UNIVERSITÀ DEGLI STUDI DELL'INSUBRIA

FACOLTÀ DI GIURISPRUDENZA

DOTTORATO DI RICERCA IN
STORIA E DOTTRINA DELLE ISTITUZIONI

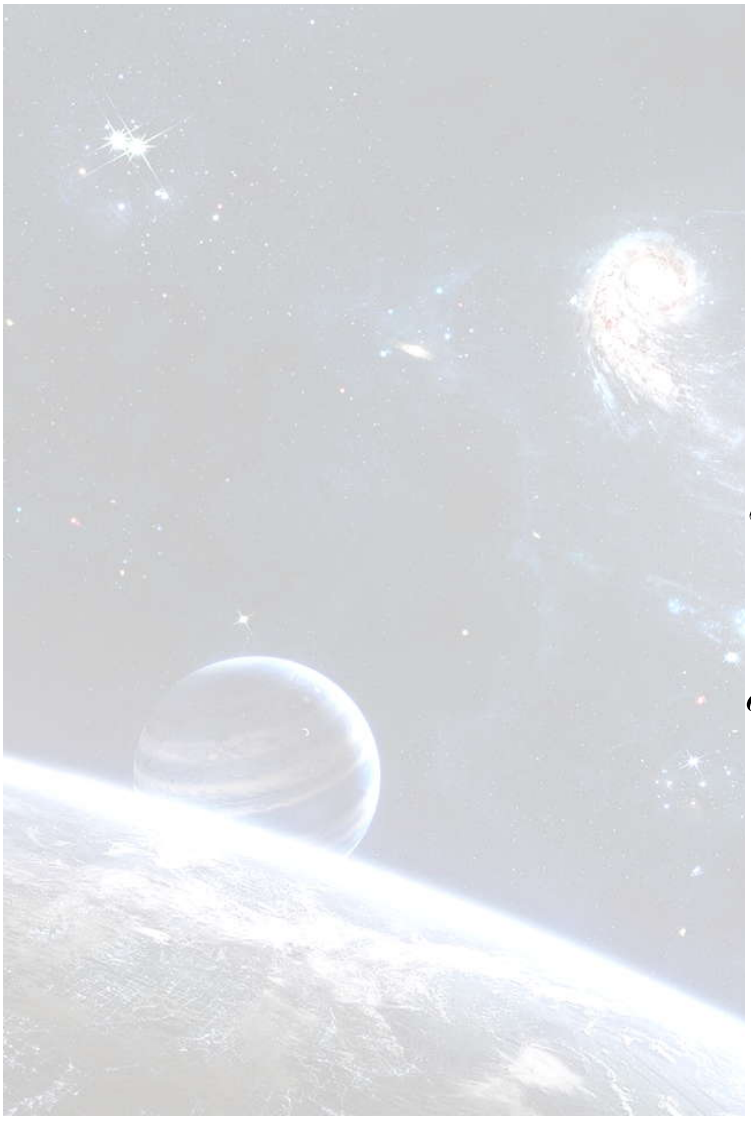
La cooperazione di polizia e giudiziaria e la circolazione della prova digitale nello spazio giudiziario europeo: un bilanciamento critico tra libertà, sicurezza e giustizia

Relatore

Chiar.ma Prof.ssa *Francesca Ruggieri*

Tesi di

Dr.ssa *Eleonora Colombo*



... Si andrà sulla Luna e poi sui pianeti e sulle stelle come oggi si va da Liverpool a New York, facilmente, rapidamente, sicuramente, e l'oceano atmosferico sarà tra breve attraversato come gli oceani terrestri. La distanza non è che una parola relativa, e finirà per essere ridotta a zero.

(J. Verne Dalla Terra alla Luna)

INTRODUZIONE

Il metodo della ricerca. La prospettiva europea e la comparazione tra gli ordinamenti italiano, tedesco e francese

CAPITOLO I

L'attuazione dello spazio di libertà, sicurezza e giustizia nell'Unione Europea: una ricostruzione dello status quo

1 Premessa: la necessità di un'analisi in prospettiva differenziata a seconda dei diritti, dei reati e dei soggetti coinvolti

2 La garanzia dei diritti fondamentali nelle procedure di cooperazione

- 2.1 La tutela dei diritti nell'ordinamento comunitario, dalla CEDU alla Carta di Nizza, tra norma scritta e interpretazione giurisprudenziale.
- 2.2 Le garanzie dei diritti fondamentali negli ordinamenti degli Stati membri in un approccio esemplificativo di diritto comparato nella normativa di attuazione della DQ MAE

3 Linguaggio e traduzione giuridica per la concreta attuazione dei diritti fondamentali

4 Crimini transnazionali, *cybercrimes* e crimini internazionali: definizioni e dati statistici

- 4.1 L'approccio globale per la prevenzione e repressione dei crimini transnazionali e internazionali

5 La cooperazione giudiziaria e di polizia nello spazio giu diziario europeo

- 5.1 Strumenti convenzionali: dalla Convenzione europea sull'assistenza giudiziaria del 1959 alla Convenzione di Bruxelles del 29 maggio 2000
- 5.2 Le procedure di cooperazione nel sistema delle fonti comunitarie, con particolare attenzione al MERP ed al MAE

6 Gli organi comunitari coinvolti nelle procedure di cooperazione: Europol, Eurojust e Olaf

- 6.1 Il quadro di attuazione della decisione istitutiva di Eurojust: ritardi, vuoti normativi e spinte riformatrici
- 6.2 Gli scambi di informazioni e dati tra Europol e le unità nazionali
- 6.3 Il coordinamento tra Olaf e le autorità investigative nazionali

CAPITOLO II

La prova digitale

SEZIONE I

Il contenuto della prova digitale nell'ambito della cooperazione nello spazio giudiziario europeo

SEZIONE II

La catalogazione dei dati e degli archivi

SEZIONE III

La prova digitale, i diritti della persona e le esigenze di giustizia e di sicurezza interna ed esterna

CAPITOLO III

La circolazione della prova digitale nell'ambito della cooperazione nello spazio giudiziario europeo

CAPITOLO IV

La cooperazione giudiziaria e di polizia in prospettiva de iure condendo: riforma del sistema e della circolazione della prova digitale ai fini di giustizia

INTRODUZIONE

Il metodo della ricerca. La prospettiva europea e la comparazione tra gli ordinamenti italiano, tedesco e francese

La Società moderna si compiace del progresso delle scienze, quale segno tangibile di prosperità e benessere.

Come osserva Mark Mazower, anche la modernità ha il suo lato oscuro[1] che non deve essere sottovalutato, affinché lo sviluppo possa figurare come una ricchezza e non un'insidia.

Le nuove tecnologie, infatti, sono portatrici di un potenziale violento, che agisce nascostamente nella mente umana.

Lo stesso concetto di "*violenza*", dunque, non si può limitare agli atti di coercizione e costrizione fisica o psichica, compiute da un soggetto per costringere un altro soggetto a fare, sopportare o omettere qualcosa[2], come vorrebbe la definizione tradizionale.

La sociologia e la psicologia moderna si interrogano costantemente sul rapporto tra l'uomo e la macchina e sul pericolo che l'essere umano divenga schiavo del mezzo tecnologico, perdendo di vista i valori etici dell'agire quotidiano.

Spesso, infatti, gli strumenti informatici (in particolare) si fondono e confondono con gli aspetti criminali, fino a diventare il mezzo o lo strumento agevolatore della commissione di fatti di reato.

E' pura fantascienza di un robot che assume sembianze umane, che sogna, che prova dei sentimenti e che ha un cuore, come mostrato nel noto film di Steven Spielberg, basato su un progetto incompleto di Stanley Kubrick, *A.I. Intelligenza Artificiale*.

Nell'enorme effluvio di *input* e di possibilità offerte dallo sviluppo scientifico, ciascun individuo e le istituzioni devono essere messi nelle condizioni di conoscere e comprendere i pericoli connessi, per evitarli o per porvi rimedio.

La percezione del rischio è qualcosa che va ben oltre il concetto tradizionale di percezione come pura esperienza sensitiva come sviluppo psichico ad un segnale di allarme o di preoccupazione. Essa poggia su un

---

[1] M. A. MAZOWER *Il lato oscuro della modernità. La violenza e lo Stato nel XX secolo* in *Lettera internazionale,* II trimestre, 2008, pag. 25.

[2] Cfr voce "*violenza*" ne *lo Zingarelli,* Zanichelli, 1995.

costrutto cognitivo, fondato sull'osservazione attenta della realtà, sulla comunicazione con gli altri, su processi di conoscenza del reale di tipo esperienzial-narrativo[3].

La cognizione del rischio si caratterizza per la rappresentazione sociale che ne è data, non soltanto mediante l'esperienza diretta del cittadino, dunque, ma anche (e soprattutto) attraverso la tematizzazione operata dai *media*[4].

La capillarità dei mezzi di comunicazione di massa, permette all'opinione pubblica di conoscere numerosi casi di cronaca giudiziaria criminale in cui il mezzo informatico-telematico è l'oggetto su cui ricadono le conseguenze del reato o il mezzo per la commissione di reati o, più semplicemente, l'elemento di agevolazione per il raggiungimento del fine illecito dell'azione.

Ormai da anni sono al centro delle notizie di cronaca giudiziaria casi di truffe o frodi informatiche, di clonazione di carte di credito o bancomat, all'illecita intrusione in archivi informatici di grosse società multinazionali quali la Sony.

A titolo esemplificativo si cita il caso ECHELON, acronimo utilizzato dalle agenzie di spionaggio degli Stati Uniti d'America per individuare i sistemi di sorveglianza e di intercettazione. Nel febbraio del 1998 il "sistema di monitoraggio globale" ha conquistato le prime pagine dei principali giornali, per primo il settimanale *Il Mondo*, il quale ha dedicato un lungo dossier per descrivere nei dettagli i meccanismi di ascolto e registrazione delle informazioni dei sistemi di telecomunicazioni internazionale. Allarmante è la capillarità dei dati captati: comunicazioni militari, messaggi diplomatici criptati, conversazioni commerciali confidenziali, oltre alle "normali" comunicazioni quotidiane: tutti i dati che transitano via telefono, fax, telex, internet. Il caso, però, è rimasto allo stadio di una mera *spy story,* poiché, al di là dell'archivio Stoa (*Scientific and Tecgnological Options Assessment*), non è stata trovata alcuna prova dell'esistenza di questo sistema di spionaggio.

Un altro caso di interesse è rappresentato dalla vicenda *Wikileaks.* Il termine, con il quale si identifica l'omonimo sito internet deriva dalla parola *Wiki*, un neologismo che indica un tipo di piattaforma software che consente la gestione collaborativa di contenuti pubblicati sul Web e dalla parola *Leaks* che significa perdite, falle, fughe di notizie. Julian Assange, responsabile del sito internet, mantenendo la promessa fatta agli internauti, ha messo a disposizione migliaia di cablogrammi con i quali ambasciatori, consoli e diplomatici americani hanno trasmesso a Washington i propri giudizi, valutazioni e

[3] Così S. BACCASTRINI – S. CERRAI *Comprendere la percezione del rischio, praticare la comunicazione sul rischio* in *Rivista italiana di comunicazione pubblica,* 20, 2004, pagg. 120-126.

[4] Così M. MORCELLINI *L'informazione e la percezione della sicurezza* in *Rivista italiana di comunicazione pubblica,* 34, 2007, pagg. 68-80.

resoconti informativi relativi a personaggi e vicende dei Paesi presso i quali erano accreditati. Molti documenti riservati sono stati pubblicati da *Wikileaks* a partire dal 28 novembre 2010, alla ricerca di indiscrezioni e pettegolezzi su uomini politici, capi di stato e di governo, personalità più o meno in vista.

Ancora, il caso della rete internazionale di attivisti informatici internazionale *Anonymous*, i quali hanno iniziato ad operare i propri attacchi dal 2006 a danno del *social network Habbo*. La guerra *on line* di questi *dark hacker* é da sempre consistita in attacchi DDos (*Distibuted denial of service attack*), con lanci di milioni di pacchetti dati contro i siti bersaglio, simulando la simultanea connessione di milioni di utenti ad un *server*, provocando un sovraccarico in grado di bloccare l'operatività del sito, rendendolo irraggiungibile dagli internauti e oscurandolo di fatto.

Ha colpito anche la recente vicenda di cronaca, del luglio 2011, occorsa in Galles dove un ragazzo sedicenne, Jashua Davies, ha ucciso a sassate l'ex fidanzata quindicenne. Il giovane da tempo premeditava l'assassinio, condividendo il progetto con gli amici su internet, in *facebook*.

Non meno scalpore ha sollevato il caso del *serial killer* Matej Curko, meglio noto come il cannibale di Kysak. Il mostro slovacco, una volta scelta e agganciata la vittima in chat, inviava messaggi diretti per posta elettronica. Per mezzo del suo avatar digitale "*Kanibm*", adescava le donne, organizzava gli incontri e dava sfogo alla sua indole folle, mutilando i corpi e cibandosi della loro carne. Le parti umane mancanti sono risultate corrispondenti alle fotografie che il cannibale teneva in un archivio. Tramite le tracce trovate nel pc di Curko, il 17 maggio 2011 è stato possibile ritrovare due ragazze sepolte nella foresta di Kysak, presunte scomparse.

Quelle riportate sono solo alcune tra le tante notizie e fatti di cronaca che riguardano le tecnologie informatico-telematiche, sia come mezzo per commettere reati o per agevolarne la commissione, sia come fonte di prove utili per la prosecuzione delle indagini penali o per la definizione di un processo.

La ricerca nasce dalla consapevolezza di questo panorama sociale contemporaneo, dalla cui analisi si sono sviluppati spunti di approfondimento e di riflessione sul crimine transnazionale, in generale, sul coinvolgimento delle infrastrutture tecnologiche e sull'approccio ai problemi da parte della giustizia penale comunitaria e nazionale.

Il presente lavoro ha preso le mosse dalla raccolta di fonti bibliografiche, normative e giurisprudenziali, sia mediante la ricerca nelle biblioteche e nei centri di ricerca italiani e stranieri, sia navigando nel *web* tra i siti delle maggiori istituzioni comunitarie ed altri siti utili.

Dagli spunti raccolti per lo sviluppo del tema, è emersa un'assenza di opere scientifiche composite che trattino del problema dell'acquisizione della

prova digitale e della sua circolazione tra gli ordinamenti giuridici degli Stati membri[5].

La materia della cooperazione di polizia e giudiziaria (da intendere anche come cooperazione informativa), della criminalità informatica e della prova digitale, in connessione con la protezione dei dati archiviati e la loro circolazione, è attuale ed in continuo divenire.

Considerati singolarmente, ciascuno dei menzionati temi interessa in maniera particolare l'Unione europea, la quale è intervenuta molte volte, specie negli ultimi anni, sia attraverso sentenze della Corte di Giustizia CE e della Corte Europea dei Diritti dell'Uomo, sia attraverso interventi normativi vincolanti o non vincolanti per gli Stati membri.

Questo complesso quadro multilivello ha richiesto un aggiornamento continuo e costante nel corso dei tre anni di studio e ricerca.

L'approccio critico è stato arricchito dalla partecipazione a seminari e convegni in Italia e all'estero, in ragione dell'attualità ed insieme della novità della tematica affrontata.

La ricerca non poteva prescindere dalla ricostruzione dello *status quo* in ambito comunitario nella materia della cooperazione e della garanzia dei diritti fondamentali, nel quadro della criminalità transnazionale e della criminalità informatica in particolare.

Da qui l'attenzione particolare alla prova digitale nell'ambito UE: definizione, fonti normative comunitarie e bilanciamento con il diritto alla *privacy*, mediante un approccio comparato tra le leggi nazionali di Italia, Francia e Germania a protezione della riservatezza dei dati e delle informazioni.

Dallo studio del ruolo fondamentale occupato dalla *digital evidence* in molti procedimenti penali nazionali o che coinvolgono più Stati, si è osservato che spesso questi stessi dati possono costituire oggetto di reato, sia nella fase statica in cui sono archiviati in banche dati, sia (e soprattutto) nella fase dinamica di circolazione.

Questo rilievo ha richiesto una preliminare ricostruzione delle modalità di catalogazione delle informazioni, dello *standard* di sicurezza delle infrastrutture e dello scambio di dati tra autorità competenti degli Stati membri, della formazione professionale dei soggetti adibiti a mansioni di archiviazione e dell'esecuzione delle procedure di trasferimento delle informazioni, anche con attenzione ai sistemi vigenti negli ordinamenti nazionali di Italia, Francia, Germania e in ambito comunitario.

[5] Come si noterà, vi è un unico testo dell'inglese Mason sulla prova elettronica, il quale però, come è solito per gli studiosi di *common law*, ha un approccio molto pratico e casistico e poco teorico e di sistema.

La problematicità intrinseca alla categoria delle prove digitali si sviluppa dalla genesi, alla raccolta, alla catalogazione, al trasferimento, avuto riguardo alla necessaria tutela dei diritti fondamentali, bilanciati con gli interessi contrapposti alla giustizia e alla sicurezza dell'Unione europea .

La realizzazione dello spazio europeo di libertà, sicurezza e giustizia, come emerso dalla ricerca effettuata, costituisce inconfutabilmente uno degli obiettivi principali dell'Europa, specie dall'entrata in vigore del Trattato di Lisbona.

Il Trattato di riforma, che ha modificato sia il Trattato sull'Unione europea, sia il Trattato che istituisce la Comunità europea, ha delineato un assetto ordinamentale nuovo, riproponendo in parte alcune soluzioni già prospettate nel testo della Costituzione per l'Europa del 2004.

Nel settore della giustizia penale sono accresciute le competenze (concorrenti) dell'Unione e si è, contemporaneamente, evoluto il sistema di protezione dei diritti, mediante l'applicazione della Carta di Nizza e della Convenzione Europea dei Diritti dell'Uomo.

È evidente come, almeno sotto un profilo metodologico, si imponga un approccio il più possibile globale ed unitario allo studio teorico e pratico degli istituti propri dello spazio giudiziario europeo, per sviluppare una piena comunitarizzazione (o europeizzazione) del diritto penale e della procedura penale[6].

In prospettiva futura, appare opportuno superare i vuoti normativi dell'ambito comunitario in materia di cooperazione di polizia e giudiziaria, specialmente avuto riguardo all'evoluzione della criminalità transnazionale, del crimine informatico e delle prove digitali. Queste, in particolare, necessitano dei giusti mezzi e di previsioni specifiche che ne agevolino la circolazione.

La materia è in continua e lenta evoluzione, verso la formazione di una giustizia penale dove libertà, sicurezza e giustizia coesistono in un sistema di bilanciamento critico, basato su regole generali che si adattano al caso concreto.

La fluidità del tema in trattazione è attestata anche da una normativa UE frammentaria, recepita in modo disomogeneo e con considerevoli ritardi dagli ordinamenti giuridici nazionali. A ciò si aggiunge una copiosa produzione giurisprudenziale comunitaria che funge da punto di riferimento per una corretta interpretazione ed applicazione del diritto.

In ragione della delicatezza della materia di cui trattasi e dell'esigenza contingente di far fronte ai problemi connessi alla criminalità globale, è necessario che le istituzioni UE predispongano delle risposte comuni, chiare e concrete.

---

[6] Così F. ROMOLI *Il nuovo volto dell'Europa dopo il Trattato di Lisbona* in *Archivio penale,* 1, 2011, pagg. 155-160.

Il futuro della giustizia penale europea dipende, in prospettiva *de jure condendo,* dall'evoluzione del sistema di cooperazione, dal rafforzamento dei poteri delle istituzioni europee e dallo sviluppo degli strumenti d'indagine, per raggiungere un sistema processuale comunitario in grado di rispondere alle istanze di tutela dei diritti fondamentali e di lotta efficace al crimine.

CAPITOLO PRIMO

L'attuazione dello spazio di libertà, sicurezza e giustizia nell'Unione Europea: una ricostruzione dello *status quo*

SOMMARIO: 1.Premessa: la necessità di un'analisi in prospettiva differenziata a seconda dei diritti, dei reati e dei soggetti coinvolti - 2. La garanzia dei diritti fondamentali nelle procedure di cooperazione - 2.1 L tutela dei diritti nell'ordinamento comunitario, dalla CEDU alla Carta di Nizza, tra norma scritta e interpretazione giurisprudenziale - 2.2 Le garanzie dei diritti fondamentali negli ordinamenti degli Stati membri in un approccio esemplificativo di diritto comparato nella normativa di attuazione della DQ MAE - 3. Linguaggio e traduzione giuridica per la concreta attuazione dei diritti fondamentali - 4. Crimini transnazionali, *cybercrimes* e crimini internazionali: definizioni e dati statistici - 5. La cooperazione giudiziaria e di polizia nello spazio giudiziario europeo - 5.1 Strumenti convenzionali: dalla Convenzione europea sull'assistenza giudiziaria del 1959 alla Convenzione di Bruxelles del 29 maggio 2000 - 5.2 Le procedure di cooperazione nel sistema delle fonti comunitarie, con particolare attenzione al MERP ed al MAE - 6. Gli organi comunitari coinvolti nelle procedure di cooperazione: Europol, Eurojust e Olaf

1. *Premessa: la necessità di un'analisi in prospettiva differenziata a seconda dei diritti, dei reati e dei soggetti coinvolti*

Il Trattato di Lisbona delinea la centralità del progetto di attuazione dello spazio europeo di libertà, sicurezza e giustizia. La realizzazione di questo obiettivo è il segno tangibile di un'Europa che cresce e che si sviluppa, per garantire principalmente che i cittadini dell'Unione possano circolare liberamente, in condizione di protezione giuridica[7].

[7] L'art. 2 così recita: "*L'unione si prefigge di promuovere la pace, i suoi valori e il benessere dei suoi popoli.*
L'Unione offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, in cui sia assicurata la libera circolazione delle persone insieme a misure appropriate per quanto concerne i

Questo spazio comune ha un impatto immediato e diretto in diverse materie di interesse generale come l'immigrazione, la lotta al terrorismo e alla criminalità organizzata.

Lo stesso Trattato individua quattro settori d'intervento fondamentali per l'attuazione dello spazio di libertà, sicurezza e giustizia: le politiche dell'immigrazione, dell'asilo e dei controlli alla frontiera; la cooperazione giudiziaria in materia civile; la cooperazione giudiziaria in materia penale; la cooperazione di polizia.

Con l'eliminazione della distinzione in pilastri dell'UE, il Trattato ha voluto valorizzare la competenza degli organi comunitari nella materia della cooperazione penale, permettendo il loro intervento ad ampio spettro in tutti i campi applicativi.

La cooperazione di polizia e giudiziaria in materia penale, quale elemento del più composito spazio comune europeo, si presenta come un caposaldo imprescindibile dell'Unione. Questa, a sua volta, si caratterizza per una pluralità di aspetti di contenuto, che richiedono un'analisi in prospettiva differenziata, per dare chiarezza e organicità alla ricostruzione dello stato dell'arte in materia e per individuare possibili linee di sviluppo.

