenti riassuntivi.

Rispetto alla prima tipologia di dati, la tutela del diritto alla protezione si realizza soprattutto attraverso il rispetto dei principi fondamentali del trattamento, primo tra tutti il *principio di finalità limitata*: l'elemento di prova dovrebbe poter essere utilizzato – in tutte le fasi processuali – soltanto ove raccolto anche per finalità di repressione dei reati.

Il problema si pone in relazione a quella tendenza, più volte registrata dal Garante europeo per la protezione dei dati, ad accordare alle autorità incaricate dell'applicazione della legge l'accesso a vari sistemi d'informazione e d'identificazione su vasta scala e l'utilizzazione ai fini di *law enforcement* di dati archiviati per finalità diverse (immigrazione e visti, dati relativi ai passeggeri dei voli aerei e dati relativi alle telecomunicazioni)[66]. Gli esempi più significativi sono quelli dell'Eurodac e del VIS: ossia, di banche dati di "primo pilastro", sviluppate in vista dell'attuazione della politica europea rispettivamente in materia di diritto d'asilo e di visti. Evidentemente, le impronte digitali contenute nell'Eurodac potrebbero essere assai utili per finalità di *law enforcement*: vi è da escludere, però, che possano essere impiegate a fini di identificazione in un procedimento penale. Per quel che riguarda il VIS, invece, recentemente è stata adottata la decisione 2008/633/GAI, che consente un accesso e un impiego limitato dei dati del sistema informazione visti da parte delle autorità di applicazione della legge, e pertanto anche nel procedimento penale[67].

In relazione alle altre banche dati, ossia a quelle che forniscono elementi conoscitivi "mediati", il problema si pone in termini diversi. Il diritto alla protezione del dato personale si declina quale *diritto al controllo della fonte dell'informazione*: in tal senso, pare assumere una certa importanza la disposizione dell'art. 10, comma 2, l. 121 del 1981 (ordinamento di pubblica sicurezza), secondo la quale «i dati e le

---

65 Non sfugge che, anche rispetto a questi dati, vi è una mediazione, come vi è una mediazione dell'apparato percettivo nella testimonianza. Nel caso specifico, la sua portata è contenuta dall'automaticità dell'acquisizione mercé un dispositivo tecnologico o dalla valenza scientifica del procedimento attinente alla raccolta e al confronto del dato.

66 Cfr. *Inventario 2007*, in <http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Priorities/06-12-12__priorities__IT.pdf>, p. 2. Con riguardo al 2008, l'Autorità ha riconosciuto che «continuerà la tendenza ad aprire le basi di dati esistenti (sia europee che nazionali) ai fini dell'applicazione della legge, nonostante lo scopo iniziale della base di dati fosse diverso» e ha rinnovato l'impegno per un controllo sull'utilizzo per finalità di *law enforcement* di dati raccolti per altri scopi (<http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Priorities/07-12-20__Priorities__2008__IT.pdf>, p. 3-4).

67 Per questi profili, cfr. *supra*, M. Gialuz, "Principio di accessibilità e banche dati di 'primo pilastro'", § 5.

informazioni conservati negli archivi del Centro possono essere utilizzati in procedimenti giudiziari o amministrativi soltanto attraverso l'acquisizione delle fonti originarie» – ossia documenti conservati presso PA, sentenze o provvedimenti dell'autorità giudiziaria, atti di procedimenti penali, atti di indagine della polizia –, «fermo restando quanto stabilito dall'art. 240 c.p.p.». In effetti, la *ratio* sottesa a questa norma sembra in qualche misura analoga a quella che sancisce il divieto di utilizzo dell'anonimo o della testimonianza indiretta: il soggetto al quale si riferisce (in senso lato) l'informazione deve poter verificare l'attendibilità della fonte dell'informazione stessa. Generalmente, tale interesse – riconosciuto dal codice in diverse disposizioni, quali quelle degli artt. 195, comma 7, 203, 240 c.p.p. – viene ricondotto a un valore processuale, quale il canone del contraddittorio o il diritto di difesa[68]. In realtà, pare poter essere ricollegato in ultima istanza proprio al diritto alla protezione del dato, che ricomprende (tra le altre) anche la facoltà del titolare di conoscere direttamente la fonte delle informazioni sul proprio conto[69].