Tale ricostruzione interessa un'ampia normativa sovranazionale, spesso di diretta applicazione, a volte norma interposta tra le regole costituzionali e la disciplina nazionale, a volte un semplice monito o invito agli Stati membri. I contenuti si moltiplicano se si considera l'elaborazione giurisprudenziale della Corte di Strasburgo e della Corte di Lussemburgo per la tutela dei diritti e delle libertà fondamentali dell'individuo, quali parametri interpretativi delle norme interne.

In ambito UE si registra un processo evolutivo che, tra vuoti e battute d'arresto, testimonia l'entusiastico sforzo verso il progresso e la realizzazione dello spazio europeo di libertà, sicurezza e giustizia. Questo richiede, *in primis*, un progressivo superamento degli angusti limiti alla cooperazione, all'armonizzazione ed al mutuo riconoscimento.

I vettori su cui si poggia la costruzione dello spazio comune europeo, sono caratterizzati dalla creazione di una giustizia penale europea, dalla fiducia tra gli Stati e le istituzioni, dal rispetto dei diritti fondamentali riconosciuti a livello comunitario, secondo un bilanciamento degli interessi contrapposti in ogni singolo caso concreto, mediante il coinvolgimento e l'intervento dei soggetti competenti.

I diversi organi comunitari assumono un ruolo più o meno determinante, secondo il caso concreto, sia sotto il profilo della prevenzione e repressione del

---

controlli alle frontiere esterne, l'asilo, l'immigrazione, la prevenzione della criminalità e la lotta contro quest'ultima (...)".

crimine transnazionale, sia per la tutela di uno *standard* minimo di garanzie dei diritti e delle libertà di ciascun individuo coinvolto.

Da qui la tensione continua tra l'esigenza di garanzia di uno spazio comune europeo sicuro e protetto da attacchi (interni ed esterni) e il soddisfacimento delle prerogative individuali riconosciute dalle Carte nazionali, UE e internazionali.

Le comuni esigenze sviluppate a partire dagli Anni '90, dalla nascita dell'Europa senza frontiere, hanno portato ad una crescente richiesta di europeizzazione che coinvolge i meccanismi di cooperazione di polizia e giudiziaria.

L'evidente incremento della normativa sovranazionale e il rafforzamento dei poteri degli organi UE, permettono di individuare le prime coordinate di "sistema" entro cui muovere i passi verso uno spazio comune europeo.

La cornice della garanzia dei diritti fondamentali riconosciuti dalla Convenzione Europea dei Diritti dell'Uomo e dalla Carta di Nizza è individuata sulla scorta delle interpretazioni giurisprudenziali della Corte Europea dei Diritti dell'Uomo e dalla Corte di Giustizia delle Comunità Europee.

L'impatto dell'entrata in vigore del Trattato di Lisbona del 2009, ha lasciato delle lacune, specie in materia di cooperazione, laddove sono solo parzialmente attuati il principio del mutuo riconoscimento e la fiducia reciproca tra gli Stati.

L'Unione europea sta attraversando una fase di costruzione di un'identità forte che si muove in una fitta rete di normative, spesso di difficile comprensione ed applicazione negli ordinamenti interni, di Carte dei diritti, di organi e istituzioni.

L'integrazione tra gli Stati membri necessita di un approccio politico e giuridico, sul piano della difesa, destinata a svincolarsi dalle logiche nazionali, per abbracciare le relazioni internazionali[8].

Il punto di svolta è da ricerca nell'adesione ad un nucleo di valori, principi e diritti comuni e nella realizzazione di una dimensione organizzativa più stabile, con proiezione comunitaria.

Ognuno di questi aspetti di relazione produce effetti nella creazione dello spazio di libertà, sicurezza e giustizia.

Sciolti i legami con l'idea tradizionale di sovranità, riconducibile ai ristretti ambiti nazionali, il germe del processo di integrazione comunitaria sta crescendo sulla base di un terreno solido, composto da norme, procedure di cooperazione, tutela dei diritti e competenze degli organi comunitari.

[8] Così A. L. VALVO *L'Unione europea dal Trattato costituzionale al Trattato di Lisbona*, Aracne editrice, 2008, pagg. 5-30.

La corretta conoscenza e la comprensione dei sistemi fondanti delle politiche comunitarie costituiscono un punto di riferimento nell'approccio ad una realtà differenziata, caratterizzata da un pluralismo sociale, politico e giuridico e da una manifestazione criminale rappresentativa che richiede mezzi e strumenti specifici e scelti.

L'impulso comunitario verso la prevenzione e la repressione della criminalità transfrontaliera ha superato l'ostaggio della sovranità nazionale per dare una connotazione sovranazionale che possa essere più rapida ed incisiva verso il cuore del problema della difesa e della sicurezza, con una risposta europea, in un clima di reciproca fiducia tra gli Stati membri.

2. *La garanzia dei diritti fondamentali nelle procedure di cooperazione*

Già con il Trattato di Amsterdam del 1997, nell'espressa previsione della creazione di uno spazio comune di libertà, sicurezza e giustizia[9], per permettere alle persone di potersi liberamente muovere all'interno del territorio dell'Unione europea e di godere, in questo contesto spaziale, del rispetto dei diritti e delle libertà fondamentali, oltre a beneficiare di condizioni di sicurezza e legalità, facendo affidamento su regimi giuridici uniformi o armonizzati.

Questi stessi scopi sono stati meglio individuati dal Consiglio di Tampere del 1999 e reiterati all'esito del Consiglio dell'Aja dell'8 marzo 2005, con l'approvazione del documento 2005/C/53/1.

Un ulteriore passo in avanti nel processo di integrazione degli ordinamenti giuridici e dei sistemi giudiziari è rappresentato dall'approvazione a Nizza, il 7 dicembre 2000, della Carta dei diritti fondamentali dell'Unione europea[10].

Ancora prima, il sistema di garanzia giudiziaria predisposto dalla Convenzione Europea dei Diritti dell'Uomo del 1950 del Consiglio d'Europa, ha rappresentato un esempio importante di *governance* di tutela dei diritti umani a livello macroregionale.

Questo testo rileva non solo per il catalogo dei diritti in essa contenuti, ma anche per la procedura di tutela tra i più avanzati a livello internazionale.

L'Europa dei diritti individuali nel terzo millennio ha ricevuto un significativo impulso dall'entrata in vigore del Trattato di Lisbona mediante il riconoscimento di una efficacia giuridicamente vincolante alla Carta di Nizza e

[9] Titolo IV, artt. 29 e seguenti, TUE.

[10] Per un approfondimento sul testo della Carta di Nizza si rinvia a L. FERRARI BRAVO – F.M. DI MAJO – A. RIZZO (a cura di), *Carta dei diritti fondamentali dell'Unione europea commentata,* Giuffré 2001.

l'adesione dell'Unione Europea alla CEDU. Questa tappa rappresenta un punto focale verso l'integrazione europea, almeno per quanto riguarda la garanzia dei diritti fondamentali[11].

Il processo d'integrazione dei diritti ha portato ad un'influenza reciproca della giurisprudenza delle Corti di Lussemburgo e di Strasburgo poiché, mentre in precedenza la Corte di Giustizia delle Comunità Europee tendeva a sostenere la propria posizione autonoma e differenziata rispetto alla Corte Europea dei Diritti dell'Uomo anche per l'interpretazione delle disposizioni della Convenzione del 1950, ad oggi le sentenze in materia dei diritti dell'uomo sono sostanzialmente analoghe, salvo che per alcuni specifici casi[12].

L'assoggettamento ad un sistema multilivello di protezione dei diritti e di controllo giudiziario accresce la garanzia dei diritti dell'uomo anche nei confronti degli *standard* offerti dagli Stati membri[13].

Le conseguenze di questa struttura sono rilevanti in materia di cooperazione giudiziaria e di polizia che scontava, precedentemente, un *deficit* di trasparenza e di tutela dei diritti, imputato alla struttura il pilastri dell'Unione Europea ed all'appartenenza di questa materia al Terzo Pilastro[14].

L'avviamento di una cooperazione strutturata permanente comunitarizza la materia, assoggettandola alla disciplina ed al sistema di garanzia della Carta di Nizza e della CEDU. Questa realizzazione è il riflesso della tensione, nel Trattato di Lisbona, tra Unione-mezzo e Unione-fine, segnata oggi dalla prevaricazione della strategia funzionalista, la quale si concentra sui vantaggi concreti perseguibili mediante l'applicazione delle procedure di cooperazione[15].

Il rapporto tra l'UE e gli Stati continua a fondarsi sul principio di leale collaborazione che impone rispetto ed assistenza reciproca, assicurando ogni misura atta ad assicurare l'esecuzione degli obblighi derivanti dai trattati o dagli atti di istituzione dell'Unione e nel rispetto dei diritti umani[16].

---

[11] Così M. CARTABIA *I diritti fondamentali in Europa dopo Lisbona: verso nuovi equilibri?* in *Giornale di Diritto Amministrativo,* 3, 2010, pagg. 221-225.

[12] Si veda la sentenza della Corte Europea del 20 febbraio 1996, Vermeulen c. Belgio, in tema di diritto ad un equo processo, nella quale la Corte ha ritenuto sussistente una violazione dell'art. 6 CEDU la mancata previsione normativa, nell'ordinamento giuridico belga, di un diritto di replica del ricorrente alle conclusioni rassegnate dall'Avvocato generale della Corte di Cassazione; la Corte di Giustizia, al contrario, non ha ritenuto applicabile questa giurisprudenza dinanzi al giudice comunitario escludendo che l'impossibilità di presentare delle osservazioni all'Avvocato generale determini una violazione del diritto al *fair trial* (ordinanza 4 febbraio 2000, causa C-17/98, Emesa Sugar NV).

[13] Come è noto, l'elenco dei diritti della Carta di Nizza e della CEDU rispecchiano quasi totalmente la tradizione giuridica dei Paesi occidentali, fungendo da controlimiti alla sovranità statale.

[14] Così M. SAVINO *La Pesc e lo spazio di libertà, sicurezza e giustizia* in *Giornale di Diritto Amministrativo,* 3, 2010, pagg. 226-231.

[15] *Ibidem,* pag. 230.

[16] Si veda l'art. 4, paragrafo 3, TUE e L. SALTARI *Il riparto di competenza tra l'Unione europea e gli Stati: ossificazione o fluidità?* in *Giornale di Diritto Amministrativo,* 3, 2010, pagg. 231-236.

La Convenzione Europea dei Diritti Fondamentali è arricchita dall'interpretazione della Corte europeo, generandosi così un'integrazione tra *law in the books* e *law in action.* Tuttavia non risulta così agevole individuare in una decisione il principio generale ad essa sotteso, considerato che la Corte è investita di un caso specifico. Ciò a dire che i Giudici si trovano a ragionare case by case, tenendo conto dei fatti e delle circostanze presenti in quell'ipotesi particolare e, di conseguenza, nulla impedisce loro di enunciare un principio che poi, possibilmente, deve essere disatteso in un caso successivo diversamente circostanziato[17].

L'adeguamento a nuovi *standard*, la risposta efficace alle innovazioni e lo sviluppo delle garanzie, richiedono una continua dinamicità anche a livello giurisprudenziale.

2.1 *La tutela dei diritti nell'ordinamento comunitario, dalla CEDU alla Carta di Nizza, tra norma scritta e interpretazione giurisprudenziale*

La tendenza a prevedere forme sempre più avanzate di cooperazione nello spazio UE, valorizza le relazioni tra organi sovranazionali e di questi con gli organi comunitari, nonché l'armonizzazione dei sistemi normativi penali.

L'attenzione ai bisogni della collettività che spesso pone in ombre le garanzie processuali e la tutela dei diritti fondamentali dell'individuo [18].

Eppure le istituzione europee, oltre a prevedere una serie di nuovi strumenti per far fronte alle mutate esigenze di cooperazione tra gli Stati, hanno adottato dei provvedimenti volti ad uniformare la garanzia dei diritti umani negli ordinamenti nazionali e di innalzare lo *standard* di protezione degli interessi dei singoli.

I progressi nelle procedure di cooperazione richiedono un bilanciamento delle esigenze di costituzione di rapporti tra organi di polizia e autorità giudiziarie e la tutela dei diritti fondamentali che, ad oggi, mancano di un approccio organico.

A causa dell'assenza di una visione sistematica, gli organi comunitari affrontano costantemente il tema delle garanzie procedurali, della protezione dei diritti dell'uomo e delle libertà fondamentali, prevedendo delle soluzioni finali di compromesso.

---

[17] Così R. GAMBINI *Armonizzazione dei diritti nazionali nel segno della giurisprudenza europea* in *Diritto Penale e Processo,* 9, 2009, pagg. 1169-1174, la quale Autrice, a sua volta, richiama il testo di A. BALSAMO – R. KOSTORIS (a cura di) *Giurisprudenza europea e processo penale,* Utet, 2008.

[18] Così E. APRILE – F. SPIEZIA *Cooperazione giudiziaria penale nell'Unione europea prima e dopo il Trattato di Lisbona,* Ipsoa, 2009, pag. 117.

Con il recepimento della Convenzione Europea dei Diritti dell'Uomo (CEDU), approvata nel diverso contesto convenzionale del Consiglio d'Europa, e della Carta dei diritti fondamentali di Nizza del 2000, l'Unione europea ha conferito un ruolo centrale ai diritti fondamentali. Il Trattato istitutivo della Costituzione europea (mai entrato in vigore) ed ancora il Trattato di Lisbona ribadiscono e sottolineano che l'Unione si fonda sul rispetto dei diritti previsti dalle menzionate Carte e dalle tradizioni costituzionali comuni, in quanto principi generali del diritto comunitario [19].

Si è venuto a creare un complesso sistema che intreccia norme convenzionali di diritto comunitario e norme appartenenti agli ordinamenti nazionali, le cui relazioni sono potenziate dalla ricca produzione giurisprudenziale della Corte di Giustizia dell'Unione europea, sempre più interessata dal sindacato di conformità delle norme interne alla luce dei diritti fondamentali, e della Corte europea dei diritti dell'uomo che influenza le scelte dei legislatori, europeo e nazionali.

Risalendo alle origini, nel 1949 è stato istituito a Londra il Consiglio d'Europa, organismo internazionale politico deputato a promuovere la realizzazione di una stretta rete di relazioni tra gli Stati per salvaguardare gli ideali e i principi che costituiscono patrimonio comune. Il 4 novembre 1950 a Roma, proprio in quest'ambito di riferimento, è stata sottoscritta la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali a cui, il 20 marzo 1952, è stato aggiunto un Protocollo addizionale, sottoscritto a Parigi [20].

A Nizza, il 7 dicembre 2000, il Parlamento europeo, il Consiglio e la Commissione hanno solennemente proclamato la Carta dei diritti fondamentali dell'Unione europea, frutto di una procedura originale, senza precedenti nella storia dell'Unione, così riassumibile: il 3 e 4 giugno 1999 il Consiglio europeo di Colonia ha conferito mandato ad una Convenzione di redigere il progetto; la Convenzione è costituita nel dicembre 1999 e ne viene approvato il progetto il 2 ottobre 2000; il Consiglio europeo di Biarritz (13/14 ottobre 2000) ha convenuto all'unanimità sul progetto e lo ha trasmesso al Parlamento europeo e alla Commissione; il Parlamento europeo lo ha approvato il 14 novembre 2000 e la Commissione il 6 dicembre 2000; il 7 dicembre 2000 a Nizza i Presidenti del Parlamento europeo, del Consiglio e della Commissione a nome delle rispettive istituzioni hanno sottoscritto e proclamato la Carta.

[19] La Corte di Giustizia, con la sentenza Rutili del 28 ottobre 1975, n. 36, è giunta ad affermare che il diritto comunitario è informato alle tradizioni costituzionali comuni degli Stati membri in materia di diritti fondamentali.

[20] Cfr E. APRILE *Diritto processuale penale europeo e internazionale,* Cedam, 2007, pagg. 141-143.

La Carta dei diritti fondamentali dell'Unione europea riassume in un unico testo, per la prima volta nella storia dell'Unione europea, i diritti civili, politici, economici e sociali dei cittadini europei nonché di tutte le persone che vivono sul territorio dell'Unione. Questi diritti sono raggruppati in sei grandi capitoli: dignità, libertà, uguaglianza, solidarietà, cittadinanza, giustizia. Si fondano soprattutto sui diritti e sulle libertà fondamentali riconosciute dalla Convenzione europea per la salvaguardia dei diritti dell'uomo, sulle tradizioni costituzionali degli Stati membri dell'Unione europea, sulla Carta sociale europea del Consiglio d'Europa e sulla Carta comunitaria dei diritti sociali fondamentali dei lavoratori, nonché su altre convenzioni internazionali alle quali aderiscono l'Unione europea o i suoi Stati membri [21].

Come già accennato, tra le novità introdotte dal Trattato di Lisbona vi è il riconoscimento, con valenza di diritto dell'Unione, dei diritti fondamentali e dei principi generali comuni degli Stati membri. In particolare l'art. 6, paragrafo 1 e 3, TUE prevede che "*l'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adottata il 12 dicembre 2007 a Strasburgo, che lo stesso valore giuridico dei Trattati*" e "*i diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni degli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali*".

Per quanto d'interesse ai fini di questa ricerca, il riferimento è in particolare all'art. 5 CEDU sul diritto alla libertà e alla sicurezza, all'art. 6 CEDU sul diritto ad un processo equo e di ragionevole durata, svolto davanti ad un tribunale indipendente ed imparziale, all'art. 8 CEDU sul diritto al rispetto della vita privata e familiare.

Questi diritti sono sostanzialmente analoghi a quelli già previsti dalla Dichiarazione Universale dei Diritti Umani adottata dall'Assemblea Generale delle Nazioni Unite il 10 dicembre 1948 e così, analogamente, nella Carta di Nizza, avuto riguardo in particolare all'art. 6 sul diritto alla libertà e alla sicurezza, all'art. 7 sul rispetto della vita privata e della vita familiare, all'art. 8 sulla protezione dei dati di carattere personale, all'art. 48 sulla presunzione d'innocenza e il diritto alla difesa.

I possibili (presunti) problemi di coordinamento tra la Carta e la CEDU sono sciolti già dall'art. 52 della Carta stessa che si riferisce alla portata dei diritti garantiti. La disposizione mira, nel suo complesso, ad introdurre una clausola generale interpretativa delle garanzie approntate nei capi che precedono, onerandosi di evitare discrasie contenutistiche su un piano

[21] Cfr http://www.europarl.europa.eu/charter/default_it.htm (consultato in data 10 ottobre 2010). Allo stesso indirizzo internet è possibile consultare anche le Dichiarazioni dei Presidenti del Consiglio europeo, della Commissione e del Parlamento sulla Carta dei Diritti.

orizzontale: "*Laddove la Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta Convenzione*"[22].

Le menzionate disposizioni della Carta di Nizza e della CEDU trovano la corretta interpretazione nella giurisprudenza della Corte di Giustizia e della Corte Europea dei Diritti dell'Uomo[23] che ne precisano i contenuti e, contestualmente, ne rafforzano il ruolo e le previsioni di garanzia.

La comunitarizzazione del III Pilastro dell'Unione ha lo scopo di rafforzare il ruolo e la competenza, anche in materia di cooperazione, della Corte di Giustizia, sia per l'integrazione dell'*acquis* di Schengen nell'UE, sia per l'incremento della tutela giurisdizionale dei diritti umani in ambito comunitario.

In base all'art. 19 TUE la Corte assicura il rispetto del diritto nell'interpretazione e nell'applicazione dei trattati (e dunque delle norme a questi equiparabili).

Continuano ad essere escluse la validità e la proporzionalità di operazioni condotte dalla polizia o da altri servizi incaricati dell'applicazione della legge di uno Stato membro o l'esercizio delle responsabilità incombenti agli Stati membri per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna (art. 276 TFUE)[24].

Parallelamente opera la Corte Europea dei Diritti dell'Uomo la quale, pur operando nello spazio geografico europeo, non ha alcun rapporto con l'UE *strictu sensu* intesa.

L'efficacia della sentenza della Corte si realizza nell'individuazione di una violazione della convenzione o dei suoi protocolli, impegnando le Parti a conformarsi alla decisione definitiva e facendo nascere in capo allo Stato l'obbligo di rimuovere le cause della violazione[25].

---

[22] Per un approfondimento sui rapporti tra la Carte dei Diritti Fondamentali dell'Unione europea e la Convenzione Europea dei Diritti dell'Uomo si rinvia a V. MANES – V. ZAGREBELSKY (a cura di) *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano,* Giuffré, 2011.

[23] L'importanza delle sentenze della Corte Europea dei Diritti dell'Uomo è attestata anche dalla mole di lavoro registrata dalle statistiche. Si pensi solo che nel 2009 ha ricevuto circa 57 mila nuovi ricorsi e l'anno si è chiuso con 119.300 ricorsi pendenti. La Corte, va ricordato, si rivolge ad una platea potenziale di circa ottocento milioni di individui. Questi dati si trovano in V. MANES – V. ZAGREBELSKY *op. cit.,* pag. 196.

[24] Per un approfondimento sul ruolo, l'organizzazione e il funzionamento della Corte di Giustizia dell'Unione europea si rinvia a R. ADAM – A. TIZZANO *Lineamenti di diritto dell'Unione europea,* Giappichelli, 2010; M. CASTELLANETA *L'obbligo di conformarsi a decisioni precedenti rende difficile il contrasto all'abuso del diritto* in *Guida al Diritto,* 37, 2009, pagg. 71-73; A FABBRICATORE *Caso Pupino: sul riconoscimento dell'efficacia diretta delle decisioni quadro* in *Diritto Penale e Processo,* 2006, pag. 640-646.

[25] Per un approfondimento sull'organizzazione e il funzionamento della Corte Europea dei Diritti dell'Uomo si rinvia a G. LATTANZI *Costretti dalla Corte di Strasburgo* in *Cassazione Penale,* 2005,

Il potenziale pericolo di sovrapposizione e conflitti tra le giurisdizioni delle due Corti è stato definitivamente scongiurato dall'entrata in vigore del Trattato di Lisbona, mediante il recepimento nel diritto dell'Unione europea sia della Carta di Nizza, sia dei principi della CEDU.

Il diritto ad un equo processo che si riflette, nel suo contenuto multiforme, anche nelle procedure di cooperazione, ha destato l'attenzione delle Corti nazionali e comunitarie, al fine di delinearne i confini di tutela. Questo diritto si sostanzia, innanzitutto, nella facoltà per l'accusa e per la difesa di prendere piena coscienza delle osservazioni, degli elementi di prova, delle procedure seguite, per poterne eventualmente fare oggetto di discussione[26], nel rispetto del carattere di segretezza delle informazioni e della fase delle indagini[27].

L'accusato deve essere avvisato nel più breve tempo possibile della natura e dei motivi dell'accusa formulata a suo carico.

La Corte europea, sul punto, ha dichiarato che si tratta di un diritto che condiziona l'intero svolgimento del procedimento e che, pertanto, già nella prima fase delle indagini, l'interessato deve essere reso edotto delle norme di legge che si assumono da lui violate, la data, il luogo del fatto e il nome della vittima[28]. L'accusato, inoltre, ha inoltre il diritto di disporre del tempo necessario e delle giuste facilitazioni per poter approntare al meglio la propria difesa, personalmente o tramite l'assistenza di un difensore da lui scelto, gratuitamente se non ha i mezzi per poterlo retribuire. Costui può godere dell'apporto del legale in ogni fase del procedimento e vi può interloquire in ogni momento che ritenga opportuno[29].

La difesa deve essere effettiva e mai puramente formale[30]. Il codificato diritto alla ragionevole durata del processo è salvaguardato dalla Corte di

---

pagg. 1125-1132; U. VILLANI *I diritti fondamentali tra Carta di Nizza, Convenzione europea dei diritti dell'uomo e progetto di Costituzione europea* in *Diritto dell'Unione europea,* 2004, I, pagg. 73-116; I. WEILER *La costituzione dell'Europa,* Il Mulino, 2003.

[26] Così, Corte Europea dei Diritti dell'Uomo, 28 agosto 1991, Brandstetter c. Austria in *www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC (*consultato in data 30 maggio 2011).

[27] L'importanza della segretezza nella fase delle indagini è affermata, *ex multis,* nella sentenza della Corte Europea dei Diritti dell'Uomo, 11 gennaio 2000, Quadrelli c. Italia in *www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC* (consultato in data 5 giugno 2011).

[28] In questi termini, Corte Europea dei Diritti dell'Uomo, 25 marzo 1999, Pélissier e Sassi c. Francia e Corte Europea dei Diritti dell'Uomo, 19 dicembre 1989, Brozicek c. Italia.

[29] Sul punto si rinvia, *ex plurimis,* a Corte Europea dei Diritti dell'Uomo, 28 novembre 1991, S. c. Svizzera in *www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC* (consultato in data 20 giugno 2011).

[30] Così Corte Europea dei Diritti dell'Uomo, 22 febbraio 1994, Tripodi c. Italia in *www.echr.coe.int/ECHR/EN/Headr/Case-Law/HUDOC* (consultato in data 20 febbraio 2011).
La Corte Europea dei Diritti dell'Uomo non ha riconosciuto alcuna violazione dell'art. 6 CEDU nel caso Mader c. Croazia (n. 56185/07) in cui il ricorrente, cittadino croato, lamentava la mancanza di assistenza giuridica durante il suo interrogatorio da parte della polizia.

Strasburgo ed ha causato un elevato numero di ricorsi e di richieste di azioni riparatorie nei confronti di molti Stati, *in primis* contro il Governo italiano[31]. La Corte ha fornito ai giudici nazionali fondamentali criteri di valutazione in ordine ai limiti temporali, superati i quali si incorre in una violazione del principio della ragionevole durata del processo, evidenziando che la verifica deve essere comunque compiuta caso per caso[32]. Il termine di durata deve essere computato a partire dal primo atto d'indagine cha abbia prodotto effetti sulla situazione giuridica dell'imputato[33].

La Corte di Strasburgo fornito delle interpretazioni particolarmente garantiste dell'art. 6, secondo paragrafo, CEDU sulla tutela del principio di non colpevolezza, secondo cui i giudici non devono partire dall'idea preconcetta che la persona sospettata abbia commesso il reato, dovendo gravare sull'accusa l'onere della prova[34]. Concretamente questo significa che una decisione giudiziale concernente l'accusato non deve sottintendere l'idea originaria che questi fosse colpevole[35].

Sul principio di presunzione di innocenza ha agito l'interpretazione marcatamente teleologica della Corte europea, imponendo non solo al giudice ma anche ad ogni rappresentante dello Stato di trattare l'interessato da innocente e prescrivendo ogni rispetto e discrezione alle autorità statali nell'atto di informare il pubblico sulle inchieste penali in corso[36].

È la stessa Corte, però, che ha legittimato varie forme di restrizione del principio, riconoscendo la legittimità delle previsioni nazionali contenenti presunzioni di fatto o di diritto[37].

D'altro lato la Corte avvisa ed insieme ammonisce i giudici nazionali che formulano indebitamente opinioni sulle vicende giudiziarie portate alla loro attenzione[38].

---

[31] Il riferimento, *ex multis,* è alle sentenze della Corte Europea dei Diritti dell'Uomo, 6 settembre 2001, Brusco c. Italia e 27 marzo 2003, Scordino c. Italia. Non è esente da condanne per irragionevole durata del processo anche altri Stati quali la Russia: si veda, a titolo esemplificativo, la sentenza della Corte Europea dei Diritti dell'Uomo nel caso Chudun c. Russia (causa n. 20641/04). Così anche la Turchia nella sentenza della Corte Europea dei Diritti dell'Uomo nel caso Cingil c. Turchi (causa n. 29672/02).

[32] Così la sentenza della Corte Europea dei Diritti dell'Uomo, 31 marzo 1992, X c. Francia.

[33] Così la sentenza della Corte Europea dei Diritti dell'Uomo, 10 dicembre 1982, Corigliano c. Italia.

[34] Così la sentenza della Corte Europea dei Diritti dell'Uomo, 25 marzo 1983, Minelli c. Svizzera. L'importanza della garanzia della presunzione d'innocenza è ribadita anche nella sentenza della Corte Europea dei Diritti dell'Uomo, 24 maggio 2011, "Affare Panteion" Konstas c. Grecia (causa n. 53466/07).

[35] Così la sentenza della Corte Europea dei Diritti dell'Uomo, 25 marzo 1983, Minelli c. Svizzera, punto n. 37.

[36] Così, fra le altre, la sentenza della Corte Europea dei Diritti dell'Uomo, 10 febbraio 1995, Allenet de Ribemont c. Francia, punto n. 38.

[37] Così, *ex multis,* nella sentenza della Corte Europea dei Diritti dell'Uomo, 25 settembre 1992, Pham Hoang c. Francia dove la Corte ha posto come unico limite quello generica di ragionevolezza.

[38] Così la sentenza della Corte Europea dei Diritti dell'Uomo, 10 febbraio 1995, Allenet de Ribemont c. Francia e la sentenza del 25 agosto 1987, Lutz c. Repubblica Federale Tedesca.

E' significativa la scelta letterale effettuata nel testo della Convenzione Europea dei Diritti dell'Uomo, e mantenuta anche nelle sentenze della Corte di Strasburgo, di collegare la presunzione al concetto di innocenza e non anche a quello di non colpevolezza, risultando così cristallizzato il brocardo latino *in dubio pro reo.*

Un provvedimento giurisdizionale o amministrativo non deve essere eseguito, ma anzi deve essere riesaminato se, alla luce della sentenza della Corte di Giustizia, risulta che il diritto comunitario non sia stato applicato in conformità a quanto stabilito dai Trattati, sulla scorta dell'interpretazione che delle norme è data dai giudici comunitari[39].

La Corte Europea dei Diritti dell'Uomo ha frequentemente richiamato l'art. 8 CEDU in materia di garanzia del diritto alla riservatezza, con particolare riferimento allo svolgimento delle attività d'indagine nel procedimento penale[40].

Il diritto alla riservatezza si scontra con le mutate esigenze di rafforzamento della sicurezza che comporta, tra l'altro, lo sviluppo di rapporti di cooperazione tra le autorità di polizia e giudiziaria e lo scambio di dati e informazioni tra questi[41]. Il diritto alla *privacy*, in base all'interpretazione resa dalla Corte Europea dei Diritti dell'Uomo, entra in conflitto con il diritto ad un equo processo, soccombendo alle esigenze della giustizia. La Corte, infatti, legittima l'introduzione nel procedimento di prove che sono state acquisite in violazione del diritto alla riservatezza senza che ciò determini una violazione

---

[39] Così la sentenza della Corte di Giustizia CE del 12 febbraio 2008, causa C-2/06, su rinvio pregiudiziale proposto dal Finanzgericht Hamburg nel procedimento WillykempterKG contro Hauptzollarnt Hamburg Jonas in *Guida al Diritto,* 2008, 2, pagg. 52-59.

[40] Si veda, tra le altre, la sentenza della Corte Europea dei Diritti dell'Uomo, 16 novembre 2003, Elci e altri c. Turchia che riguardava un caso di perquisizioni eseguite in un'abitazione e negli studi dei ricorrenti. Le condanne da parte della Corte per violazione dell'art. 8 CEDU si registrano in numero elevato. Tra le più recenti è possibile citare la sentenza della Corte Europea dei Diritti dell'Uomo, 10 novembre 2005, Argenti c. Italia; sentenza della Corte Europea dei Diritti dell'Uomo, 11 gennaio 2005, Musumeci c. Italia e 14 ottobre 2004, Ospina Vargas c. Italia.

[41] Si pensi, a titolo esemplificativo, alla questione dei rapporti e della necessità di adeguare e bilanciare le esigenze di tutela dei diritti fondamentali e delle libertà con il soddisfacimento di nuove esigenze di sicurezza pubblica nella discussa previsione dell'istallazione dei *body scanner* negli aeroporti. L'introduzione di questi strumenti rispetta il principio di proporzionalità tra interessi pubblici contrapposti? La questione è ancora oggi al vaglio di esperti che si interrogano sul ruolo e sull'importanza dei *body scanner* per la sicurezza, specie mediante lo studio degli aeroporti in cui sono già utilizzati in via sperimentale. A tutela della riservatezza viene garantita la visione dell'immagine scannerizzata dell'immagine solo da parte di un analista che risiede in un luogo chiuso e senza possibilità di guardare direttamente l'interessato. Il passeggero che verrebbe comunque perquisito, il quale è libero di scegliere tra la sottoposizione al metodo tradizionale o la procedura automatizzata.
Sulla valutazione dell'impatto dei *body scanner* sui diritti fondamentali si invita alla consultazione del sito internet del Parlamento europeo (www.europarl.europa.eu). Sul punto sono interessanti le dichiarazioni rilasciate dal Garante Privacy italiano, dott. Pizzetti, consultabili sul sito www.mytech.it.

dell'art. 6 CEDU[42]. Questo scarto generato dai Giudice comunitari nell'irrinunciabile rapporto tra il diritto alla *privacy* ed il diritto ad un equo processo è parzialmente superato dalla previsione dell' *exclusionary rule*.

Alla luce di questo sistema legislativo e giudiziale di protezione dei diritti fondamentali, i cittadini sono carichi di nuove aspettative anche e soprattutto per il crescente flusso della giurisprudenza della Corte Europea dei Diritti dell'Uomo, in un processo di confronto a volte agonistico con la Corte di Giustizia UE. La giurisprudenza di Strasburgo realizza una cd. *judicial law making* che riconosce autorevolezza ai propri precedenti e impone agli Stati parte della Convenzione un obbligo di conformità. La Corte EDU infatti ha un potere vincolante diretto verso i Paesi coinvolti nel caso particolare sottoposto alla sua giurisdizione, ma anche un potere vincolante indiretto per tutti gli altri Stati perché traccia la corretta interpretazione delle disposizioni convenzionali per evitare di incorrere in violazioni[43]. Tuttavia, riconoscendo alle pronunce della Corte Europea dei Diritti dell'Uomo l'autorità della cosa interpretata, si richiede di conseguenza un vaglio attento dei principi ivi espressi e della loro trasferibilità negli ordinamenti interni. Per questo motivo la stessa Corte segue un approccio argomentativo capace di gestire il pluralismo degli ordinamenti statali, aprendosi alla considerazione di un margine nazionale di apprezzamento nazionale che permette di adattare lo *ius commune* alle specificità dei singoli Stati e di coniugare l'universalismo dei diritti umani con il relativismo delle tradizioni nazionali[44].

D'altronde, come attestato in plurime sentenze della Corte di Strasburgo, la Convenzione non si interessa di diritti astratti ma di diritti concreti di cui è titolare ciascun individuo per il solo fatto di appartenere alla giurisdizione di un Stato europeo[45].

Molte sentenze della Corte europea, infatti, si interessano ad un caso concreto sottoposto al suo controllo giurisdizionale, non sono portatrici di principi generali ed astratti[46].

---

[42] Così, *ex multis,* nella sentenza della Corte Europea dei Diritti dell'Uomo, Khan c. United Kingdom del 2000.

[43] Cfr V. MANES – V. ZAGREBELSKY (a cura di), *op.cit.,* pagg. 20-22.
La tesi pluralista ritiene che le sentenze della Corte EDU abbiano efficacia diretta ed esecutiva e che vincolino anche gli Stati terzi, poiché è proprio la giurisprudenza europea a concretizzare e rinnovare i contenuti della Convenzione.

[44] Cfr M. DELMAS MARTY – M. L. IZORCHE *Marge nationale d'appréciation et internationalization du droit* in *Revue international du droit compare,* 2000, pagg. 753 ss.
Gli Autori ritengono che il margine di apprezzamento identifica il diritto di ogni Stato ad invocare le peculiarità del proprio sistema giuridico per giustificare un certo scarto dalle prescrizioni della convenzione.

[45] Il riferimento è latamente anche al contenuto dell'art. 1 CEDU.

[46] Si consideri, per esempio, la sentenza della Corte Europea dei Diritti dell'Uomo, 17 luglio 2003, Craxi c. Italia. In questo caso il giudice di Strasburgo ha riconosciuto la violazione dell'art. 8 CEDU da parte dello Stato italiano per mancato adempimento di una fase processuale che avrebbe garantito la tutela

Da quanto ricostruito emerge il prezioso contributo fornito dalla Carta di Nizza, dalla Corte Europea dei Diritti dell'Uomo e dalla giurisprudenza delle Corti nella prospettiva del riconoscimento di uno *standard* minimo armonizzato di garanzia dei diritti fondamentali. Questo sistema si riflette direttamente sulle legislazioni nazionali, imponendo degli obblighi di interpretazione conforme e, se del caso, di riforma della disciplina interna in conformità alla norma comunitaria.

2.2 *Le garanzie dei diritti fondamentali negli ordinamenti degli Stati membri in un approccio esemplificativo di diritto comparato nella normativa di attuazione della DQ MAE*

Nell'ideale accoglimento dell'invito fatto agli Stati di fare proprio il principio del riconoscimento reciproco, come nelle conclusioni del Consiglio di Tampere del 15 e 16 ottobre 1999, il 13 giugno 2002 è stata adottata la Decisione quadro 2002/584/GAI, relativa al mandato d'arresto europeo e alla procedura di consegna tra Stati membri.

Il progetto è nato da un Trattato bilaterale sottoscritto tra la Repubblica italiana e il Regno di Spagna per il perseguimento di reati gravi attraverso il superamento dell'ormai vetusta procedura dell'estradizione, firmato il 28 novembre 2000 a Roma e basato proprio sul mutuo riconoscimento tra i due Stati, nella consapevolezza del rispetto degli obblighi sanciti dalla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950.

Tale Trattato è stato superato dal mandato di arresto, appunto.

La decisione quadro 2002/584/GAI ha segnato un passo importante nel lento processo di integrazione dei sistemi giudiziari penali all'interno dell'Unione europea poiché costituisce uno dei pochi istituti la cui disciplina è stata recepita in tutti gli ordinamenti degli Stati membri. L'obiettivo che si è inteso raggiungere riguarda la previsione di una forma semplificata ed accelerata di consegna delle persone ricercate ai fini dell'esercizio dell'azione penale o dell'esecuzione di una pena o di una misura di sicurezza privativa della libertà[47]. Trattasi di un regime giuridico che, a differenza della procedura estradizionale, prescinde dall'intermediazione dell'autorità politica, svolgendosi interamente a livello giurisdizionale.

---

della riservatezza del ricorrente. In particolare, erano state pubblicate sui quotidiani nazionali diverse intercettazioni telefoniche private di Craxi senza che fosse prima celebrata tra le parti l'udienza stralcio, in cui cancellare tutte le registrazioni non utili ai fini di giustizia.

[47] Cfr art. 1 Decisione quadro, pubblicata in Gazzetta Ufficiale CE, 18 luglio 2002, L. 190/1.

L'attuazione del mandato di arresto realizza un miglioramento rilevante della cooperazione giudiziaria e di polizia, al fine di impostare una lotta efficace alle forme più gravi di criminalità. Questo strumento tanto innovativo è soggetto alla valutazione critica della Commissione europea e richiede un costante bilanciamento tra le esigenze di sicurezza e giustizia e la tutela dei diritti fondamentali, specie afferenti alle garanzie procedurali.

Con riferimento ai soli principi generali della Decisione quadro, il mandato di arresto europeo può essere emesso in caso condanna con una sentenza definitiva ad una pena detentiva o ad una misura di sicurezza privativa della libertà di durata non inferiore a quattro mesi; reati puniti con una pena detentiva o con una misura di sicurezza privativa della libertà di durata massima non inferiore a dodici mesi. Fra i reati che comportano la consegna senza verifica della doppia incriminazione del fatto e a condizione che siano puniti nello Stato membro di emissione di una pena massima pari o superiore a tre anni, figurano: terrorismo, tratta di esseri umani, corruzione, partecipazione a un'organizzazione criminale, falsificazione di monete, omicidio, razzismo e xenofobia, stupro, traffico di veicoli rubati, frodi, comprese quelle che ledono gli interessi finanziari dell'Unione. Per i reati diversi da quelli elencati, la consegna può essere subordinata alla condizione che il fatto per il quale è stata richiesta la consegna costituisce un reato ai sensi della legge dello Stato membro d'esecuzione (norma della doppia incriminazione). Gli Stati membri designano le autorità giudiziarie competenti in materia e ne informano il segretario generale del Consiglio e, se lo ritengono necessario, designano anche un'autorità centrale incaricata di prestare assistenza alle autorità giudiziarie. Il mandato di arresto deve obbligatoriamente contenere una serie di informazioni, quali l'identità della persona, l'autorità giudiziaria emittente, la sentenza definitiva, la natura del reato e la pena. In allegato alla Decisione quadro si trova un formulario utilizzato per le richieste di mandato di arresto.

A livello procedurale, l'autorità emittente comunica il mandato d'arresto europeo direttamente all'autorità giudiziaria d'esecuzione. Ogni Stato può adottare le misure coercitive necessarie e proporzionate nei confronti di una persona ricercata. Le decisioni relative all'esecuzione di un MAE sono sottoposte ad un "controllo sufficiente" da parte dell'autorità giudiziaria dello Stato di esecuzione. Il testo della Decisione prevede diverse ipotesi di rifiuto (art. 4). In attesa di una decisione, l'autorità dell'esecuzione procede all'audizione della persona interessata. Entro sessanta giorni successivi all'arresto, l'autorità giudiziaria deve prendere una decisione definitiva sull'esecuzione del mandato d'arresto europeo. Successivamente notifica immediatamente la decisione presa dall'autorità emittente. Qualora le informazioni comunicate dall'autorità emittente risultino insufficienti,

l'autorità d'esecuzione può richiedere informazioni supplementari. La persona interessata può esprimere il suo consenso alla consegna in modo irrevocabile ed essendo pienamente informata delle conseguenze. Ogni Stato membro resta libero di prevedere che, a certe condizioni, il consenso è irrevocabile mediante una dichiarazione da presentare nell'atto di adozione della Decisione quadro[48].

La Corte di Giustizia UE, con la sentenza del 3 maggio 2007, resa nell'ambito del procedimento C-305/05, incardinato sulla domanda di pronuncia pregiudiziale sollevata dall'*Arbitragehof* del Regno di Belgio, ha preso per la prima volta posizione su alcuni aspetti della Decisione quadro MAE, in particolare generando spunti di riflessione sui principi di legalità, uguaglianza e non discriminazione[49]. In particolare, la Corte ha ritenuto che la soppressione del principio di doppia incriminazione per le trentadue categorie di reato elencate, non determina una violazione del principio di legalità, atteso che la definizione degli stessi e delle sanzioni resta di competenza degli Stati; così l'individuazione di fattispecie di reato di cui all'art. 2 Decisione quadro non comporta alcuna violazione del principio di uguaglianza, trattandosi di condotte che, per loro natura e per l'entità della pena comminata, giustificano l'applicazione di una modalità obbligatoria. Occorre peraltro considerare che l'opposizione di possibili contro limiti all'esercizio di un potere punitivo carente dal punto di vista della garanzia dei diritti procedurali e dei diritti fondamentali richiamati dall'art. 6 TUE, discende dalle modalità di applicazione della Decisione quadro da parte degli Stati membri che delineano un obbligo di *standard* di tutela dell'interessato, anche mediante l'individuazione di motivi di non esecuzione e di regimi di garanzia elevati in particolari circostanze.

In considerazione del carattere comunque vincolante della Decisione quadro e della sua sostanziale omogeneità con la strumento della direttiva comunitaria, pare inoltre possibile ritenere sussistente, in capo al giudice nazionale, un obbligo di interpretazione conforme del diritto nazionale al

---

[48] Per un approfondimento sulla disciplina del mandato di arresto europeo si rinvia, *ex multis*, a A. BALSAMO *La decisione quadro sul mandato d'arresto non viola il diritto comunitario* in *Cassazione penale,* 2007, pagg. 881-886; A. BERNARDI – C. GRANDI *Gli effetti della prescrizione e dell'amnistia sull'estradizione e sul mandato di arresto europeo* in *Cassazione penale,* 2005, pagg. 3561-3577; E. BRUTI LIBERATI – I. J. PATRONE *Il Mandato di Arresto europeo* in *Questione Giustizia,* 2002, pagg. 70-89; M. CHIAVARIO *Giustizia: il mandato di cattura europeo mette a nudo le contraddizioni italiane* in *Guida al Diritto,* 2001, pagg. 11 ss.

[49] Per una consultazione del testo della sentenza della Corte di Giustizia CE si rinvia a *Cassazione penale,* 2007, pagg. 3078 ss.

Quanto al commento alla decisione si veda G. DE AMICIS – O. VILLONI *Mandato di arresto europeo e legalità penale nell'interpretazione della Corte di Giustizia* in *Cassazione penale,* 2008, pagg. 383-405.

contenuto e alle finalità della Decisione, sia nell'ipotesi in cui esista una specifica norma di attuazione, sia quando questa manchi[50].

Il successo complessivo dell'impatto dell'attuazione del mandato di arresto europeo è attestato a chiare lettere già nella relazione della Commissione europea del 23 febbraio 2005[51] dalla quale si rileva che, superato il ritardo iniziale di trasposizione, la sua applicazione risulta efficace e i tempi di consegna di una persona avvengono in media tra tredici e quarantatre giorni, contro i precedenti nove mesi.

Il quadro normativo di recepimento della Decisione MAE mostra uno scarto tra la speditezza dei lavori in seno all'UE[52] e gli sforzi di attuazione dei Legislatori nazionali. Solo sei Stati, infatti, hanno rispettato il termine fissato dalla Decisione quadro[53], mentre la maggior parte delle leggi risalgono a1 2004 o addirittura, come per il caso dell'Italia, al 2006.

La disciplina contenuta nella Decisione quadro MAE presenta alcune carenze a livello di tutela dei diritti fondamentali. Per esempio, nel *considerandum* 13 è stabilito che "*nessuna persona dovrebbe essere allontanata, espulsa o estradata verso uno Stato membro allorquando sussista un serio rischio che essa venga sottoposta alla pena di morte, alla tortura o ad altri trattamenti inumani o degradanti*". La formulazione appare restrittiva nel rispetto della pluralità di ipotesi previste ad esclusione dell'estradizione per rischio di violazione di diritti fondamentali e anche di diritti processuali[54].