In quest'ottica, una norma riferibile specificamente a un archivio, quale quella del Centro di Elaborazione Dati, sembra poter essere generalizzata ed applicata anche alle banche dati europee, come espressione di un principio generale che esclude l'utilizzazione di elementi di prova di fonte ignota. Una conferma in tal senso sembra peraltro poter venire dall'art. 5, par. 5, della Raccomandazione (87) 15 del comitato dei ministri del Consiglio d'Europa (diretta a disciplinare l'utilizzo dei dati a carattere personale nel settore di polizia), secondo il quale «prima che i dati personali siano comunicati deve essere verificata la loro qualità. Nei limiti del possibile, in tutte le trasmissioni di dati, devono essere indicate le decisioni giudiziarie e le decisioni di proscioglimento e i dati basati su opinioni o considerazioni personali devono essere verificati alla fonte prima di essere trasmessi e occorre indicare il loro livello di accuratezza e affidabilità».

Né in senso contrario pare possa deporre la mancata reiterazione di una norma analoga nella recente decisione quadro 2008/977/GAI, che pone una disciplina generale in materia di protezione dei dati personali nell'ambito della cooperazione giudiziaria e di polizia in materia penale[70]. È ben vero che l'art. 9 della proposta originaria della Commissione (COM (2005) 475 def., del 4 ottobre 2005)[71] riprendeva quasi testualmente la disposizione dell'art. 5, par. 5, della Rac-

---

68 Cfr., per la testimonianza indiretta, da ultimo, C. Cesari, "Testimonianza indiretta (diritto processuale penale)", in *Enciclopedia del diritto. Annali*, II.1, Milano, Giuffrè, pp. 1136 sgg.; con riguardo all'anonimo, cfr. per tutti P. Corso, *Notizie anonime e processo penale*, Padova, Cedam, 1977, p. 162.

69 Vale la pena riprendere il punto di vista di A.A. Dalia, *op. cit.*, p. 63, il quale ritiene la previsione della necessità di acquisire la fonte come finalizzata proprio a eliminare l'«intermediazione della banca».

70 In *GUUE*, L 350, 30 dicembre 2008, p. 60.

71 *Documento del Consiglio n. 2005/0202 (CNS)*, 4 ottobre 2005, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0475:FIN:IT:PDF>.

comandazione; in realtà, non sembra che la riformulazione del dettato normativo possa assumere significato decisivo: a ben considerare, l'art. 8 della decisione 2008/977/GAI sembra riaffermare proprio il valore della piena controllabilità della fonte, laddove prescrive allo Stato membro che trasmette i dati di corredarli «delle informazioni disponibili che consentono allo Stato membro ricevente di valutare il livello di esattezza, completezza, aggiornamento e affidabilità». Certo, il legislatore europeo avrebbe potuto (e dovuto) essere più chiaro su un punto decisivo come questo. Vi è da auspicare che il legislatore nazionale sia più coraggioso e che, in sede di attuazione della decisione quadro nell'ordinamento italiano, precisi la portata di tale previsione generica e subordini espressamente l'impiego nel procedimento penale dei dati trasmessi all'acquisizione delle fonti documentali originarie.

Di più: sarebbe una buona occasione per specificare il riferimento – di per sé ambiguo – al "procedimento giudiziario", contenuto nell'art. 10, comma 2, l. 121 del 1981. Tale locuzione è stata interpretata restrittivamente, nel senso che la norma opererebbe solo con riguardo al dibattimento[72]. In realtà, pare che essa debba trovare applicazione anche al di fuori del dibattimento, quanto meno in materia cautelare: in tale ambito, infatti, operano, per espressa scelta del legislatore, tanto l'art. 195 c.p.p., quanto l'art. 203 c.p.p.