Va inoltre osservato che l'elenco dei diritti del ricercato, contenuti nell'art. 11 Decisione quadro, appare scarno rispetto al catalogo previsto dall'art. 6 CEDU.

---

[50] Il riferimento è alla nota sentenza Pupino della Corte di Giustizia CE, 16 giugno 2005, in *Cassazione penale,* 2005, pagg. 3167 ss.

[51] Cfr COM(2005) 63 definitivo.
La relazione non è mai stata pubblicata in Gazzetta Ufficiale CE ma è consultabile sul sito *internet* http://europa.eu/legislation_summaries (consultato in data 15 gennaio 2010).

[52] L'accordo politico tra gli Stati membri dell'Unione europea è stato raggiunto sin dal dicembre 2001, a pochi mesi di distanza del tragico evento dell'11 settembre alle *Twin Towers* ed a seguito di un Consiglio europeo straordinario le cui conclusioni affermavano che *"l'ordine di arresto sostituirà l'attuale sistema di estradizione tra Stati membri. Infatti le procedure attuali di estradizione non rispecchiano il livello di integrazione e di fiducia tra gli Stati membri dell'Unione europea. Pertanto l'ordine di arresto europeo consentirà la consegna diretta delle persone da autorità giudiziaria ad autorità giudiziaria, garantendo al tempo stesso i diritti e le libertà fondamentali".*
Cfr G. DE AMICIS *Attuazione del mandato d'arresto europeo e tutela dei diritti fondamentali: ambito di applicazione e limiti delle garanzie procedurali a favore di indagati e imputati nel territorio dell'Unione europea* in *Quaderni del Consiglio Superiore della Magistratura,* 148, 2006.

[53] Si tratta di Belgio, Danimarca, Spagna, Portogallo, Regno Unito e Svezia.
Cfr V. BAZZOCCHI *Il mandato di arresto europeo e le Corti supreme nazionali* in *Il Diritto dell'Unione Europea,* 3, 2007, pagg. 103-125.

[54] La Corte di Giustizia CE, nella sentenza del 26 giugno 1992, Drozd c. Francia e Spagna, ha statuito il limite all'estradizione anche nei casi di rischio di violazione di diritti processuali.

Sulla base di tali rilievi non deve pertanto stupire l'intervento di diverse Corti nazionali a tutela dei diritti fondamentali previsti nelle rispettive Carte costituzionali.

Il caso della Germania è particolarmente interessante poiché, quasi profeticamente, poco prima dell'adozione della Decisione quadro sul mandato di arresto europeo, è stato revisionato, con Legge federale del 29 novembre 2000, l'articolo 16, paragrafo 2, del *Grundgesetz*. La nuova disposizione ammette che una deroga al divieto d'estradizione di un cittadino tedesco possa essere prevista per consentire la consegna di quest'ultimo ad un'autorità di un altro Stato membro dell'Unione europea o ad una Corte internazionale, a condizione che i principi fondamentali alla base della *rule of law* siano rispettati[55].

La Legge federale tedesca del 21 luglio 2004, *Europaisches Haftdefehsgesetz*, di recepimento della Decisione MAE è stata sottoposta al vaglio di costituzionalità del *Bundesverfassunsgericht* ed annullata *in toto* per violazione dell'art. 16 Legge fondamentale. La Corte ha ritenuto infatti che il Legislatore tedesco non avesse sfruttato appieno ed in modo coerente i margini di adeguamento consentiti dalla Decisione quadro, venendo meno al principio dello Stato di diritto. In particolare, i Giudici costituzionali hanno riscontrato un mancato rispetto del principio di proporzionalità, di certezza del diritto e di tutela del legittimo affidamento. Il Legislatore viene chiamato a riformulare i motivi di inammissibilità della consegna in rapporto al singolo caso concreto, secondo la gravità del fatto, le esigenze di effettiva repressione dei reati e gli interessi dell'indagato tutelati costituzionalmente, tenendo altresì in debita considerazione gli obiettivi derivanti dalla creazione di uno spazio giuridico comune europeo[56]. In un passaggio della sentenza la Corte ha affermato che la mera esistenza dell'art. 6 TUE e di uno *standard* comune europeo dei diritti fondamentali assicurato dalla CEDU, da solo non giustifica l'assunto secondo cui le conformazioni dello Stato di diritto tra i Paesi membri dell'Unione europea non facciano corrispondere un esame nazionale nel singolo caso concreto.

In Francia la legge di attuazione del mandato di arresto europeo è del 2004. In più casi la Corte di Cassazione francese si è trovata a decidere di

[55] Cfr O. POLIICINO *Incontri e scontri tra ordinamenti e interazioni tra giudici nella nuova stagione del costituzionalismo europeo: la saga del mandato di arresto europeo come modello d'analisi* in *http://www.ejls.eu/4/58IT.htm* (sito consultato in data 16 novembre 2010).

[56] Il riferimento è alla sentenza della Corte costituzionale tedesca del 18 luglio 2005 in V. BAZZOCCHI *op.cit.*, pag. 107-108.

ricorsi presentati da persone interessate dall'esecuzione di un mandato di arreso, lamentando violazioni dell'art. 6 CEDU [57].

Il Consiglio europeo nel 2007, nel *report* compilato in relazione all'osservazione dell'attuazione della Decisione quadro sul mandato di arresto europeo in Francia[58], ha valutato positivamente gli sforzi compiuti anche in supporto a coloro che, praticamente, eseguono o avanzano una richiesta di mandato di arresto. Nel territorio francese è attiva una rete intranet, accessibili dalle autorità giudiziarie e di polizia che attuano il MAE ove possono trovare una lista di esperti a cui rivolgersi, delle indicazioni sulle procedure da seguire, un forum di domande/risposte per evitare violazioni di leggi o di diritti fondamentali nell'applicazione della norma in materia.

Le riforme al codice di procedura penale francese tutelano i diritti della persona interessata, fin dal suo arresto: diritto ad essere informato, a informare a mezzo telefono del proprio stato, ad essere assistito da un interprete e da un legale, con il quale poter interloquire quando lo ritiene opportuno.

Il gruppo di esperti ha però riferito di un disequilibrio tra accusa e difesa nella parte in cui la legislazione francese non prevede un accesso rapido alle informazioni da parte del difensore della persona interessata da una richiesta di mandato di arresto europeo che, proposto appello, si trova a dovere preparare l'udienza di discussione.

La Francia, come l'Italia (e così anche l'Austria), ha reso la dichiarazione unilaterale ai sensi dell'art. 32 Decisione MAE, indicando alcune condizioni di diritto transitorio per la definitiva sostituzione del sistema dell'estradizione con il mandato di arresto europeo, continuando ad applicare il sistema tradizionale di consegna delle persone per tutti i reati commessi prima di una certa data[59] .

L'Italia ha implementato la Decisione quadro MAE solo con la legge 12 aprile 2005, n. 69, pubblicata sulla Gazzetta Ufficiale del 29 aprile 2005, n. 98, quindi con sedici mesi di ritardo rispetto alla data fissata dalla norma europea per la sua attuazione negli ordinamenti nazionali [60].

---

[57] è il caso, a titolo esemplificativo, della sentenza della Corte di Cassazione francese, 27 giugno 2006, n. 84186, consultabile sul web all'indirizzo: http://www.asser.nl/Default.aspx?site_id=8&level1=10789&level2=10830&level3=10987 (consultato in data 30 giugno 2011).

[58] Cfr Report del Consiglio europeo del 20 luglio 2007 in *http://www.asser.nl/eurowarrant-webroot/documents/cms_eaw_id1553_1_CouncilDoc.9972.2.07%20Rev%202.pdf* (sito consultato in data 2 luglio 2011).

[59] La Francia ha indicato la data del 1à novembre 1993, l'Italia del 7 agosto 2002, data di entrata in vigore della Decisione quadro.
Cfr G. DE AMICIS *op.cit.,* pagg. 17-18.

[60] La Decisione quadro, infatti, prevedeva il termine ultimo del 31 dicembre 2003 per l'attuazione del MAE negli Stati membri.

Il recepimento della Decisione ha sollevato fin dall'inizio dubbi di incompatibilità con la Costituzione italiana, in particolare con il diritto di uguaglianza, il diritto di riservatezza, il principio di riserva di legge e la necessaria determinatezza delle fattispecie penali. La legge italiana, infatti, si discosta sotto diversi punti di vista dalle scelte operate dalla norma comunitaria, specie in relazione alla reintroduzione del principio di doppia incriminazione, della subordinazione della consegna alla sussistenza di gravi indizi di colpevolezza, all'obbligatorietà di casi di rifiuto della consegna[61].

L'art. 2 della Legge indica le garanzie di ordine costituzionale che debbono essere osservate nell'esecuzione del mandato di arresto europeo. La norma rinvia a un insieme di diritti fondamentali, principi e regole in materia di giusto processo, libertà fondamentale, diritto di difesa, principio di uguaglianza, responsabilità penale e qualità della sanzione penale, contenuti nella Convenzione Europea dei diritti dell'uomo e delle libertà fondamentali e nella Costituzione italiana, la cui concreta verifica può rendere necessaria una richiesta di idonee garanzie allo Stato membro di emissione. L'ampio richiamo ai diritti fondamentali della CEDU e dei Protocolli addizionali rileva per tutte le previsioni che racchiudono diritti inviolabili dell'imputato o del condannato e danno corpo a valori fondanti della società democratica, suscettibili di limitare l'applicazione delle procedure di cooperazione.

La Commissione europea, nel rapporto del 2007, ha ritenuto la disposizione dell'art. 2, L. 60/05 in contrasto con l'art. 6 TUE poiché fa riferimento ai soli principi costituzionali comuni agli Stati membri [62].

Un'importante apertura ai diritti fondamentali della CEDU in tema di equo processo e giudizio contumaciale è stata operata di recente dalla giurisprudenza di legittimità che, muovendo dal presupposto per cui il legislatore italiano ha accettato incondizionatamente la forza vincolante delle sentenze della Corte di Strasburgo, ha stabilito che, nel pronunciare sulla richiesta di restituzione nel termine per appellare proposto da un condannato dopo che il suo ricorso è stato accolto dalla Corte, il giudice è tenuto a conformarsi alle decisioni con cui si è riconosciuto che il processo celebrato *in absentia* non è un processo equo, non potendosi escludere il diritto alla celebrazione di un nuovo processo per violazione dell'art. 6 CEDU [63].

---

[61] Per i riferimenti e gli opportuni approfondimenti sulla legge italiana di attuazione della Decisione quadro sul mandato di arresto europeo si rinvia a G. DE AMICIS *op.cit.;* C. M. PAOLUCCI *Cooperazione giudiziaria, op.cit.,* pagg. 601-672; E. APRILE – F. SPIEZIA *Cooperazione giudiziaria penale, op.cit.,* pagg. 182-186; E. APRILE *Diritto processuale penale europeo e internazionale,* Cedam, 2007, pagg. 82-101.

[62] Cfr Rapporto di valutazione della Commissione europea dell'11 luglio 2007, SEC(2007) 979.

[63] Il riferimento è alla sentenza della Corte di Cassazione, sez. I, 12 luglio 2006, Somogyi in *Diritto e Giustizia,* 2006, 38, pagg. 51 ss.

Le Sezioni Unite della Corte di Cassazione italiana hanno delineato i confini dell'art. 18, lett. e), stabilendo il principio secondo cui l'autorità giudiziaria italiana deve verificare, ai fini della consegna, se nella legislazione dello Stato membro di emissione sia espressamente fissato un termine di durata della custodia cautelare fino alla sentenza di condanna di primo grado o, in mancanza, se un limite temporale implicito sia comunque desumibile da altri meccanismi processuali che instaurino, obbligatoriamente e con cadenze predeterminate, un controllo giurisdizionale, funzionale alla legittima prosecuzione della custodia cautelare o, in alternativa, all'estinzione della stessa[64]. L'interpretazione della condizione ostativa va inquadrata nel più ampio contesto normativo ed ermeneutico del diritto alla ragionevole durata della custodia cautelare *ante iudicium,* così come riconosciuto dall'art. 5 CEDU.

L'art. 13 comma 5 della Legge italiana statuisce l'assolutezza della garanzia costituzionale che, in base all'interpretazione data dalle Sezioni Unite della Corte di Cassazione, deve essere inquadrata in un più ampio contesto multilivello, che tiene conto non solo dello scopo della norma comunitaria e dell'elaborazione giurisprudenziale della Corte europea dei diritti dell'uomo, ma anche della necessaria esigenza di raccordare il quadro normativo e giurisprudenziale europeo con il sistema processuale ed i principi fondamentali in tema di limiti temporali massimi della carcerazione preventiva "*al di là dei quali verrebbe compromesso il bene della libertà personale, che costituisce una delle basi della convivenza civile*"[65].

A maggiore tutela del diritto alla libertà personale, la Corte di Cassazione si è pronunciata affermando che "*in ragione dei principi di comune civiltà giuridica propri dello spazio giuridico europeo e fissati nella Convenzione europea dei diritti dell'uomo, i provvedimenti restrittivi della libertà personale devono essere fondati su indizi di colpevolezza, cioè su elementi evocativi di un fatto di rilevanza penale attribuibile ad un soggetto, che rendono possibile l'affermazione della sua responsabilità penale a seguito di un regolare processo*"[66]

In relazione al parametro fissato nell'art. 3 Cost., l'esplicitazione a livello nazionale di garanzie fondamentali in qualche misura ricavabili dal testo della Decisione quadro o comunque desumibili dalle generali finalità di rispetto dei principi di cui all'art. 6 TUE, dovrebbe avvenire secondo un criterio di ragionevolezza, tale da non pregiudicare l'impianto strutturale e la funzionalità propria dello strumento comunitario che si attua.

A garanzia del diritto di difesa nella procedura camerale finalizzata alla decisione in ordine alla consegna, la Corte di Cassazione ha stabilito che

[64] Il riferimento è alla sentenza della Corte di Cassazione, Sezioni Unite, 5 febbraio 2007, n. 4614, Ramoci in *Cassazione penale,* 2007, pagg. 1911 ss.
[65] Così la sentenza della Corte costituzionale, 22 luglio 2005, n. 299 in *Cassazione penale,* 2005, pagg. 3246 ss.
[66] Cfr Corte di Cassazione, sez. VI, 23 settembre 2005, n. 3455, Ilie, CED, rv. 232053.

"*quando l'interessato abbia nominato due difensori, entrambi hanno diritto all'avviso della data dell'udienza camerale; tuttavia, ove sia stata omessa la comunicazione a uno dei difensori, si verifica una nullità a regime intermedio*"[67].

Alla luce della generalità del principio di non discriminazione e della possibilità demandata ai singoli Stati membri di modulare eventuali differenze di disciplina, le limitazioni alla parità di trattamento tra il cittadino italiano e il cittadino di uno Stato diverso, sono consentite, secondo la Corte costituzionale italiana, solo se proporzionate ed adeguate[68].

Le differenze tra le varie legislazioni nazionali d'attuazione del MAE; come previsto e legittimato dalla Decisione quadro, rende a volte difficile coniugare l'efficacia dello strumento di cooperazione, l'accrescimento della fiducia reciproca tra gli Stati membri e la tutela dei diritti fondamentali. L'affidamento tra i Paesi dell'UE e l'agevolazione degli scambi per i fini della sicurezza e della giustizia si scontrano spesso con le diversità di disciplina che ostacolano i rapporti ed i flussi di richiesta ed esecuzione del mandato di arresto europeo, anche in considerazione di una diversa previsione di garanzia dei diritti.

3. *Linguaggio e traduzione giuridica per la concreta attuazione dei diritti fondamentali*

Dal punto di vista giuridico, l'Unione europea si caratterizza per le diversità di tradizioni e per i particolarismi normativi che, da soli, rendono difficile una comunicazione ed una circolazione di dati ed informazioni tra gli Stati, unito al plurilinguismo e ai problemi di traduzione giuridica.

L'Europa unita si presenta come una realtà multiculturale e multilinguistica.

A livello pratico si osserva quotidianamente che la traduzione da e verso ogni lingua dell'UE è ormai impraticabile[69].

Questo può potenzialmente pregiudicare la piena garanzia dei diritti fondamentali di ciascun individuo, sia nel caso estremo in cui non venga fornita alcuna traduzione di un atto o di una disposizione di legge in una lingua comprensibile per l'interessato, sia quando le differenze tra i diritti

[67] Cfr Corte di Cassazione, sez. VI, 2 aprile 2008, n. 18726, CED, rv. 239722.
[68] Cfr Corte costituzionale, 21 giugno 2010, n. 227 in *www.cortecostituzionale.it* (consultato in data 25 gennaio 2011).
[69] Così B. POZZO – V. JACOMETTI *Le politiche linguistiche delle istituzioni comunitarie dopo l'allargamento,* Giuffré, 2006, pagg. 4-5.

nazionali rendono impossibile la traduzione di concetti giuridici facenti parte di altre tradizioni giuridiche.

Da ciò emerge il ruolo fondamentale del giurista-linguista ovvero, per coloro che guardano con scetticismo la figura che unisce competenze linguistiche a conoscenze giuridiche, della collaborazione stretta tra i traduttori e interpreti e gli esperti di diritto, per cercare di identificare i significati che corrispondono al medesimo concetto negli Stati membri [70].

I concetti giuridici sono intimamente collegati con le vicende intellettuali e culturali di un dato contesto e quindi con la lingua con cui questo si esprime. Il linguaggio giuridico di un dato ordinamento riverbera tassonomie specifiche che si sono sviluppate nel corso di anni, decenni, secoli, millenni e che si fondano sullo sviluppo storico di un dato sistema giuridico.

Le sfide del linguaggio e della traduzione giuridica sono aumentate considerevolmente a seguito dell'ampliamento dell'Unione europea verso i Paesi dell'Est.

La stessa di Corte di Giustizia si confronta giornalmente con il multilinguismo che caratterizza l'Unione europea nella sua funzione di assicurazione dell'uniforme interpretazione del diritto comunitario.

La presenza di testi multilingua, tutti facenti fede come previsto dall'art. 314 TUE, rende indubbiamente più complesso il ruolo dell'interprete perché il raffronto tra i diversi testi può far emergere conflitti tra i relativi contenuti.

I diversi scenari prospettabili muovono tutti dall'assunto che la presenza di testi ufficiali esclude che possa accordarsi la preferenza all'uno o all'altro, implicando di cercare, nel raffronto, un significato oggettivo che esprima la volontà comune degli Stati[71].

L'operazione di traduzione, qualsiasi materia interessi, è caratterizzata da determinate regole comuni di base ma per tradurre correttamente il linguaggio giuridico sono necessarie delle competenze superiori, al fine di superare gli ostacoli tecnici propri del mondo del diritto.

Secondo il giurista belga J. B. Herbots, la differenza tra traduzione giuridica e traduzione ordinaria risiede nel fatto che *il testo da tradurre è una regola giuridica, una decisione giudiziaria o un atto giuridico che ha conseguenze giuridiche volute e da conseguirsi*[72].

---

[70] La diatriba tra i sostenitori della figura del giurista-linguista e i sostenitori della necessaria divisione in almeno due soggetti delle competenze linguistiche (di traduzione ed interpretazione) e delle conoscenze giuridiche, è sorta in seno al convegno tenutosi il 14 luglio 2011 presso l'Università degli Studi dell'Insubria, dal titolo *Giuristi, lingua ed Unione europea: la circolazione dei concetti in un mondo multilingua.*

[71] Cfr B. POZZO – V. JACOMETTI *op.cit.*, pagg. 93-98.

[72] Cfr J. B. HERBOTS *La tradution juridique. Un point de vue belge* in *Cahiers de droit,* 1987, pagg. 813-844.

Indipendentemente dal metodo usato, lo scopo della traduzione giuridica è produrre testi che siano almeno equivalenti se non identici. La nozione di equivalenza rimane controversa a causa delle difficoltà incontrate dagli studiosi di traduzione e dai linguisti nel definire il termine in maniera precisa. Di conseguenza, l'equivalenza viene associata a differenti e vaghe etichette che possono creare confusione ed incomprensioni. Il problema risiede, nel campo del diritto, nel ricerca un equivalente non solo a livello linguistico ma anche giuridico, fondendo ed amalgamando i due ingredienti costitutivi del testo che producono l'equivalenza ricercata [73].

In un quadro europeo e mondiale di globalizzazione dei rapporti socio-economici, e quindi anche giuridici, lo scambio tra autorità straniere e l'impatto con atti, norme e sentenze "nate altrove", costituiscono un ineliminabile elemento caratterizzante dello spazio UE[74].

Lo sviluppo dei rapporti di cooperazione tra gli Stati membri ha definitivamente consegnato all'interprete un quadro normativo e giuridico multilivello, caratterizzato da un plurilinguismo e dalle relazioni tra ordinamenti giuridici di diversa tradizione.

Ci si muove, dunque, su un terreno sdrucciolevole che richiede un controllo serrato non solo di mera traduzione linguistica ma anche di interpretazione dei concetti.

Un'opera interpretativa si può dire proficua se è in grado di risalire efficacemente all'intenzione del legislatore o del giudice "altro", facendo salva la lettera e lo spirito del testo tradotto [75].

La ricchezza della lingua e del linguaggio giuridico spesso produce confusione, ora a causa di un uso atecnico di alcuni termini ora con l'utilizzo di espressioni diverse per indicare lo stesso concetto o lo stesso istituto.

Da una considerazione empirica e d'esperienza, la lingua maggiormente usata a livello internazionale, nelle conferenze, negli atti, nella diplomazia è certamente l'inglese. È sotto gli occhi di tutti l'influenza della lingua inglese in molte espressioni del vivere quotidiano.

Per questi motivi non è illogico ragionare sulla possibilità di applicare un idioma comune per la comunicazione in ambito UE che ben può essere rappresentato dalla lingua inglese, generando un abbattimento dei costi di traduzione e un maggiore grado di comprensione delle comunicazioni, delle norme, degli atti da parte dei soggetti interessati.

---

[73] Per un approfondimento sulle differenze e le difficoltà di traduzione nel *plain language* e nel linguaggio giuridico, si rinvia a B. POZZO (a cura di) *Ordinary language and legale language,* Giuffré, 2005.

[74] E. SELVAGGI *L'arabo, il parto, il siro in suoo sermon l'udì: riflessioni sulla Babele delle lingue nei rapporti giurisdizionali con autorità straniere* in *Scritti in onore di Mario Pisani,* La Tribuna, 2010.

[75] Cfr *Ibidem.*

Questo scenario si scontra con le difficoltà di traduzione-interpretazioni di tutti i termini ed i concetti giuridici in questa possibile lingua comune dell'Unione per una sorta di insufficienza epistemologica e semantica, in contrapposizione con la ricchezza dei linguaggi giuridici nazionali.

Ad oggi esiste un solo vecchio dizionario di inglese giuridico che non permette una traduzione precisa ed efficace di una pluralità di termini e concetti ricorrenti negli atti, nelle norme e nelle sentenze.

Gli interpreti devono cercare di colmare il vuoto, di caso in caso, anche da uno studio dei casi in cui un determinato istituto viene applicato, per cercare di comprenderne il significato intimo[76].

Alcune banche dati di terminologia giuridica multilingua, quali lo IATE[77], aiutano, tuttavia, i linguisti ma queste non si possono ritenere esaustive e non offrono la soluzione interpretativa corretta in tutte le circostanze[78].

Nel campo del diritto privato sono già stati attivati da tempo dei progetti di approfondimento ed analisi per la creazione di un linguaggio comune dei contratti, del commercio e delle transazioni, in particolare con il noto progetto *Unidroit*: queste riflessioni in materia di diritto penale e processuale penale sono ancora poche e timide.

Il Trattato di Lisbona ha imposto una vigorosa accelerata agli studi e al ricorso alla lingua anglosassone come lingua franca, anche per il rito penale e per l'armonizzazione di esso nello spazio comune europeo[79].

Anche il diritto penale ed il diritto processuale penale non vivono più delle sole norme interne agli ordinamenti giuridici nazionali, ma devono misurarsi con una pluralità di fonti comunitarie a cui devono uniformarsi.

Già l'attuazione di queste normative sovranazionali, l'adattamento rispetto alle interpretazioni giurisprudenziali offerte dai giudici comunitari, il coinvolgimento di più Stati in procedure di cooperazioni e in procedimenti penali, richiedono una maggiore attenzione nella prospettiva di una ricerca linguistica idonea a garantire la comprensione dei fatti e degli atti ai soggetti interessati.

---

[76] Secondo quanto riferito da Arianna Grasso, linguista, in occasione del già menzionato convegno svolto a Como il 14 luglio 2011, è in uscita un nuovo dizionario di inglese giuridico che, rispetto al precedente, è arricchito da molti più lemmi rispondenti al moderno linguaggio giuridico dell'UE. Questo nuovo strumento per l'interpretazione in lingua inglese è munito di definizioni e di esempi di frasi e di situazioni in cui una determinata parola, un concetto o un istituto sono applicati, per aiutare a raggiungere una traduzione più precisa e di qualità.

[77] Questa banca dati è liberamente consultabile in rete, al sito http://iate.europa.eu/iatediff/switchLang.do?success=mainPage&lang=it.

[78] Così Arianna Grasso, linguista esperta di inglese giuridico, nell'intervento tenuto al menzionato convegno comasco del 14 luglio 2011.

[79] Così Francesca Ruggieri nell'intervento svolto presso l'Accademia della Crusca a Firenze in data 1 ottobre 2010.

Nel più ampio contesto della garanzia dei diritti procedurali e dei diritti fondamentali, il diritto alla traduzione degli atti, alla presenza di un interprete quando non si comprende la lingua utilizzata acquista un ruolo centrale per la tutela dell'equo processo e del diritto di difesa di ogni individuo.

La qualità della traduzione e dell'interpretazione è essenziale affinché si realizzi una concreta attuazione di tutti quei diritti fondamentali che, direttamente o indirettamente, sono connessi al fenomeno del linguaggio.

Se esiste un termine corrispondente, il linguista si può limitare a un'operazione di traduzione e quindi di trasposizione dell'idioma dall'una all'altra lingua, ma se questo non è realizzabile, si renderà necessaria una perifrasi in grado di trasmettere il significato autentico[80].

Il mutamento originato dal nuovo sistema processuale penale, marcatamente influenzato dal diritto comunitario, coinvolge tutti i formanti propri degli studi comparatistica, generando anche una stretta compenetrazione tra diritto e linguaggio.

L'incrementato interesse verso la lingua è sottolineato anche nei testi delle norme comunitarie, con particolare riferimento alla disciplina degli strumenti e delle procedure di cooperazione quali il mandato di arresto europeo e il mandato europeo di ricerca della prova[81].

La conoscenza delle lingue e dei linguaggi giuridici, almeno quelli principali, è innanzitutto uno strumento volto a garantire all'indagato o imputato alloglotta il controllo del giudice sull'effettivo adempimento dell'obbligo di traduzione degli atti[82].

La Convenzione Europea dei Diritti dell'Uomo, all'art. 6, garantisce a chiare lettere il diritto dell'indagato/imputato ad un interprete per comprendere gli atti e le accuse a lui mosse.

La tutela di questo diritto ha subito una forte accelerazione a seguito dell'entrata in vigore della Direttiva sull'interpretazione e la traduzione, a cui gli Stati membri sono obbligati a dare attuazione entro il 2013 ma che prevede già degli effetti anticipati.

Il 20 ottobre 2010, il Parlamento europeo e il Consiglio hanno adottato la Direttiva 2010/64 riguarda proprio i procedimenti penali.

La Direttiva, in concreta applicazione del Trattato di Lisbona, segna un passo importante nel quadro del rafforzamento dei diritti procedurali dei sospettati e degli accusati. Essa si applica ai procedimenti penali ed alle procedure di esecuzione del Mandato di arresto europeo[83].

---

[80] Cfr *Ibidem*.
[81] Cfr *Infra* capitolo Secondo, Sezione III.
[82] Così Filippo Spiezia in occasione dell'intervento tenuto al convegno di Como del 14 luglio 2011, già più volte menzionato.
[83] Cfr art. 1.

Il diritto all'interpretazione e alla traduzione si snoda temporalmente dal momento in cui la persona è resa edotta dalle autorità competenti, mediante una notificazione o con altri mezzi di informazione, che è sospettata o accusata di aver commesso un reato, fino alla conclusione del procedimento penale[84].

L'accusato o sospettato può beneficiare di una interpretazione gratuita ogni qualvolta non comprende la lingua in uso durante un'udienza o un qualsiasi contraddittorio con le autorità, questo per salvaguardare il diritto all'equo processo di cui all'art. 6 CEDU[85].

Il diritto alla traduzione è previsto in una disposizione della Direttiva dai confini nebulosi, caratterizzata dall'utilizzo di termini e locuzioni generiche. Questo diritto, infatti, prevede la traduzione in forma scritta (o anche oralmente nei soli casi di necessità e urgenza) di tutti quei documenti che sono essenziali per l'accusato al fine di esercitare compiutamente il proprio diritto di difesa e il proprio diritto ad un equo processo. Non è fornito alcun catalogo, almeno generale ed esemplificativo, di quelli che debbono considerarsi come "documenti essenziali".

Questo quadro di riferimento, di conseguenza, richiede che vi sia un periodo di tempo sufficiente ed adeguato per procedere ad una traduzione e allo studio dell'atto così tradotto[86].

Il diritto all'interpretazione e alla traduzione si possono dire realmente garantiti soltanto se la traduzione e l'interpretazione rispettano un certo s*tandard* qualitativo. Per raggiungere questo obiettivo, la Direttiva prevede l'istituzione di un registro di traduttore e interpreti indipendenti, che possiedono una comprovata qualifica e professionalità[87].

La Direttiva in analisi segna un importante balzo in avanti verso la previsione di diritti procedurali di alto livello nei procedimenti penali degli Stati membri, oltre a rappresentare un esempio emblematico di attuazione dei dettati del Trattato di Lisbona[88].

La Direttiva non definisce la locuzione "procedimento penale" ma è comprensibile che per individuarne i confini è necessario considerare la giurisprudenza della Corte EDU, con particolare riferimento all'interpretazione dell'art. 6 CEDU.

[84] Cfr art. 1 comma 2.

Questo articolo è stato più volte riformulato durante i lavori preparatori, a causa di plurime eccezioni di incompatibilità con l'art. 6 CEDU sollevate da alcuni Stati membri.

[85] Cfr art. 2.

Anche questa disposizione della Direttiva è stata oggetto di plurime rivisitazioni, anche al fine di meglio bilanciare il diritto dell'indagato/imputato a comprendere quanto gli accade con una valutazione attenta dell'impatto economico da supportare da parte dello Stato per un interprete.

[86] Cfr art. 3.

[87] Cfr art. 5.

[88] Per un approfondimento sui lavori preparatori della Direttiva 2010/64/EU si invita alla lettura di S. CRAS – L. DE MATTEIS *The Directive on the right to interpretation and translation in criminal proceedings* in *Eucrim,* 4, 2010, pagg. 153-163.

4. *Crimini transnazionali, cybercrimes e crimini internazionali: definizioni e dati statistici*

Il nuovo sistema economico-sociale globalizzato e lo sviluppo delle nuove tecnologie, pongono continue sfide alla giustizia penale ed agli operatori del diritto criminale.

È ormai superato l'approccio alla criminalità limitato entro i confini nazionali, in considerazione dell'incremento di reati che coinvolgono almeno due o più Stati dell'Unione europea ed extra-UE, nonché in uno spazio virtuale a cui è estranea ogni forma di demarcazione territoriale [89].

Si pensi alle lotte comuni contro i traffici di droga e la tratta di esseri umani, la criminalità organizzata e, soprattutto, il terrorismo.

Le categorie dei reati internazionali, dei reati transnazionali e dei crimini informatici costituiscono un settore particolarmente complesso anche in ragione della necessità di un costante adeguamento della disciplina alle caratteristiche di una realtà in continua evoluzione, specie con riferimento al settore informatico.

Il carattere di transnazionalità e di internazionalità del reato si sovrappongono, molto spesso, a livello concettuale, come si può rilevare dal significato stesso dei termini.

La Convenzione delle Nazioni Unite contro il crimine organizzato transnazionale precisa che: "*un reato è di natura transnazionale se: a) è commesso in più di uno Stato; b) è commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avviene in un altro Stato; c) è commesso in uno Stato, ma in esso è implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; o d) è commesso in uno Stato ma ha effetti sostanziali in un altro Stato*" [90].

Il caso del terrorismo internazionale, che campeggia nell'elenco delle categorie di reati di natura internazionale per lo sviluppo che lo ha caratterizzato negli ultimo anni, in particolare a partire dai noti eventi dell'11 settembre 2001 negli USA è eloquente.

Secondo un'altra prospettiva, il semplice reato di terrorismo rappresenta una delle forme di manifestazione della criminalità transnazionale, nell'ipotesi in cui una sfera di azione frammentata non esaurisca la propria potenzialità offensiva nel territorio di un unico Stato [91].

---

[89] Così J. A. E. VERVAELE nel Rapporto Generale scritto in occasione del XVIII International Conference AIDP, tenutosi ad Istanbul, 20-27 settembre 2009.

[90] Cfr Art. 3 Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, consultabile in *internet* al sito: http://www.admin.ch/ch/i/ff/2005/6037.pdf (consultato in data 20 aprile 2011).

[91] Così A. PECCIOLI *Il terrorismo quale settore chiave per l'armonizzazione del diritto penale* in *Diritto Penale e Processo*, 6, 2007, pag. 801.

È fuor di dubbio, dunque, il carattere di transnazionalità del reato (o meglio dei reati) di terrorismo[92], eppure questo non ha permesso l'immediato superamento delle difficoltà interpretative legate all'individuazione dei casi di terrorismo internazionale dai casi di terrorismo semplice.

Si pensi ai molteplici orientamenti divergenti sorti in Italia in relazione al concetto di "*attività terroristica*" e alla definizione delle condotte con finalità di terrorismo, nonché ai problemi ermeneutici legati all'individuazioni dei confini degli atti con finalità terroristica "*anche internazionale*". L'indeterminatezza normativa ha generato un dibattito a livello dogmatico in seno all'ordinamento giuridico italiano, specie tra gli interpreti del diritto.

I problemi di teorizzazione dei limiti di applicazione della normativa applicabile ai reati di terrorismo e ai nuovi reati di terrorismo internazionale, attraverso la necessaria definizione delle due locuzioni, non ha interessato solo l'Italia ma l'intero sistema giuridico internazionale.

A tutt'oggi non si può ritenere superata la questione, sebbene siano state fornite delle definizioni ormai comunemente accettate e utilizzate dagli operatori del diritto.

Dalla lettura delle fonti internazionali e delle definizioni in uso si osserva che la distinzione tra terrorismo internazionale e terrorismo semplice si sostanzia principalmente sul fatto che quest'ultimo non sempre e non per forza produce effetti in più Stati o produce eventi lesivi in uno Stato diverso da quello in cui il gruppo è radicato, si organizza e prepara le proprie attività criminose[93].

La distinzione chiave è dunque tra terrorismo interno e terrorismo internazionale, quest'ultimo qualificato come un reato che presenta degli elementi di estraneità rispetto ad uno Stato ed ha pertanto rilevanza internazionale o, addirittura, ha nel suo stesso scopo quello di sovvertire l'ordine internazionale, mettendo in pericolo le relazioni internazionali e la pace[94].

Si ricordano le conclusioni della Conferenza di Siracusa del 1973 ove è contenuta la seguente definizione di terrorismo internazionale: "*Individual or collective coercive conduct employing strategie of terror and violence which contain an international element or are directed against an interest nationally protected target*

Per un'analisi della categoria della criminalità transnazionale si veda V. MILITELLO – L. PAOLI – J. ARNOLD (a cura di) *Il crimine organizzato come fenomeno transnazionale,* Giuffré, 2000.

[92] L'uso della locuzione al plurale è dovuta dal fatto che le modalità di esplicitazione e di configurazione di un'azione terroristica sono molteplici e possono assumere aspetti differenti tra loro.

[93] Sul punto si rinvia alla lettura di L. QUADRELLA *Il nuovo terrorismo internazionale come crimine contro l'umanità,* Editoriale Scientifica, 2006; G. FLORA *Profili penali del terrorismo internazionale: tra delirio di onnipotenza e sindrome di auto castrazione* in *Rivista Italiana di Diritto e Procedura penale,* 2008, pagg. 63-75.

[94] Cfr L. QUADRELLA *op.cit.,* pag. 10.

and whose aim is to produce a power-oriented act. Such conduct contains an International element when: 1) the perpetrator and victim are citizens of different states or 2) the conduct is performed in whole or in part in more than one state"[95].

Da questo breve *excursus,* emerge chiaramente che è l'elemento di estraneità rispetto allo Stato a caratterizzare il reato internazionale e lo stesso vale a dirsi per i crimini transnazionali.

A partire dalla nascita dell'Unione europea, la tendenza spesso è quella di utilizzare l'aggettivo "transnazionale" in particolare per quei reati che coinvolgono più Stati membri dell'Unione, per riservare l'aggettivo "internazionale" a quelle forme criminalità che allargano i propri confini oltre quelli comunitari, per interessare la Comunità Internazionale.

Anche il crimine informatico, in alcune sue forme di manifestazione, può assumere il carattere di transnazionalità e internazionalità, così come, invece, può svolgersi e produrre l'evento lesivo solo all'interno del territorio di uno Stato, sebbene questo accada molto raramente a causa dell'uso della rete *internet* globalizzata.

Definire precisamente ed in maniera esauriente il crimine informatico è un esercizio teorico molto complicato, in ragione dell'eterogeneità delle modalità di azione esercitabili e degli strumenti informatici utilizzati. Per questo motivo e per la continua evoluzione tecnologica, ogni tentativo di racchiudere in una definizione normativa il concetto di *cybercrime* risulta sempre inadeguato e immediatamente obsoleto.

Il reato informatico colpisce un nuovo bene economico che può essere identificato nel bene informatico, anche se si tratta di un bene immateriale, come lo sono del resto anche i prodotti intellettuali, che può essere venduto o ceduto in uso, rubato, danneggiato, manomesso o distrutto[96].

Nel 1989 il Comitato degli esperti sulla criminalità informatica del Consiglio d'Europa ha stilato un elenco di reati informatici, distinguendo due fattispecie: la prima comprende quei reati per i quali appare necessario e urgente provvedere ad adeguate sanzioni, trattandosi di forme di criminalità riconosciute e diffuse; la seconda concerne quei reati la cui previsione e repressione va rimessa all'iniziativa legislativa dei singoli Stati.

Compongono la prima specie la frode informatica, il falso informatico, il danneggiamento dei dati dei programmi, il sabotaggio informatico, l'accesso non autorizzato in un sistema informatico, l'interruzione non autorizzata di comunicazioni telematiche, la riproduzione non autorizzata di una topografia di semiconduttore. Nella seconda specie, invece, trovano spazio l'alterazione dei dati dei programmi informatici, lo spionaggio informatico, l'utilizzazione

[95] Cfr M. C. BASSIOUNI *International Terrorism and Political Crimes,* Springfield, 1975.
[96] Cfr V. FROSINI *La criminalità informatica* in *Diritto dell'Informazione e dell'Informatica,* 1997, pag. 488.

non autorizzata di un elaboratore, di un sistema o di una rete telematica, l'utilizzazione non autorizzata di un programma informatico protetto [97].

Secondo le definizioni comunemente ritenute più esaurienti, i crimini informatici sono reati commessi con l'ausilio del computer; i *computer crimes* sono illeciti che rientrano nell'ambito dei reati economici perché, interessando principalmente gli interessi individuali, danneggiano anche gli interessi economici della collettività; il crimine informatico rappresenta qualsiasi atto o fatto contrario alle norme penali, nel quale il computer è stato usato come oggetto del fatto, come strumento o come simbolo; il *computer crime* è ogni condotta antigiuridica disonesta o non autorizzata, concernente l'elaborazione automatica e/o la trasmissione dei dati; il crimine informatico è un crimine nel quale un sistema di elaborazione o una sua parte è oggetto o soggetto di reato[98].

L'ultima definizione riportata sembra meglio individuare le diverse forme di esplicitazione della criminalità informatica ove, appunto, lo strumento tecnologico è, alternativamente, il mezzo attraverso il quale si compie in tutto o in parte il reato, ovvero è l'oggetto su cui ricadono gli effetti lesivi del reato[99].

Nell'ambito del contrasto alla criminalità informatica, attesa l'odierna dimensione tecnica globale del fenomeno, i documenti emanati a livello internazionale, fra cui il testo fondamentale rappresentato, ad oggi, dalla Convenzione del Consiglio d'Europa sul *cybercrime,*aperta alla firma a Budapest il 23 novembre 2001. Il testo del Trattato presenta una serie di disposizioni di diritto penale sostanziale che riguardano una lisa di fattispecie criminali, categorizzate come crimini informatici, che le Parti contraenti si impegnano a sanzionare. Le condotte illecite indicate sono: l'accesso illegale a tutto o a parte di un sistema informatico, con eventuale violazione di misure di sicurezza e al fine di ottenere dati informatici o con altra finalità delittuosa [100]; l'intercettazione illegale di dati informatici, in caso di trasmissioni non pubbliche, con destinazione, provenienza o all'interno di un sistema informatico, comprese le emissioni elettromagnetiche provenienti da un

---

[97] *Ibidem,* pag. 489.

[98] Cfr R. BORRUSO – G. BUONOMO – G. CORASANITI – G. D'AIETTI *Profili penali dell'informatica,* Giuffré, 1994.

[99] Anche in relazione al tema del crimine informatico non è questa la sede per trattare dei problemi dogmatici, di diritto penale sostanziale, legati al *nomen iuris* e all'individuazione dei confini di una categoria concettuale criminale.
Per un approfondimento si rinvia, *ex multis,* a L. PICOTTI (a cura di) *Il diritto penale dell'informatica nell'epoca di internet,* Cedam, 2004; V. S. DESTITO – G. DEZZANI – C. SANTORIELLO *Il diritto penale delle nuove tecnologie,* Cedam, 2007; M. CHIAVARIO (a cura di) *Nuove tecnologie e processo penale,* Giappichelli, 2003; L. CUOMO – R. RAZZANTE *La disciplina dei reati informatici,* Giappichelli, 2007.

[100] Cfr art. 2 Convenzione di Budapest.

sistema informatico[101]; l'attentato all'integrità dei dati o del sistema[102]; l'abuso di dispostivi, cioè la produzione, vendita, diffusione, messa a disposizione o possesso di dispostivi che permettono l'accesso a un sistema informatico o che comunque agevolano la commissione dei menzionati reati[103]; la falsità informatica con o senza finalità fraudolenta[104]; la frode informatica[105]; la produzione, offerta, messa a disposizione, diffusione, trasmissione, procacciamento o possesso di materiale pedopornografico per il tramite di un sistema informatico[106]; gli illeciti legati alla proprietà intellettuale, per il cui catalogo è fatto semplice rinvio ad altre convenzioni internazionali[107].

Le forme di criminalità legate all'*information technology* si sono sviluppate a tal punto da richiedere degli interventi normativi chiarificatori e di regolamentazione e lo sviluppo di politiche comunitarie di cooperazione per la lotta comune a questi reati.

Si pensi, appunto, alla menzionata Convenzione di Budapest e poi alla proposta di Decisione quadro COM (2002) 173 definitivo relativa agli attacchi contro i sistemi di informazione, la Comunicazione della Commissione al Parlamento europeo, al Consiglio e al Comitato delle Regioni, COM (2007) 267 definitivo, verso una politica generale di lotta contro la cibercriminalità.

Secondo l'FBI, meno del 15% dei crimini informatici viene scoperto e meno del 10% di questi crimini viene denunciato[108].

Già dalla fine degli Anni '70 si sono sviluppate le prime embrionali forme di *cybercrimes* e, nel 1999, in base ad un sondaggio condotto dal *Computer Emergency Response Team* (CERT), l'Agenzia parastatale statunitense che si occupa degli incidenti nella rete, ha registrato 20241 intrusioni illegali sul *network,* quasi il doppio dell'anno precedente[109].

Altre statistiche hanno rilevato che le perdite economiche connesse a furti elettronici di carte di credito, sempre nel 1999, hanno superato i 2 miliardi di dollari[110].

Secondo il rapporto del 2007 dell'*Internet Crime Complaint Center* americano, le denunce di reati informatici sono calate rispetto agli anni precedenti. Dei crimini denunciati, il 36% sono frodi d'asta con la percentuale più alta; percentuale più bassa, solo il 3%, per i furti d'identità.

---

[101] Cfr art. 3 Convenzione di Budapest.
[102] Cfr artt. 4 e 5 Convenzione di Budapest.
[103] Cfr art. 6 Convenzione di Budapest.
[104] Cfr art. 7 Convenzione di Budapest.
[105] Cfr art. 8 Convenzione di Budapest.
[106] Cfr art. 9 Convenzione di Budapest.
[107] Cfr art. 10 Convenzione di Budapest.
[108] Si veda, a tal fine, il sito internet www.fbi.gov.
[109] Cfr N. GARAPPA *Internet e diritto penale* in *www.diritto.it.*
[110] *Ibidem.*

Il Consiglio d'Europa calcola duecento milioni di danni annui conseguenti ad illeciti informatici[111].

Il rapporto del 2008 di Symantec, azienda interessata alla materia della sicurezza informatica, sottolinea l'individuazione di 12.885 vulnerabilità dei sistemi informatici, di cui solo 394 sono state risolte con solerzia[112].

Secondo gli ultimi dati, riferiti all'anno 2008, il record di crimini informatici commessi è detenuto dal Giappone con un incremento del 15,5% rispetto al 2007 e un aumento del 300% rispetto al 2004 dei casi di furto di credenziali[113].

5. *La cooperazione giudiziaria e di polizia nello spazio giudiziario europeo*

Lo sviluppo della globalizzazione dei rapporti sociali ed economici, la liberalizzazione delle regole sugli spostamenti di persone e di beni, la diffusione di strumenti tecnologici e informatici idonei ad agevolare le relazioni umane al di là dei confini dello Stato, sono risultati fattori che hanno da un lato agevolato uno *standard* elevato di benessere sociale ma, d'altro lato, hanno agevolato gli autori di reato nella commissione di atti illeciti di carattere transnazionale e internazionale[114].