Un ultimo limite fondamentale, che interessa qualsiasi banca dati, è quello relativo al divieto di decisioni fondate unicamente su un trattamento automatizzato di dati. Ora, tale regola assume nel nostro ordinamento carattere assoluto: l'art. 14 del d.lgs. 30 giugno 2003, n. 196 (codice privacy) – che trova applicazione anche al trattamento effettuato per ragioni di giustizia e a quello da parte di forze di polizia, non essendo tra le norme escluse ai sensi degli artt. 47 e 53 – stabilisce infatti che «nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato». Una disposizione, questa, che riprende l'art. 17 l. 31 dicembre 1996, n. 675, il quale aveva dato attuazione all'art. 15 della direttiva 95/46/CE[73]. Si badi, però, che una norma analoga era stata posta proprio dall'art. 9, comma 4, l. 121 del 1981, sia pure in termini più restrittivi, in quanto si faceva riferimento alle "decisioni giudiziarie"[74].

Ancora una volta, la decisione quadro sulla protezione dei dati personali nel "terzo pilastro" sembra meno restrittiva, in quanto non esclude in assoluto la

---

72 Il riferimento è a S. Fratucello, "La protezione dei dati personali come limite all'accertamento penale nel 'codice della privacy'", in *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, a cura di D. Negri, Roma, Aracne, 2007, p. 137.

73 Cfr. G. Buttarelli, *op. cit.*, pp. 341 sgg.; P. Ceccoli, "*sub* art. 14", in *Codice della privacy*, tomo I, Milano, Giuffrè, 2004, p. 191. In termini generali, sul *profiling*, cfr. *supra*, M. Gialuz, "La cooperazione informativa", cit., nota 31.

74 Tale disposizione è stata poi abrogata proprio dalla l. 31 dicembre 1996, n. 675 (art. 43).

possibilità di ricorrere a decisioni fondate esclusivamente su trattamenti automatizzati: si limita a richiedere che essa sia adottata solo se «autorizzata da una legge che precisi i provvedimenti atti a salvaguardare gli interessi legittimi della persona interessata» (art. 7 della decisione quadro 2008/977/GAI).

6. Conclusioni

All'esito delle riflessioni svolte, si può fornire una risposta all'interrogativo dal quale si sono prese le mosse. Senza dubbio le banche dati europee possono funzionare come fonti di prova che, avendo carattere essenzialmente transnazionale, consentono di superare almeno in parte le dinamiche tradizionali dell'assistenza giudiziaria e di fornire direttamente elementi conoscitivi agli attori del procedimento penale.

Come si è visto, la portata di tale affermazione varia a seconda della tipologia di banca dati e della natura dell'informazione che si prende in considerazione.

Per quel che riguarda quelle che possono qualificarsi come "banche dati europee in senso stretto", ossia i sistemi informativi europei centralizzati (SIS, SID, TECS di Europol, EPOC-II di Eurojust, Eurodac, VIS) e le banche dati interconnesse (quali saranno i casellari giudiziari europei e le banche dati relative alle immatricolazioni dei veicoli), che garantiscono una disponibilità *immediata* dell'informazione, si può asserire che permettono di aggirare parzialmente gli strumenti tradizionali di assistenza. Esse forniscono ai soggetti del procedimento penale degli elementi conoscitivi: a quali soggetti e in quali fasi dipende dalla natura del dato.

Ove venga in rilievo un'informazione di origine giudiziaria oppure documentale (ossia riferibile a una *res* prodotta al di fuori del procedimento), quale quella relativa alle precedenti condanne o al numero di immatricolazione di un veicolo, il sistema informativo consente di fornire l'elemento conoscitivo da utilizzare direttamente nella fase preliminare: con riguardo all'ambito cautelare e a quello dibattimentale, il rispetto del diritto alla protezione del dato – che si declina in termini processuali come diritto al contraddittorio e alla difesa – postula l'acquisizione del documento originale dal quale il dato è estratto.