In questo mutato scenario si è palesata sempre più chiaramente la necessità di adottare un approccio globale di prevenzione e repressione delle fattispecie criminose, richiedendo una revisione continua dei principi tradizionali, risultati ormai insufficienti[115].

Di fronte ad attacchi criminali su larga scala, l'intervento a livello nazionale è insufficiente, mentre è auspicabile un'azione a livello europeo, in maniera comune ed armonizzata.

La mancanza o il sottoutilizzo di strutture immediate per la cooperazione operativa transnazionale rimane un punto debole dello spazio europeo di libertà, sicurezza e giustizia[116].

Ai sensi dell'art. 31, paragrafo 2, del Trattato dell'Unione europea, quale modificato dal Trattato di Nizza, il Consiglio europeo incoraggia la cooperazione[117].

---

[111] Si veda il sito internet del Consiglio d'Europa: www.coe.int.
[112] Si veda il sito internet di Symantec: www.symantec.com.
[113] I dati riferiti al Giappone sono consultabili in internet alla pagina: www.primaonline.it/ 2009/02/26/69125/internet-giappone-boom-crimini-informatici.htm (consultato in data 17 giugno 2009).
[114] Cfr E. APRILE *Diritto processuale penale europeo e internazionale,* Cedam, 2007, pagg. 1-3.
[115] Così G. ZICCARDI CAPALDO *Terrorismo internazionale e garanzie collettive,* Giuffré, 1990.
[116] Cfr Comunicazione della Commissione al Parlamento europeo, al Consiglio e al Comitato delle Regioni, COM (2007) 267 definitivo, verso una politica generale di lotta contro la cibercriminalità.

A seguito degli attacchi terroristici dell'11 marzo 2004 in Spagna, il Consiglio europeo del 25 marzo 2004 ha sollecitato lo viluppo dei poteri di Eurojust e di Europol, al fine di promuovere la cooperazione, in particolare nella lotta contro il terrorismo[118].

I cittadini dell'Unione europeo esigono uno spazio UE prospero e pacifico, che tuteli i diritti e garantisca l'incolumità.

La sfida per la prevenzione e la repressione della criminalità, specie di quella transnazionale, non può prescindere dallo sviluppo della reciproca fiducia tra gli Stati e dall'incremento delle relazioni di cooperazione, sfruttando al meglio le procedure messe a disposizione delle autorità di polizia e giudiziarie, con l'apporto degli organi comunitari quali Europol, Eurojust e Olaf[119].

5.1 Strumenti convenzionali: dalla Convenzione europea sull'assistenza giudiziaria del 1959 alla Convenzione di Bruxelles del 29 maggio 2000

I programmi di cooperazione e di integrazione giudiziaria in materia penale hanno un carattere del tutto peculiare.

La prima volta in cui, nel quadro europeo, si è fatto riferimento alla cooperazione in materia penale è stato in concomitanza con l'istituzione del Gruppo di Trevi, un foro intergovernativo finalizzato ad aumentare il livello di cooperazione interstatale nella lotta al terrorismo, nel 1975 [120].

L'allora Presidente della Repubblica francese, Valery Giscard D'Estaing, nel 1977, nella sua celebre dichiarazione al Consiglio europeo di Bruxelles, ha evidenziato la necessità di dare vita ad uno spazio giuridico europeo di giustizia e sicurezza, agevolando la cooperazione tra gli Stati membri in materia penale.

Fino al 1992 le relazione tra Stati membri e Unione europea erano disciplinate in maniera sostanzialmente analoga ai rapporti con Paesi Terzi.

Un passo in avanti è stato compiuto già con il Trattato di Maastricht del 1992 (entrato in vigore l'1 novembre 1993), mediante l'inserimento della

---

[117] Cfr Relazione della Commissione sul recepimento, dal punto di vista legislativo, della decisione del Consiglio del 28 febbraio 2002 che istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità.

[118] Cfr Documento del Consiglio europeo 7906/04.

[119] Così la Comunicazione della Commissione al Parlamento europeo e al Consiglio, COM (2009) 262 definitivo, per uno spazio di libertà, sicurezza e giustizia a servizio del cittadino.

[120] Così R. ADAM *La cooperazione in materia di giustizia e affari interni tra comunitarizzazione e metodo intergovernativo* in *Diritto dell'Unione Europea,* 1998, pagg. 491-509.

cooperazione nel settore della Giustizia e Affari Interni tra gli obiettivi comuni dell'Unione.

È solo con il Trattato di Amsterdam del 1977 che il III Pilastro dell'Unione, ridenominato "*cooperazione di polizia e giudiziaria in materia penale*", viene dotato di un'appropriata base giuridica per consentire l'adozione di iniziative comuni, attraverso una collaborazione più stretta fra forze di polizia, autorità doganali e giudiziarie e un avvicinamento delle norme di diritto penale tra gli Stati membri, in modo da "*fornire ai cittadini un livello elevato di sicurezza in uno spazio di libertà e giustizia*"[121].

In sostanza, il Trattato in parola affianca alla cooperazione intergovernativa quella giudiziaria tra gli Stati membri in materia penale[122].

Anche sul piano delle fonti adottabili dalle istituzioni comunitarie nell'ambito del III Pilastro è stata introdotta un'articolata gamma, tra cui spiccano le decisioni quadro.

Altra novità rilevante è rappresentata dalla competenza, concessa alla Corte di Giustizia, di poter esercitare la propria attività d'interpretazione anche nel campo della cooperazione in materia penale[123].

Con le modifiche del 1997 talune delle materie originariamente di competenza del settore Giustizia e Affari Interni (GAI) sono state trasferite dal Terzo al Primo Pilastro. Ciò è accaduto, per esempio, per la cooperazione nell'ambito della mobilità delle persone e del trattamento delle persone.

Vi sono, poi, delle materie che necessariamente le competenze sono sia del Terzo sia del Primo Pilastro, trattandosi di argomenti di natura prettamente comunitaria ma che possono avere dei riflessi anche sulla cooperazione di polizia e giudiziaria in materia penale[124].

L'azione comune 98/427/GAI del Consiglio dell'Unione europea ha stabilito che gli Stati membri depositassero, presso il Segretariato generale, una dichiarazione sulla buona prassi nell'assistenza giudiziaria in materia penale, indicando le modalità a cui ciascun Paese si obbligava a conformarsi, secondo la buona prassi ed in osservanza dei principi di celerità ed efficienza[125].

In questo contesto sono divenute un fondamentale punto di riferimento la Conclusioni del Consiglio europeo di Tampere del 15-16 ottobre 1999,

---

[121] Cfr art. 2 TUE.

[122] Si vedano anche gli artt. 3 e 29 TUE.

[123] Per un'analisi sul punto si rinvia a M. FLETCHER *The European Court of Justice. Carving Itself an influential role in the EU's Third Pillar* in *www.unc.edu/euce/eusa 2007/papers/fletcher-m-08i.pdf* (consultato in data 30 luglio 2011).

[124] Così E. APRILE *op.cit.*, pag. 22.
Sul punto si veda anche SS. RIONDATO *Competenza penale della Comunità europea,* Cedam, 1996.

[125] Così E. CALVANESE – G. DE AMICIS *La Rete giudiziaria europea: natura, problemi e prospettive* in *Cassazione penale,* 2001, pagg. 706 ss.

all'esito del quale è stata ribadita la necessità di evitare che gli autori di reato potessero avvantaggiarsi delle differenze tra i sistemi giuridici degli Stati membri, stabilendo una serie di priorità dell'Unione europea [126].

Il 29 maggio 2000 il Consiglio dell'Unione europea ha adottato la Convenzione relativa all'assistenza giudiziaria in materia penale che, nei propositi, avrebbe dovuto superare, almeno parzialmente, le previsioni della Convenzione di assistenza giudiziaria in materia penale di Strasburgo del 1959.

Considerate le differenze tra i sistemi giuridici e giudiziari degli Stati membri e l'evidente necessità d'instaurare una cooperazione in materia penale, la Convenzione si è proposta lo scopo di facilitare l'assistenza giudiziaria tra gli Stati membri.

Le richieste di assistenza giudiziaria e tutti gli scambi di informazioni devono avvenire mediante la presentazione di istanze dirette tra le autorità degli Stati membri direttamente coinvolte. Eccezionalmente, e solo per le richieste di trasferimento temporaneo o transito di persone detenute e per le notifiche di informazioni relative alle condanne, è prescritto il transito della richiesta all'autorità centrale.

Per assicurare l'utilizzabilità della prova assunta in uno Stato diverso, la Convenzione stabilisce che l'autorità giudiziaria debba osservare "*le formalità e le procedure espressamente indicate dallo Stato membro richiedente*" [127].

Nell'Accordo sono contenute delle disposizioni riguardante la disciplina delle operazioni di intercettazione delle comunicazione [128]. A tal fine è previsto che l'autorità nazionale competente possa chiederne l'esecuzione all'autorità competente presso lo Stato richiesto per mezzo di un'istanza all'uopo compilata.

Il Consiglio europeo ha, in seguito, adottato un Protocollo aggiuntivo alla Convenzione al fine di agevolare l'assistenza giudiziaria in alcuni settori, quali la criminalità organizzata e la criminalità in materia finanziara [129].

Gli scopi individuati dal Consiglio di Tampere sono stati reiterati nel corso del Consiglio dell'Aja dell'8 marzo 2005, con l'approvazione del documento 2005/C/53/1 sul "*rafforzamento delle libertà, della sicurezza e della giustizia dell'Unione europea*".

Il punto di partenza di questo quadro dinamico di riferimento della cooperazione in materia penale, muove dalla Convenzione europea di

---

[126] Al riguardo, *ex plurimis,* J. A. E. VERVAELE *L'europeizzazione del diritto penale e la dimensione penale dell'integrazione europea* in *Rivista Trimestrale di diritto penale dell'economia,* 2005, pagg. 142 ss.

[127] Cfr art. 4 Convenzione sull'assistenza giudiziaria in materia penale.

[128] Cfr artt. 17-22 Convenzione sull'assistenza giudiziaria in materia penale.

[129] Per un approfondimento sulla Convenzione del 2000 si rinvia a E. ANODINA *Cooperazione-integrazione penale nell'Unione europea* in *Cassazione penale,* 2001, pagg. 2905 ss.

estradizione del 1957, firmata a Parigi il 13 dicembre 1957. Trattasi del primo strumento internazionale che pone una regolamentazione multilaterale dell'estradizione tra i Paesi dell' Europa, laddove, in precedenza, la materia era affidata soltanto ad accordi bilaterali. La Convenzione europea è ispirata ad una logica di collaborazione intergovernativa[130], attesa la rinuncia a stabilire un'unica procedura di estradizione e rimettendo, a tal punto, alla disciplina dei singoli Stati membri[131].

I due Protocolli aggiuntivi del 1975 e del 1978 hanno completato il sistema di garanzie previsto a tutela dell'estradando e aggiornano alcune aspetti relativi all'istituto. Il primo ha introdotto delle modifiche sia sul piano processuale ed in particolare sul *ne bis in idem*, sia sul piano del diritto sostanziale. Con il secondo protocollo si è inteso rafforzare la cooperazione penale nella lotta alla criminalità nel settore economico.

Il principale strumento di cooperazione giudiziaria in ambito europeo è rappresentato dalla Convenzione sull'assistenza giudiziaria in materia penale, firmata a Strasburgo il 20 aprile 1959.

Detta Convenzione è stata ratificata ed applicata da tutti i quarantasette Paesi membri del Consiglio d'Europa, nonché da Israele.

Gli Stati si sono accordati reciprocamente a fornire l'assistenza giudiziaria più ampia possibile in qualsiasi procedura relativa a reati la cui competenza è, al momento dell'assistenza, dell'autorità giudiziaria della parte richiedente[132].

Gli articoli 1, 3 e 4 hanno previsto pochi limiti alla natura e al numero di richieste di assistenza giudiziaria che possono essere proposte dalle autorità competenti degli Stati membri. Il *focus* della Convenzione riguarda l'ottenimento della prova nell'ambito di un procedimento penale. L'art. 1 ha escluso dall'operatività l'esecuzione delle decisioni di arresto e di condanna e i reati militari che non corrispondono a fattispecie di diritto comune. L'art. 2 ha previsto la possibilità di rifiuto d'assistenza nel caso in cui si proceda per reati politici, reati fiscali, ovvero se la Parte richiesta ritenga che l'esecuzione della domanda costituisca pericolo per la sovranità, la sicurezza, l'ordine pubblico o altri interessi essenziali per la nazione. Ai sensi dell'art. 3 può essere richiesto il compimento di atti istruttori o la comunicazione di confessioni, fascicoli o documenti. Tali atti e documenti saranno trasmessi in copia o fotocopia autentica, salvo che vi sia espressa richiesta di trasmissione degli originali.

---

[130] Il metodo intergovernativo attribuisce il potere decisionale ai Governi degli Stati di riferimento e non alle istituzioni comunitarie, perseguendo l'obiettivo di apprestare uno spazio di libertà, di sicurezza e di giustizia all'interno dell'Unione europea.

[131] L'art. 22 della Convenzione recita: "*Salvo disposizione contraria della presente Convenzione, la legge della Parte richiesta è la sola applicabile alla procedura di estradizione e a quella dell'arresto provvisorio*".

[132] Cfr art. 1 Convenzione del 1959.

L'art. 5 ha limitato l'applicazione di misure coercitive ai soli casi in cui è applicabile, tra Stato richiesto e richiedente, il principio di doppia incriminazione. Questo ha rappresentato un primo ostacolo alla cooperazione, assieme alla facoltà di rifiuto d'assistenza. Molti degli Stati che hanno adottato la Convenzione hanno previsto il rifiuto di collaborazione nel caso in cui si proceda per reati tributari[133].

L'Accordo ha previsto che le domande di cooperazione, così come quelle di trasferimento temporaneo, dovessero essere trasmesse dal Ministro della Giustizia della Parte richiedente al Ministro della Giustizia della Parte richiesta e ritrasmesse con le medesime modalità. Solo in casi di urgenza è stat legittimata la trasmissione diretta tra le autorità giudiziarie degli Stati coinvolti, per il tramite dell'Organizzazione Internazionale di Polizia criminale (Interpol).

Le domande e gli atti allegati non dovevano essere tradotti nella lingua del Paese rogato, salvo che quest'ultimo abbia dichiarato di riservarsi la facoltà di esigere che questi siano accompagnati da una traduzione in una propria lingua ovvero in una delle lingue del Consiglio d'Europa (francese o inglese)[134].

La prova della consegna veniva fornita per mezzo di una ricevuta datata e firmata dal destinatario o con dichiarazione della Parte richiesta di contestazione del fatto, della forma e della data di consegna.

A seguito dello sviluppo delle nuove forme di criminalità e della necessità di accelerare il processo di integrazione europeo, la disciplina della Convenzione del 1957 e del 1959 si sono rivelate inadeguate. Solo a far tempo dal già menzionato Trattato di Maastricht del 1992 si è realizzata una vera svolta in materia di cooperazione.

La collaborazione tra le autorità degli Stati si è caratterizzata, come tradizionalmente, per il rapporto di tipo orizzontale tra entità territorialmente sovrane. Il principale limite allo sviluppo piena della materia è rappresentato, da sempre, dalla gelosia degli Stati rispetto all'esercizio della propria sovranità in materia penale[135].

L'insufficienza del tradizionale sistema rogatoriale si è manifestato da tempo, avvertendosi l'urgenza di dotarsi di mezzi di cooperazione più rapidi e più incisivi.

Già nel 1996-1997 sono iniziate le prime consultazioni e discussioni per l'elaborazione di quella che poi è divenuta Convenzione europea di mutua assistenza in materia penale nel 2000. La Convenzione di Bruxelles del 29

---

[133] Cfr J. A. E. VERVAELE *European Evidence Warrant,* Intersentia, 2005, pagg. 20-21.
[134] Cfr C. M. PAOLUCCI *op.cit.,* pagg. 29-33.
[135] Così N. PARISI *Su taluni limiti nell'attività di ricerca e acquisizione della prova penale nei reati informatici* in *Studi in onore di Mario Pisani,* La Tribuna, 2010, pagg. 443-445.

maggio 2000 contiene un numero considerevole di disposizioni utili ed addizionali, rispetto alle misure esistenti per la cooperazione giudiziaria previste dalla Convenzione del 1959 e dalla Convenzione Schengen del 1990[136].

La Convenzione del 2000 ha previsto, per esempio, le disposizioni sulle intercettazioni di telecomunicazioni e sulle modalità di organizzazione delle Squadre Investigative Comuni.

L'azione per la creazione di uno spazio comune europeo si è mossa anche lungo la direttrice della creazione di organi comunitari con funzioni in materia di cooperazione, in particolare Europol per lo sviluppo dei rapporti tra le forze politiche, le autorità doganali e le altre autorità competenti degli Stati membri e Eurojust per una più stretta collaborazione tra le autorità giudiziarie e le altre autorità competenti degli Stati membri[137].

Dopo il fallimento del Trattato per una nuova Costituzione europea, le più importanti innovazioni sono scaturite dall'entrata in vigore del Trattato di Lisbona, il quale ha ridisegnato l'architettura delle istituzioni europee, modificando i procedimenti normativi ed i profili istituzionali, con rilevanti conseguenza anche in tema di cooperazione giudiziaria e di polizia.

L'anno 2008 si è caratterizzato per un'elevata produzione normativa da parte degli organi dell'Unione, dalla Decisione su Eurojust e la Decisione 2008/976/GAI del 16 dicembre 2008 relativa alla Rete giudiziaria europea, alla nuova Decisione sostitutiva della Convenzione Europol del 1995.

Questo processo normativo ha rappresentato un chiaro segnale della volontà di "europeizzazione" dei sistemi penali nazionali, anche e soprattutto mediante l'armonizzazione delle discipline nazionali di diritto penale sostanziale.

Con particolare riguardo ad alcune materie delicate, quali il diritto di stabilimento, la tutela dei mercati finanziari e la tutela dell'ambiente, è stata sentita la necessità, a livello comunitario, di una omogeneizzazione delle normative penali poiché la mera cooperazione penale si è rivelata inadeguata per combattere le moderne forme di criminalità.

Il settore della cooperazione giudiziaria è quello che ha registrato le novità più importanti, a fronte delle accresciute istanze di contrasto al crimine organizzato transnazionale. In materia, si pensi al potenziamento delle funzioni di coordinamento di Eurojust ed Europol, nonché lo sviluppo del principio del reciproco riconoscimento delle decisioni giudiziarie, come già

[136] Nel novembre del 2001 la Convenzione di Bruxelles è stata dotata di un Protocollo addizionale.
[137] Così E. APRILE – F. SPIEZIA *op.cit.*, pagg. 2-5.
Per un approfondimento si rinvia a M. CHIAVARIO *Cooperazione giudiziaria e di polizia in materia penale a livello europeo* in *Rivista italiana di diritto e procedura penale*, 2005, pagg. 957 ss.

auspicato nelle conclusioni formulate dal Consiglio europeo di Tampere il 15 e 16 ottobre 1999[138].

La normativa sovranazionale si sta continuamente sviluppando all'interno di una cornice più o meno definita di principi generali che consentono di poter identificare un vero e proprio sistema.

Molte Decisioni quadro del Consiglio hanno perseguito l'obiettivo del rafforzamento delle crescenti esigenze di cooperazione per la prevenzione ed il contrasto alla criminalità sovranazionale.

Tuttavia la stessa Corte di Giustizia delle Comunità europee, nella sentenza del caso C-303/2005 del maggio 2007, ha sottolineato l'importanza di perseguire l'armonizzazione delle norme procedurali nazionali, come strumento per la facilitazione delle attività di cooperazione[139].

In un quadro frammentato ed in lenta, ma costante, evoluzione, l'entrata in vigore del Trattato di Lisbona ha costituito un'unità, principalmente mediante la soppressione della costruzione a pilastri dell'Unione europeo. La competenza in materia di cooperazione giudiziaria e di polizia diviene così di competenza concorrente dell'Unione con gli Stati membri[140].

I principali riferimenti normativi si sostanziano nell'art. 31 e nell'art. 69 del Trattato di Lisbona. La prima disposizione prevede non solo la facilitazione e l'accelerazione della cooperazione tra i ministeri competenti e le autorità giudiziarie o autorità omologhe degli Stati membri e la facilitazione dell'estradizione, ma anche la garanzia delle compatibilità normative applicabili negli Stati, nella misura necessaria per agevolare la cooperazione. La seconda disposizione, confermando la rilevanza dei processi di armonizzazione in materia procedurale, prevede che il Consiglio europeo possa stabilire norme procedurali minime che tengano conto delle differenti tradizioni giuridiche degli Stati membri, nella misura necessaria ad agevolare l'applicazione del principio del mutuo riconoscimento.

Questo processo, però, registra il perdurare di alcune problematiche legate all'assenza di alcuni passaggi ed alcuni elementi essenziali per la piena realizzazione di un sistema di cooperazione completo ed efficace.

Tra le *empasse* di natura politica si registrano proprio avuto riguardo alla difficoltà si individuazione ed approvazione di norme minime comuni, capaci di offrire un livello equivalente di protezione a sospettati ed accusati in tutto il territorio dell'Unione europea.

---

[138] Cfr E. APRILE – F. SPIEZIA *op.cit.*, pagg. 7-11.
[139] Cfr *Ibidem*, pag. 18.
[140] Cfr B. NASCIMBENE *Cooperazione giudiziaria penale: diritto vigente e orientamenti futuri nel quadro della Costituzione europea* in *Diritto penale e processo,* 10, 2004, pagg. 1295- 1306.

Solo il rafforzamento della reciproca fiducia tra gli Stati può portare alla realizzazione di un assetto di europeizzazione del sistema penale in ambito comunitario.

La tendenza a prevedere in ambito europeo forme sempre più sviluppate di cooperazione, anche mediante la valorizzazione del ruolo e delle funzioni degli organi comunitari, abbraccia le esigenze di tutela di interessi collettivi, con il rischio di limitare le garanzie processuali e la tutela dei diritti della persona indagata o imputata di un reato.

D'altra parte, anche storicamente, la cooperazione internazionale è sempre dipesa da sottili trame di rapporti politici tra Stati, rispetto alle quali la posizione del singolo è stata subordinata rispetto agli interessi governativi[141].

L'Unione europea, dal canto suo, pur non essendo ancora riuscita a raggiungere un livello soddisfacente, ha previsto non solo degli efficaci strumenti di cooperazione ma si è sforzata di incrementare i mezzi di tutela dei diritti di difesa e delle libertà fondamentali, anche in questo settore, cercando uno *standard* uniforme di tutela tra gli Stati membri.

Tuttavia le trattative per l'adozione di una proposta di decisione quadro su una serie di diritti di carattere procedurale nei procedimenti penali degli ordinamenti nazionali hanno raggiunto una situazione di stallo in occasione del Consiglio europeo GAI del 12-13 giugno 2007.

L'assenza di una visione organica di tali tematiche continua a caratterizzare le iniziative normative in materia di cooperazione, portando una inevitabile realizzazione di non sempre soddisfacenti soluzioni finali di compromesso[142].

5.2 *Le procedure di cooperazione nel sistema delle fonti comunitarie, con particolare attenzione al MERP ed al MAE*

Con il Trattato di Schengen del 14 giugno 1985 è notevolmente migliorato il sistema di scambio delle informazioni tra gli Stati membri per la localizzazione delle persone ricercate, dei contatti tra le autorità nazionali competenti in occasione dell'arresto delle persone e si è consentita l'estradizione senza seguire la procedura formale, previa acquisizione del consenso della persona interessata.

Per migliorare la cooperazione giudiziaria, in particolare in materia di estradizione, sono state approvate la Convenzione di Bruxelles del 1995 e di Dublino del 1996.

---

[141] Cfr *Ibidem,* pagg. 116-119.

[142] Così C. A. FANEGO *Proposta di decisione quadro su determinati diritti processuali nei procedimenti penali nel territorio dell'Unione europea* in *Cassazione penale,* 2008, pagg. 3042 ss.

Le basi più solide verso l'adozione di nuovi e più incisivi strumenti si sono avute all'esito del vertice di Tampere del 1999.

I precedenti strumenti sono stati superati dalla Decisione quadro 2002/584/GAI sul mandato di arresto europeo (MAE), che ha istituito un sistema semplificato e accelerato di consegna delle persone ricerca e ai fini dell'esercizio dell'azione penale o dell'esecuzione di una pena o di una misura di sicurezza privativa della libertà. Trattasi di un regime giuridico che supera le procedure di estradizione e, a differenza di queste ultime, si svolge interamente a livello giurisdizionale, prescindendo dall'intermediazione politica, nella specie dei Ministri di Giustizia.

Gli eventi dell'11 settembre 2011 hanno messo in luce, in maniera quasi prepotente, l'esigenza di realizzare le priorità dello sviluppo della cooperazione per la lotta alla criminalità transnazionale.

L'accelerazione è stata evidente, specie se si osservano le iniziative normative poste in essere in specie dal Consiglio europeo, tra cui l'introduzione del sistema MAE.

Nel preambolo della Decisione quadro 2002/584/GAI si afferma che il mandato di arresto europeo costituisce la prima concretizzazione nel settore del diritto penale del principio di riconoscimento reciproco, definito dal Consiglio europeo come il fondamento della cooperazione giudiziaria.

La disciplina del mandato, come risulta dal punto 35 delle conclusioni di Tampere, nasce dall'opportunità di abolire le procedure formali di estradizione[143].

L'art. 1 della Decisione precisa che il mandato di arresto europeo è costituito da una "*decisione giudiziaria emessa da uno Stato membro (richiedente) in vista dell'arresto e della consegna, da parte di un altro Stato membro (richiesto), di una persona ricercata ai fini dell'esercizio di un'azione penale o dell'esecuzione di una pena o una misura di sicurezza privative della libertà*".

Lo Stato d'esecuzione può subordinare la consegna alla condizione che i fati per i quali è stato emesso il mandato costituiscano reati anche ai sensi del suo ordinamento giuridico. Tale facoltà di applicare la regola della doppia incriminazione non opera però, e questo è sicuramente uno dei profili più innovativi e allo stesso tempo problematici, in riferimento ad un *numerus clausus* di trentadue reati elencati nell'art. 2, paragrafo 2, della Decisione quadro, per i quali è sufficiente chesiano previsti dalla legislazione penale

[143] Così C. M. PAOLUCCI *op.cit.*, pagg. 591-593.
Per un approfondimento sul MAE si rinvia, *ex plurimis,* a AA.VV. *Mandato d'arresto europeo e garanzia delle persone,* Giuffré, 2004; N. GALANTINI *Prime osservazioni sul mandato di arresto europeo* in *Foro Ambrosiano,* 2002, pagg. 264 ss.; E. SELVAGGI *Il mandato di arresto europeo alla prova dei fatti* in *Cassazione penale,* 2002, pagg. 1978 ss.

dello Stato emittente il mandato d'arresto, purché siano puniti con una pena detentiva non inferiore a tre anni di reclusione[144].

Il punto 8 dei *consideranda* della Decisione quadro prevede che i provvedimenti d'esecuzione di un mandato d'arresto devono essere sottoposta ad un controllo sufficiente. L'iniziale verifica formale, avente ad oggetto l'esistenza della decisione, la sua forma e la corrispondenza del contenuto alle previsioni della Decisione, è seguita dalla verifica sulla legittimazione dell'autorità richiedente, della sussumibilità della fattispecie criminosa in uno dei reati previsti dall'art. 2, ovvero, in caso contrario, che si tratti di un fatto punito come reato anche nell'ordinamento giuridico penale dello Stato richiesto.

Altro elemento di rilevante novità è rappresentato dalla parte di disciplina che si concentra sui cd. *constitutional complaints,* cioè sulla possibilità che gli Stati membri valutino l'ammissibilità del andato d'arresto anche nei confronti del cittadino dello Stato membro d'esecuzione, a fronte della prassi generalmente riconosciuta e codificata in molti ordinamenti giuridici, per cui lo Stato sovrano non consente l'estradizione del proprio cittadino. Al riguardo la Decisione quadro prevede che lo Stato d'esecuzione possa ostacolare la consegna di un cittadino o di un residente solo in casi eccezionali, previsti dall'art. 4, paragrafo 6, ovvero soltanto allorquando il mandato di arresto è stato rilasciato ai fini dell'esecuzione della pena o di una misura di sicurezza privativa della libertà di una persona ricercata che dimora nello Stato membro d'esecuzione, ne è cittadino o vi risiede, se tale Stato si impegna ad eseguire esso stesso tale pena o misura di sicurezza conformemente al diritto interno. In assenza di tale impegno, il regime vigente è evidentemente quello dell'obbligo di consegna gravante sullo Stato membro d'esecuzione del mandato.

La differenza tra estradizione e mandato di arresto europeo è lampante. Con l'estradizione entrano in contatto due Stati sovrani, di cui il primo invoca la cooperazione dell'altro che decide, caso per caso, di prestarla o meno, in considerazione di motivi che trascendono il contesto strettamente giuridico, addentrandosi nell'ambito delle relazioni internazionali il cui principio di opportunità politica acquisisce un ruolo rilevante. Al contrario, il mandato d'arresto s'inserisce in uno scenario istituzionale ove l'assistenza viene chiesta e prestata nell'ambito di un sistema giuridico integrato a carattere sovranazionale, all'interno del quale gli Stati, rinunciando parzialmente alla loro sovranità, trasferiscono le proprie competenze ad organi ad essi estranei, dotati anche di poteri normativi.

L'interesse che ha suscitato negli ordinamenti giuridici nazionali l'attuazione del mandato di arresto europeo e le relative difficoltà di

[144] Così C. TRACOGNA *La tutela della libertà personale nel procedimento di consegna attivato dal mandato d'arresto europeo* in *Rivista Italiana di Diritto e Procedura Penale,* 2007, pagg. 988-1020.

omogeneizzazione, ha portato ad adire la Corte di Giustizia UE in materia, la cui sentenza è stata a lungo attesa per i contenuti di motivi di ricorso proposti.

La Corte è stata interpellata, a norma dell'art. 35 TUE, dalla *Cour d'Arbitrage* belga sulla validità giuridica della Decisione quadro 2002/584/GAI[145].

Il giudice nazionale ha messo in discussione il fondamento normativo utilizzato dal Consiglio per adottare la Decisione quadro MAE, interrogandosi sull'idoneità dello strumento prescelto. In particolare, secondo il giudice di rinvio, la Decisione sarebbe invalida in quanto la disciplina del mandato d'arresto europeo avrebbe dovuto essere adottata come una convenzione e non con una decisione quadro. In base all'art. 34, paragrafo 2, TFUE che delinea le materie oggetto di regolamentazione con una decisione quadro, secondo il giudicante belga, limita ai soli casi in cui la *ratio legis* sia quella di avvicinare le disposizioni legislative e regolamentari degli Stati membri.

Con riguardo al secondo motivo di ricorso, quello di natura sostanziale, il giudice di rinvio riteneva che il principio d'uguaglianza sarebbe stata violata dall'art. 2 della Decisione, laddove prevede un elenco chiuso di reati, così disattendendo senza giustificazione al requisito della doppia incriminazione, mantenendolo in vita per le altre fattispecie.

Il principio di legalità sarebbe invece stato leso a causa della mancata chiarezza e precisione nella configurazione delle fattispecie di reato previste dalla Decisione quadro, per cui lo Stato richiesto si troverebbe a disporre di informazioni insufficienti per accertare se i reati attribuiti al ricercato rientrino effettivamente in una delle categorie previste dall'art. 2 dell a Decisione MAE.

I Giudici comunitari hanno sottolineato che non è possibile interpretare le disposizioni del Trattato nel senso di ridurre l'autorizzazione all'adozione di una decisione quadro esclusivamente nei settori di cui all'art. 31, paragrafo 1 (e) TUE: "*Rientra nella discrezionalità del Consiglio di privilegiare lo strumento giuridico della decisione quadro quando, come in questa fattispecie, siano presenti le condizioni per l'adozione di tale atto*".

In riferimento alla presunta violazione del principio di legalità, i Giudici della Corte di Giustizia hanno precisato che la Decisione quadro MAE non sia volta ad armonizzare i reati in questione per quanto riguarda i loro elementi costitutivi e le relative pene e, di conseguenza, anche gli Stati membri sono legittimati a riportare pedissequamente l'elenco dei reati di cui all'art. 2 nelle leggi nazionali, pur modificandone eventualmente la definizione stessa di reati e applicando le sanzioni già previste dal diritto dello Stato emittente.

---

[145] Il riferimento è alla sentenza della Corte di Giustizia delle Comunità europee nel caso C-303/05, Advocaten voor Wereld VZW c. Leden van de Ministerraad.
Cfr O. POLICINO *op.cit,*

In relazione alla presunta violazione del principio di uguaglianza e non discriminazione, i Giudici comunitari hanno fatto espresso riferimento al *mutual trust* tra gli Stati membri, precisando che già la *ratio* del Consiglio europeo intendeva individuare quelle categorie di reati che arrecano all'ordine e alla sicurezza pubblica un pregiudizio tale da giustificare l'eliminazione dell'obbligo di controllo della doppia incriminazione.

Allo scopo di favorire lo scambio di informazioni ed il mutuo riconoscimento tra gli Stati membri dell'Unione europea, la seconda misura adottata, dopo il mandato di arresto europeo, è costituita dal mandato europeo di ricerca della prova.

Il 14 novembre 2003 la Commissione europea ha avanzato una proposta di Decisione quadro del MERP, avente ad oggetto l'ottenimento di oggetti, documenti e dati da utilizzare nei procedimenti in materia penale [146].

Sotto la guida della Presidenza olandese questo progetto è divenuto una priorità assoluta dell'Unione e in occasione del *Working Party* sulla cooperazione in materia penale è stata esaminata la proposta di Decisione quadro della Commissione[147].

La Decisione quadro sul MERP[148] ha perseguito gli scopi proposti già nelle conclusioni del Consiglio europeo di Tampere, rendendo più veloce ed efficace la cooperazione in materia penale.

Il MERP viene emesso dalle autorità competenti designate dagli Stati membri: giudici, organi giurisdizionali, magistrati inquirenti, pubblici ministeri o qualsiasi altra autorità giudiziaria.

Esso è applicabile nei procedimenti penali avviati con riferimento a un illecito penale previsto come tale in base alla legislazione nazionale dello Stato di emissione; in procedimenti avviati dalle autorità amministrative in relazione a fatti punibili in base alla legislazione nazionale dello Stato di emissione a titolo di violazioni di norme giuridiche e quando la decisione può dar luogo a un procedimento dinanzi a un organo giurisdizionale competente in materia penale; in procedimenti avviati dalle autorità giudiziarie in relazione a fatti punibili in base alla legislazione nazionale dello Stato di emissione perché configurano violazioni di norme giuridiche e quando la decisione può dar luogo a ulteriori procedimenti dinanzi a un organo giurisdizionale competente segnatamente in materia penale; in collegamento con i procedimenti di cui sopra relativi a reati o violazioni per i quali una

[146] La proposta di Decisione quadro sul mandato europeo di ricerca della prova è COM (2003) 688 finale.

[147] In occasione dello stesso *Working Party* è stata esaminata anche la proposta di Decisione sullo scambio d'informazioni in materia penale e l'iniziativa di Decisione in materia di *data retention*.

[148] La Decisione quadro 2008/978/GAI sul mandato europeo di ricerca della prova è entrata in vigore il 19 gennaio 2009 ed è stata pubblicata in Gazzetta Ufficiale CE L 350 del 30 dicembre 2008.

persona giuridica può essere considerata responsabile o punita nello Stato di emissione.

Lo Stato di emissione deve assicurarsi che le prove richieste siano necessarie e proporzionate ai fini dei procedimenti e che, in circostanze analoghe, l'acquisizione di tali prove siano previste dal diritto nazionale, quali *condiciones sine qua non*. .

Se l'autorità competente di uno Stato di emissione ha motivi legittimi per ritenere che prove pertinenti si trovino sul territorio di un altro Stato membro, essa potrà trasmettere la richiesta di mandato di ricerca della prova all'autorità competente dello Stato richiesto, con ogni mezzo che consenta di conservare una traccia scritta, tra cui anche il sistema di telecomunicazione protetto della Rete giudiziaria europea.

Se il MERP non è stato emesso o convalidato da un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero, l'autorità di esecuzione può decidere di non procedere all'esecuzione di quanto richiesto, previa consultazione con l'autorità competente dello Stato di emissione prima di procedere a formalizzare il rifiuto.

L'autorità di esecuzione ottempera alle formalità espressamente indicate dall'autorità di emissione, salvo i casi in cui la Decisione quadro 2008/978/GAI disponga diversamente. Tali formalità non devono tuttavia essere in conflitto con i diritti fondamentali tutelati dallo Stato di esecuzione.

Il rifiuto può legittimamente applicarsi, nel termine di trenta giorni dalla ricezione della richiesta, qualora sia in contrasto con il principio del *ne bis in idem*; qualora, in taluni casi indicati nella decisione quadro, i fatti non costituiscano reato a norma della legislazione dello Stato di esecuzione; qualora non sia possibile eseguire il MERP con qualsiasi delle misure a disposizione dell'autorità di esecuzione nel caso specifico; qualora il diritto dello Stato di esecuzione preveda immunità o privilegi che rendono impossibile l'esecuzione dello stesso; qualora il mandato di ricerca non sia stato convalidato da un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero nello Stato di emissione, quando richiesto; qualora il MERP si riferisca a reati che sono stati commessi nel territorio dello Stato di esecuzione o dello Stato di emissione, quando la legislazione dello Stato di esecuzione non consente l'azione penale; qualora la sua esecuzione leda gli interessi della sicurezza nazionale; qualora il formulario sia incompleto o non compilato correttamente.

Il riconoscimento o l'esecuzione del mandato europeo di ricerca delle prova può essere subordinato alla verifica della doppia incriminazione, se per la sua esecuzione è richiesta una perquisizione o un sequestro e se non è riferito ad uno dei reati elencati specificamente nella Decisione quadro.

Lo Stato di esecuzione deve provvedere a raccogliere quanto richiesto nel termine di sessanta giorni dalla ricezione della richiesta, salvo i casi in cui sussistano motivi legittimi per un rinvio[149].

Sono tanti gli aspetti positivi del mandato europeo di ricerca della prova nel quadro dello sviluppo di forme efficaci ed efficienti di cooperazione. Tuttavia si rilevano alcuni inconvenienti nella pratica applicativa poiché, per i limiti dell'oggetto entro cui è applicabile il MERP, costringe ad utilizzare strumenti diversi anche all'interno del medesimo procedimento[150].

Per questa ragione, il mandato europeo di ricerca della prova è destinato a costituire solo un primo passo verso uno sviluppo più pregnante del principio di mutuo riconoscimento, il quale porterà necessariamente all'introduzione di strumenti utilizzabili nella generalità delle operazioni d'indagine di un qualsiasi procedimento penale che coinvolge più Stati. In questo contesto, si pensi alla proposta di Decisione quadro della Commissione europea sull'Ordine Europeo d'Indagine che risponde alla menzionata finalità e che, ad oggi, è ancora oggetto di discussione e modifiche prima di una decisiva (e attesa) attuazione.

Altra questione controversa, attiene la definizione del concetto di "prova esistente", l'unica categoria a cui è applicabile il mandato europeo di ricerca della prova, è l'individuazione dei confini dell'area di significanza. Si tratta, dunque, di oggetti, dati e documenti specifici già costituiti, di cui si chiede ad uno Stato estero la raccolta ed assicurazione. Sono escluse tutte le prove costituende, quali le intercettazioni, per cui non è possibile avanzare una richiesta di MERP. Questa regola di esclusione limita fortemente l'ambito di applicazione della Decisione quadro 2008/978/GAI, specie se si considera il ruolo fondamentale delle prove costituende (le intercettazioni *in primis*) per orientare la prosecuzione delle indagini e, conseguentemente, rappresentare un supporto valido alla formazione di un quadro probatorio completo, ai fini del giudizio[151].

La libertà di scelta del regime linguistico da parte degli Stati membri e l'esistenza di un modulo predefinito per avanzare la richiesta di MERP, agevolano l'applicazione dello strumento negli ordinamenti nazionali e, di conseguenza, lo sviluppo della cooperazione. Resta ancora irrisolto il problema legato alla comprensione della richiesta presso lo Stato d'esecuzione il quale si troverà costretto, nella maggioranza dei casi, a provvedere ad una traduzione del *form* ricevuto, con un notevole ampliamento dei tempi di

[149] http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/jl0015_it.htm (consultato in data 30 maggio 2009).
[150] Così J. A. E. VERVAELE *European Evidence Warrant,* Intersentia, 2005.
[151] *Ibidem,* pagg. 12-15.

risposta allo Stato richiedente, oltre al rischio di pregiudizio dell'efficacia della misura di collaborazione.

Nulla quaestio in relazione alle disposizioni della Decisione quadro sul mandato europeo di ricerca della prova che prevedono un regime minimo di garanzia dei diritti fondamentali nello svolgimento delle procedure di richiesta ed esecuzione.

Gli Stati membri sono obbligati ad adottare le disposizioni necessarie per assicurare che ogni soggetto interessato disponga di mezzi d'impugnazione contro il riconoscimento e l'esecuzione di un MERP, anche se solo in determinate ipotesi che gli ordinamenti nazionali sono liberi di individuare discrezionalmente.

L'accelerazione e la semplificazione nel trasferimento delle prove di un procedimento penale hanno un forte impatto anche nella realizzazione di un vero *due process*.

In questi termini è altresì funzionale la previsioni della Decisione quadro di limitati casi in cui lo Stato d'esecuzione può apporre il rifiuto.

Mancano delle disposizioni specifiche in tema di ammissibilità della prova così raccolta, in considerazione del fatto che ogni ordinamento giuridico nazionale prevede dei modi differenti e non uniformati di esecuzione delle operazioni d'indagine[152].

Si tenga conto che il collezionamento della prova, infatti, pur costituendo solo una parte del processo penale, rappresenta una sezione complessa e delicata che può pregiudicare irreversibilmente lo svolgimento dell'intero giudizio ed anche la decisione finale[153].

6. *Gli organi comunitari coinvolti nelle procedure di cooperazione: Europol, Eurojust e Olaf*

La costituzione di un avanzato sistema globale di assistenza giudiziaria e di polizia, al fine di prevenire efficacemente le forme più gravi di criminalità transnazionale, non può prescindere dalla coordinazione tra le diverse autorità coinvolte nei procedimenti penali.

Per far fronte all'internazionalizzazione della criminalità, nel 1914 a Monaco di Baviera e poi nel 1923 a Vienna venne costituita l'Organizzazione Internazionale di Polizia Criminale, la quale attualmente ha sede a Lione.

---

[152] Si pensi al caso della prova digitale che, per il tecnicismo ontologico che la contraddistingue, richiede un intervento delicato di personale esperto affinché si proceda alla raccolta senza pregiudicarne i risultati e l'utilizzabilità nei giudizi di uno Stato diverso da quello d'esecuzione, ove sussistano regole e principi diversi di ammissibilità e genuinità dei contenuti.

[153] Cfr J. A. E. VERVAELE *op.cit.*, pagg. 126-129.

L'Interpol ha uno statuto riconosciuto dall'ONU e si prefigge lo scopo di assicurare la più ampia possibile mutua assistenza tra autorità di polizia criminale, nei limiti delle leggi esistenti nei diversi Paesi e dello spirito della Dichiarazione Universale dei diritti umani.

Questa Organizzazione è strutturata in una sede centrale e diverse sedi periferiche a livello nazionale ed opera attraverso una propria connessione telematica, costituita da una banca dati mondiale collocata presso il Segretariato Generale di Lione.

L'Interpol può scambiare informazioni di polizia in relazione a fatti costituenti reato di diritto comune, relative alle indagini ed alla prevenzione di delitti.

L'O.I.C.P. (Organizzazione Internazionale di Polizia Criminale) è attualmente composta da centottantasei Stati e si occupa principalmente di favorire l'esecuzione delle procedure rogatori ali ed estradizionali, di agevolare lo scambio di informazioni e le richieste di accreditamento per l'estero[154].

La risposta alle mutate esigenze di cooperazione tra autorità di polizia è stata data anche per il tramite della previsione normativa che ha introdotto la possibilità di costituire le squadre investigative comuni (*Joint Investigation Team*).

Le basi normative in materia hanno connotazioni internazionali, essendo contenute dalla Convenzione ONU del 2000 sul crimine organizzato. In questo Accordo è stabilito il principio secondo cui, qualora uno o più Stati stiano conducendo un'indagine, un'azione penale o un procedimento giudiziario in relazione agli stessi fatti criminosi, le competenti autorità degli Stati coinvolti si devono consultare e valutare l'opportunità di coordinare le proprie azioni, anche tramite la sottoscrizione di accordi bilaterali o multilaterali, finalizzati alla costituzione di organi investigativi comuni[155]. Questi ultimi organi sono espressamente previsti dall'art. 19 della menzionata Convenzione, la quale prevede, nell'ipotesi di assenza di accordi o intese, di intraprendere indagini comuni sulla base di accordi predisposti caso per caso, nel pieno rispetto della sovranità dello Stato parte nel cui territorio tale indagine avrà luogo. L'Accordo ONU, dunque, pur utilizzando una terminologia volutamente generica, fa riferimento alle squadre investigative comuni.

Per quanto riguarda l'Unione europea, la previsione della costituzione di squadre investigative comuni ed il loro funzionamento si trova nell'art. 13 della Convenzione adottata dal Consiglio a norma dell'art. 34 TFUE, relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea.

---

[154] Per le informazioni principali su Interpol si rinvia a C. M. PAOLUCCI *op.cit.,* pagg. 467-470.
[155] Cfr E. APRILE – F. SPIEZIA *op.cit.,* pagg. 196-198.

Tale strumento nasce da una proposta italiana, positivamente sperimentata mediante l'applicazione di un Accordo italo-svizzero, concluso a Roma il 10 settembre 1998, a completamento ed integrazione della Convenzione di Strasburgo del 1959.