Laddove si tratti invece di un dato che è il frutto di una precedente indagine amministrativa, si aggiungerà il limite funzionale: il "documento" corrispondente potrà essere acquisito – attraverso il mandato europeo di ricerca della prova o mediante rogatoria – solo a condizione che non sia possibile acquisire la prova costituenda.

Non troppo dissimile il discorso relativo alle banche dati europee in senso lato, ossia alle banche dati nazionali per le quali è previsto un collegamento mediato, per effetto dell'accesso indiretto (si allude alle banche dati dattiloscopiche e a quelle genetiche) o dell'obbligo di trasmettere le informazioni in attuazione del canone di disponibilità. In apparenza, oltre ai limiti indicati in precedenza, sembrerebbe esservi un vincolo territoriale: anche l'uso in indagini, per i dati

più sensibili (ossia impronte digitali e profili DNA), sembrerebbe richiedere il ricorso ai canali più garantiti dell'assistenza giudiziaria. In realtà, l'attuazione della decisione quadro n. 960 del 2006 dovrebbe consentire di trasmettere in forma semplificata anche questi dati: ovviamente, solo a fini investigativi e con l'esclusione di un utilizzo "a fini di prova davanti all'autorità giudiziaria", ossia per l'adozione di misure cautelari.

In definitiva, dunque, le banche dati europee possono produrre *direttamente* elementi di prova da utilizzare nella fase del procedimento penale che presenta il minor tasso di formalizzazione, ossia la fase delle indagini preliminari. Almeno con riguardo a questa, si può asserire che esse contribuiscono – insieme ad altri strumenti – al successo di quelle forme alternative di cooperazione in materia penale, che stanno erodendo il campo di applicazione del tradizionale strumento rogatoriale[75]. Si dà peraltro un'eccezione, che deriva dalla tipologia del provvedimento da adottare sulla base delle informazioni derivanti dagli archivi informatici: laddove si tratti di un vero e proprio giudizio – sia pure interinale – sulla responsabilità – qual è quello sotteso all'adozione di una misura cautelare – non si possono impiegare informazioni trasmesse dalle autorità di *law enforcement*, ma è necessario ottenere il documento originario mediante gli strumenti dell'assistenza giudiziaria o l'emissione di un mandato europeo di ricerca della prova.

Per quel che concerne la fase strettamente processuale, occorre distinguere: con riferimento al dibattimento, non v'è dubbio che non si possa utilizzare direttamente l'elemento cognitivo trasmesso dalla banca dati. La banca dati consentirà di individuarlo, ma poi dovrà essere acquisito mediante canali più garantiti. In relazione invece all'udienza preliminare e ai riti alternativi, si deve ulteriormente precisare: va esclusa la possibilità di utilizzare il dato dell'archivio nazionale trasmesso ai sensi della decisione n. 960 del 2006, in quanto essa stessa si riferisce alla sola fase di indagine; si potranno invece utilizzare i dati resi disponibili da quelle che si sono definite banche dati europee in senso stretto.

Ad ogni modo, le banche dati svolgeranno un ruolo fondamentale nell'individuazione delle prove da acquisire successivamente mediante gli strumenti tradizionali di assistenza oppure attraverso le forme previste dalla Convenzione europea di assistenza giudiziaria – purtroppo non ancora ratificata dal nostro Paese –, o, ancora, oggi, attraverso il mandato europeo di ricerca della prova.

---

75 Cfr., per tutti, E. Selvaggi, "Le nuove forme della cooperazione: un ponte verso il futuro", in *Rogatorie penali e cooperazione giudiziaria internazionale*, a cura di G. La Greca e M.R. Marchetti, Torino, Giappichelli, 2003, pp. 465 sgg. Con riguardo, invece, alle nuove prospettive di cooperazione contemplate dalla Convenzione Cybercrime con riferimento specifico ai dati informatici, si leggano, E. Selvaggi, *Cooperazione giudiziaria veloce ed efficace*, in "Guida al diritto", 2008, n. 16, p. 72; Id., *Task force operativa 24 ore al giorno*, *ivi*, 2008, n. 16, pp. 75 sgg.