In base all'art. 22 del menzionato Accordo, nell'ambito dei fatti oggetto di procedimenti penali in ciascuno dei due Stati, le autorità giudiziarie interessate, eventualmente accompagnate dagli organi di polizia, possono, previa informazione al Ministero della Giustizia, alla Direzione Generale degli Affari Penali e all'Ufficio federale di polizia, operare congiuntamente in seno a gruppi di indagine comuni.

In attesa dell'entrata in vigore della Convenzione sull'assistenza giudiziaria del 2000, al fine di anticiparne l'introduzione e gli effetti benefici negli Stati, il Consiglio europeo, il 13 giungo 2002, ha adottato la Decisione quadro 2002/465/GAI, relativa all'istituzione delle squadre investigative comuni[156].

In tale accordo è stata dettata una disciplina dettagliata circa la composizione e sulla modalità di funzionamento di dette squadre, rimettendo al legislatore nazionale la soluzione del problema relativo all'utilizzabilità degli atti assunti in territorio estero.

Come si evince anche dal testo del *considerandum* 6 della Decisione quadro, essa risponde alla necessità di prevedere delle misure più efficaci per le indagini in materia di traffico di stupefacenti, di tratta di esseri umani e terrorismo[157].

Le squadre investigative comuni, le quali possono essere composte da rappresentanti degli Stati membri interessati e da soggetti terzi, sono chiamate ad operare quando più Stati membri svolgono indagini su reati che, per le circostanze contingenti, esigono un'azione coordinata.

In ossequio al principio della *lex loci,* è previsto che la squadra debba operare in conformità al diritto dello Stato membro in cui interviene [158].

In una riflessione generale sugli strumenti investigativi nel contesto delle iniziative internazionali per combattere il riciclaggio, il crimine organizzato e il finanziamento al terrorismo, sono degni di nota alcuni nuovi modelli di raccolta delle prove in continua espansione.

Ci si riferisce, in particolare, ad un piano di collaborazione di natura amministrativa e di polizia che si sostanzia nelle funzioni delle Fiu (*Financial Investigation Unit*).

---

[156] La Decisione quadro è stata pubblicata in Gazzetta Ufficiale CE del 20 giugno 2002, L. 162, ed è entrata in vigore il 20 giugno 2002.

[157] Cfr E. APRILE – F. SPIEZIA *op.cit.,* pag. 198.

[158] Per un approfondimento sul JIT e sulla normativa italiana di attuazione della Decisione quadro del Consiglio europeo 2002/465/GAI, si rinvia a E. APRILE – F. SPIEZIA *op.cit.,* pagg. 196-204; C. M. PAOLUCCI *op.cit.,* pagg. 475-485.

Un numero considerevole di Stati ha istituito le Fiu, con compiti di acquisizione ed analisi delle informazioni ricevute dalle banche e da qualsiasi altra istituzione finanziaria.

Le Unità di diversi Stati possono scambiarsi direttamente le informazioni su operazioni finanziarie sospette[159].

Nel quadro europeo della cooperazione di polizia, è acquisito particolare rilevanza l'istituzione di Europol, un Ufficio di polizia europeo, con la Convenzione firmata a Bruxelles il 26 luglio 1995.

Nasce nel 1994 a titolo provvisorio come E.D.U. (Unità europea antidroga), sulla base di un accordo ministeriale, in base al quale i funzionari dei vari Paesi membri vengono inviati all'Aja al fine di sviluppare progetti di cooperazione investigativa contro traffici illeciti di stupefacenti.

Già il Trattato di Maastricht del 7 febbraio 1992 aveva previsto la formazione di un Ufficio Europeo di Polizia agli articoli K1 e K2, corrispondenti agli articoli 29 e 30 dopo le modifiche apportate dal Trattato di Amsterdam, allo scopo di ottenere una cooperazione rafforzata tra le forze di polizia.

L'attivazione di Europol presupponeva indizi dell'esistenza di una struttura o organizzazione criminale e che due o più Stati fossero lesi dal fatto criminoso.

Ciascuno Stato membro, ai sensi dell'art. 4 della Convenzione, ha costituito o designato un'unità nazionale, incaricata di svolgere le funzioni di collegamento, scambio e analisi di dati, mediante l'utilizzo di una rete protetta di gestione e circolazione delle informazioni.

Europol predispone rapporti operativi e tecnici quando lo Stato membro non ne dispone, fornisce informazioni su speciali tecniche d'indagine, collabora con Stati membri e Paesi Terzi. Può scambiare dati per orientare e supportare le indagini e intrattenere rapporti con gli uffici di Olaf, Eurojust e dell'ONU.

Nella prospettiva del Trattato di Amsterdam era stato previsto l'incremento delle attribuzioni di Europol, con maggiori compiti di coordinamento e di effettuazione di specifiche attività investigative da parte delle competenti autorità degli Stati membri.

Il 30 novembre 2000 il Consiglio ha adottato l'atto che stabilisce in base all'art. 43, paragrafo 1 della Convenzione, un protocollo che modifica l'art. 2 e l'allegato di detto Accordo, estendendo le competenze di Europol anche alla materia del riciclaggio.

A norma dell'art. 26 comma 1 della Decisione del 28 febbraio 2002 che istituisce Eurojust, Europol deve mantenere una stretta collaborazione con

[159] Per un approfondimento sul ruolo delle Fiu, si rinvia a E. APRILE – F. SPIEZIA *op.cit.*, pagg. 209-212.

quest'organo, anche al fine di agevolare la prevenzione e lotta alla criminalità e di evitare inutili sovrapposizioni funzionali.

Europol è ora contemplata dall'art. 88 TFUE, come modificato a seguito del Trattato di Lisbona, nella quale disposizione si precisa che questo Organo ha il compito di sostenere e potenziare l'azione delle autorità di polizia e degli altri servizi incaricati dell'applicazione della legge degli Stati membri e la reciproca collaborazione nella prevenzione e lotta contro la criminalità grave che interessa due o più Stati membri, il terrorismo e le forme di criminalità che ledono un interesse comune oggetto di una politica dell'Unione [160].

Il paragrafo 2 della medesima disposizione prevede la possibilità per il Consiglio europeo ed il Parlamento, per mezzo di regolamenti previsti all'uopo, di determinare la struttura, il funzionamento, i compiti di Europol all'interno degli ambiti classici di attività.

Il 6 aprile 2009 è stata adottata la Decisione quadro 2009/371/GAI che istituisce Europol e sostituisce le precedenti disposizioni normative in materia.

Tale Decisione riconosce ad Europol la più ampia capacità giuridica riconosciuta alle persone giuridiche di diritto interno [161].

L'art. 3 non apporta nessuna modifica in seno agli scopi dell'attività di Europol.

All'art. 4 della Decisione, è stabilita la competenza di Europol in materia di criminalità organizzata, di terrorismo e di altre forme gravi di criminalità elencate nell'allegato all'Accordo [162].

I compiti principali attualmente attribuiti ad Europol sono: raccogliere, conservare e scambiare informazioni e *intelligence;* comunicare senza indugio alle autorità competenti degli Stati membri le informazioni che le riguardano e ogni altro collegamento constatato tra i reati; facilitare le indagini negli Stati membri, in particolare trasmettendo alle unità nazionali tutte le informazioni pertinenti; chiedere alle autorità competenti degli Stati interessati di avviare, svolgere o coordinare indagini e di proporre l'istituzione di squadre investigative comuni in casi specifici; fornire *intelligence* e supporto analitico agli Stati membri in relazione ad eventi internazionali di primo piano;

[160] Cfr art. 88 TFUE.

[161] Cfr art. 2 Decisione quadro 2009/371/GAI.

[162] L'allegato alla Decisione quadro 2009/371/GAI presenta il seguente elenco di reati: traffico illecito di stupefacenti, attività illecite di riciclaggio di denaro, criminalità nella materia del nucleare e della radioattività, organizzazione clandestina di immigrazione, tratta di esseri umani, criminalità connessa al traffico di veicoli rubati, omicidio volontario, lesioni personali gravi, traffico illecito di organi e tessuti umani, rapimento, sequestro e presa di ostaggi, razzismo e xenofobia, furti organizzati, traffico illecito di beni culturali, truffe e frodi, racket ed estorsioni, contraffazioni e pirateria, falsificazione di atti amministrativi e traffico di documenti falsi, falsificazione di monete e di altri mezzi di pagamento, criminalità informatica, corruzione, traffico illecito di armi, munizioni ed esplosivi, traffico illecito di specie animali protette, criminalità ambientale, traffico illecito di sostanze ormonali ed altri fattori di crescita.

preparare valutazioni delle minacce, analisi strategiche e rapporti di situazione in relazione all'obiettivo, incluse valutazioni della minaccia costituita dalla criminalità organizzata[163].

Europol funge anche da supporto alle squadre investigative comuni[164] e può chiedere agli Stati membri di avviare indagini penali, dopo averne dato avviso ad Eurojust[165].

La Decisione detta inoltre una dettagliata disciplina sul sistema di trattamento delle informazioni e contiene anche delle norme sulla protezione del segreto delle informazioni di Europol[166].

Nel quadro di sviluppo della cooperazione giudiziaria, con un'azione comune adottata il 22 aprile 1996 dal Consiglio europeo, è stato previsto uno scambio di magistrati di collegamento diretto a migliorare la collaborazione tra queste autorità dei diversi Stati membri dell'Unione europea.

L'obiettivo di tale azione è quello di rendere più rapida ed efficace lo scambio di informazioni sui sistemi giuridici e giudiziari dei Paesi membri.

Sulle funzioni del Magistrato di collegamento, l'art. 2 dell'Azione Comune è molto generico, riferendosi a qualsiasi attività intesa a facilitare, nonché accelerare, in particolare tramite l'istituzione di contatti diretti con i servizi competenti e con le autorità giudiziarie dello Stato di destinazione, tutte le forme di cooperazione giudiziaria in campo penale[167].

Le funzioni del Magistrato di collegamento possono finire per sovrapporsi, in taluni casi, a quelle della Rete Giudiziaria Europea.

Il *European Judicial Network* è una rete di punti di contatto, istituita con azione comune del Consiglio europeo del 29 giugno 1998, sulla base dell'art. K3 TFUE.

La creazione di questa Rete ha lo scopo precipuo di migliorare qualitativamente la cooperazione giudiziaria in materia penale tra gli Stati membri dell'UE.

I diversi punti di contatto, dislocati nei territori nazionali, sono a disposizione delle autorità giudiziarie locali e delle altre autorità competenti dei Paesi nonché dei punti di contatto designati dagli altri Stati.

In base agli articoli 4 e seguenti dell'Azione comune, la Rete facilita l'istituzione di contatti adeguati tra le persone individuate quali punti di contatto degli Stati membri; organizza riunioni periodiche tra i rappresentanti

---

[163] Cfr art. 5 Decisione quadro 2009/371/GAI.
[164] Cfr art. 6 Decisione quadro 2009/371/GAI.
[165] Cfr art. 7 Decisione quadro 2009/371/GAI.
[166] Per un approfondimento su Europol si rinvia, *ex multis*, a C. M. PAOLUCCI *op.cit.,* pagg. 471-473; E. APRILE – F. SPIEZIA *op.cit.,* pagg. 243-248; A. PAGOTTO *La cooperazione in campo investigativo* in *www.csm.it* (sito consultato in data 10 ottobre 2010).
[167] Cfr art. 2 Azione comune del Consiglio europeo del 22 aprile 1996.
Sul Magistrato di collegamento si rinvia a C. M. PAOLUCCI *op.cit.,* pag. 431.

nazionali; fornisce informazioni aggiornate anche attraverso una rete di telecomunicazioni in grado di collegare direttamente i punti di contatto.

L'art. 8 specifica quali sono i dati ai quali devono avere accesso i punti di contatto: i dati completi sugli altri punti di contatto, l'elenco delle autorità giudiziarie degli altri Paesi, i testi giuridici delle convenzioni in vigore.

L'Azione comune 98/428/GAI è stata sostituita dalla Decisione quadro 2008/976/GAI del 16 dicembre 2008 che lascia sostanzialmente immutati gli aspetti principali della Rete ma introduce la figura del corrispondente nazionale e degli incaricati degli aspetti tecnici[168].

Agli strumenti preesistenti viene aggiunta una rete di telecomunicazioni protetta, in grado di favorire la circolazione sicura dei dati e delle informazioni tra le autorità giudiziarie degli Stati membri, anche attraverso il collegamento con il sistema automatico di gestione dei fascicoli di Eurojust previsto in base all'art. 16 della Decisione quadro 2002/187/GAI[169].

Eurojust costituisce un organismo dell'Unione europea fra i più innovativi ed incisivi nel settore della cooperazione giudiziaria penale europea.

La sua istituzione è avvenuta con la Decisione quadro del 28 febbraio 2002 (2002/187/GAI).

Eurojust ha preso il posto dell'Unità provvisoria di cooperazione giudiziaria, istituita dal Consiglio europeo con la precedente decisione del 14 dicembre 2000 (n. 2000/799/GAI), cd. Pro-Eurojust, così concludendo il percorso avviato con il Consiglio europeo di Tampere del 1999.

Dotato di personalità giuridica, Eurojust è un organo collegiale, con sede all'Aja dal 2002, composto da ventisette membri nazionali, nominati da ciascuno Stato membro dell'Unione europea. I membri nazionali sono magistrati del pubblico ministero o giudici, ovvero funzionari di polizia con prerogative assimilabili a quelle giudiziarie.

Eurojust, al fine di rafforzare la lotta contro le forme gravi di criminalità organizzata[170], interviene nell'ambito delle indagini ed azioni penali che coinvolgono almeno due Stati membri e nel caso di fattispecie criminose tra quelle elencate nella stessa Decisione quadro.

Si presenta, sostanzialmente, come il corrispondente giudiziario di Europol, con il quale mantiene stretta collaborazione.

La particolarità di questo organismo di agevolazione e coordinamento delle indagini risiede nel fatto che, data la sua posizione, è in grado di avere una visione globale ed aperta nel quadro di un'investigazione. Eurojust

[168] Cfr art. 2 Decisione quadro 2008/976/GAI.
[169] Cfr art. 9 Decisione quadro 2008/976/GAI.
Sulla Rete Giudiziaria Europea si rinvia a C. M. PAOLUCCI *op.cit.*, pagg. 432-435.
[170] Cfr considerando 3 Decisione quadro 2002/87/GAI.

permette di ottenere una visione d'insieme del fatto penalmente rilevante, superando i limiti territoriali, e così di poter meglio inquadrare e combattere anche le forme più gravi di criminalità transnazionale.

L'attività principale dell'organo è il coordinamento delle indagini ed in particolare la promozione della collaborazione tra le autorità competenti degli Stati membri e l'agevolazione dell'attuazione dell'assistenza giudiziaria internazionale e l'esecuzione delle richieste di estradizione.

L'ambito di competenza di Eurojust comprende tutte le forme più gravi di criminalità e per i reati per i quali è altresì competente Europol.

Questo Organismo di coordinamento può svolgere la sua attività per il tramite di uno o più membri nazionali[171] o attraverso il collegio[172].

L'opera di relazione svolta da Eurojust ha carattere di facoltatività, non avendo la possibilità di impartire direttive vincolanti per prevenire o risolvere i possibili contrasti nascenti tra le autorità nazionali interessate.

Al fine di migliorare i rapporti tra gli Stati membri ed Eurojust è previsto che gli stessi informino questo organismo dei procedimenti che possano rientrare nella sua area di competenza[173].

Uno degli aspetti caratterizzanti e qualificanti l'azione di Eurojust nei rapporti con le autorità giudiziarie nazionali, discende direttamente dall'approfondimento dei poteri conferiti al membro nazionale o al collegio.

Nella pratica dei rapporti di cooperazione giudiziaria sta crescendo il ruolo di Eurojust nella lotta alle forme di criminalità transfrontaliera, in particolare in materia di crimini organizzati e terrorismo.

Questa indicazione è confortata dai dati statistici che mostrano un incremento considerevole dei casi trattati: nel mese di dicembre 2007 è stata registrata una crescita di oltre il 50% rispetto all'anno precedente e nel 2008, già nel mese di ottobre, sono stati registrati più di mille casi [174].

Accanto alle note positive sul miglioramento del funzionamento di Eurojust e sulla rapidità dello svolgimento delle attività, si riscontrano ancora degli ostacoli al suo ottimale coinvolgimento.

Questa considerazione più volte avanzata dal Consiglio europeo ha portato, per l'effetto, alla nuova Decisione quadro di Eurojust adottata nel dicembre del 2008.

L'obiettivo perseguito con questo nuovo Accordo, dal punto di vista strettamente tecnico-politico, è stato quello di agevolare la funzionalità dell'organismo, superando i particolarismi e le diffidenze create dalla gelosia endemica degli Stati membri.

---

[171] Cfr art. 6 Decisione quadro 2002/187/GAI.
[172] Cfr art. 7 Decisione quadro 2002/187/GAI.
[173] Cfr art. 13 Decisione quadro 2002/187/GAI.
[174] Così E. APRILE – F. SPIEZIA *op.cit.*, pag. 227.

I nuovi contenuti, infatti, hanno lo scopo di accrescere le competenze, il ruolo e l'operatività di Eurojust anche e soprattutto per combattere efficacemente il crimine organizzato e il terrorismo [175].

Dal punto di vista attuativo, Eurojust ha stabilito punti di contatto e siglato accordi con gli Stati Uniti d'America, con la Norvegia, con la Svizzera, così mostrando l'interesse a coordinare le indagini transnazionali anche in relazione a quelle categorie di reati che tipicamente sviluppano i loro effetti negativi anche in Paesi non membri dell'Unione europea [176].

Le differenze agevolano le manifestazioni criminose e il tendenziale spostamento dell'autore di reato alla ricerca della minore (eventuale) reazione giuridica, ma costituiscono anche una barriera alla piena realizzazione della funzionalità di Eurojust[177].

A seguito delle modifiche operate nel 2008, sono stati rafforzati strutturalmente i *desk* nazionali, allo scopo di garantire una continuità ed effettività nella realizzazione degli scopi dell'organismo [178].

Il ruolo del membro nazionale è rafforzato, prevedendo la possibilità che questi richiedano direttamente alle autorità competenti degli Stati membri di svolgere attività investigative e stimolino le autorità stesse a rispondere in tempi rapidi..

In fase di attuazione, gli Stati sono liberi di definire la natura e l'estensione dei poteri da attribuire al proprio membro nazionale, entro i limiti minimi degli s*tandard* generali comuni, previsti dalla Decisione [179].

La possibilità che il membro nazionale sia anche parte di un'autorità competente è funzionale al miglioramento del flusso di informazioni e della cooperazione tra Eurojust e i Paesi membri.

I membri nazionali, in base all'art. 9.4 hanno acquisito il potere di accesso quanto meno non equivalenti a quelli delle autorità giudiziarie nazionali con riferimento al registro del casellario giudiziale, registro delle persone arrestate, registro delle indagini pendenti, registro della Direzione Nazionale Antimafia e degli altri registri dello Stato di appartenenza, allorché ritenga che le informazioni siano necessarie per lo svolgimento delle funzioni.

L'incremento degli obblighi informativi di cui all'art. 13 è strettamente finalizzato a mettere l'organismo sovranazionale in condizione di poter assolvere ai compiti affidati.

---

[175] *Ibidem,* pag. 227.
[176] Così A. PAGOTTO *op.cit.*
[177] Si è solito parlare del cd. *forum shopping* il quale spesso può determinare addirittura l'impunità di un autore di reato. Per questi motivi è necessario prevedere delle misure idonee ed efficaci per dissuadere da queste pratiche e per contrastare gli spostamenti nel territorio UE a tale scopo.
[178] Cfr art. 2 Decisione quadro del 2008.
[179] Cfr art. 9 Decisione quadro del 2008.

Sono rilevanti anche le modifiche apportate ai poteri del collegio, anche al fine di valorizzare il funzionamento di quest'organo. Il collegio, oltre ai poteri già conferiti precedentemente, potrà emettere pareri in forma scritta, non vincolanti, nei casi in cui due o più Stati membri non raggiungano un accordo su un conflitto di giurisdizione ovvero di rifiuto congiunto ad intraprendere un'indagine penale.

Altro profilo di innovazione riguarda il rafforzamento della cooperazione di Eurojust con la Rete giudiziale europea e con i corrispondenti nazionali[180].

Tra i principali organi comunitari per la cooperazione, in particolare con riferimento alla tutela degli interessi finanziari dell'Unione, si annovera l'istituzione dell'OLAF, l'Ufficio Europeo per la lotta Antifrode, con la Decisione quadro del 28 aprile 1999 della Commissione europea.

Questo Ufficio risponde all'esigenza di potenziamento della lotta contro le frodi comunitarie e la correzione, a danno del bilancio dell'Unione.

La tutela degli interessi finanziari ha da sempre rivestito un ruolo di notevole importanza in ambito europeo, tanto da riguardare sia interventi normativi sia giurisprudenziali.

Il più importante degli strumenti adottati nel settore è rappresentato dalla Convenzione PIF – Convenzione relativa alla tutela degli interessi finanziari della Comunità europea del 26 luglio 1995, entrata in vigore solo il 17 ottobre 2002, sebbene molte disposizioni erano già contenute nei trattati istitutivi, in specie nell'art. 280 TCE, ora art. 325 TFUE, come modificato dal Trattato di Lisbona[181].

Il particolare interesse dell'Unione per la materia è confermato dalla lettera del Regolamento 2988/95 del Consiglio del 18 dicembre 1995, relativo alla tutela degli interessi finanziari delle Comunità europee, ma anche nelle proposte volte alla tutela di tali interessi e confluite nel *Corpus Juris* e nel Libro Verde dell'OLAF e infine nel Trattato di Lisbona[182].

Lo scopo e le funzioni dell'OLAF sono dettagliate nel testo del regolamento (CE) n. 1073 del 1999 e n. 1074 del medesimo anno, a cura del Parlamento europeo e del Consiglio.

---

[180] Cfr art. 12 Decisione del 2008.
Per un approfondimento sul ruolo e le funzioni di Eurojust, *ex multis*, si rinvia a F. SPIEZIA – E: APRILE *op.cit.,* pagg. 213-236; C. M. PAOLUCCI *op.cit.,* pagg. 443-461; M. PANZAVOLTA *Eurojust: il braccio giudiziario dell'Unione* in AA.VV. *Profili del processo penale nella costituzione europea,* Giappichelli, 2005; E. CALVANESE – G. DE AMICIS *Commento alla decisione istitutiva di Eurojust* in *Guida al Diritto,* 2002, 24, pagg. 2-11; E. CALVANESE *Cooperazione giudiziaria tra Stati e trasmissione spontanea di informazioni: condizioni e limiti di utilizzabilità* in *Cassazione penale,* 2003, pagg. 449-462.

[181] Cfr C. M. PAOLUCCI *op.cit.,* pag. 435.

[182] I testi di tutti gli strumenti adottati in materia sono reperibili sul sito http://ec.europa.eu.

Si tratta di un ufficio investigativo del tutto indipendente ed autonomo rispetto alla Commissione europea, ai Governi nazionali e a qualsiasi altra istituzione. Non ha funzioni giurisdizionali né è un organo inquirente, bensì è un organo amministrativo che utilizza gli strumenti tipici delle indagini amministrative, pur verificando situazioni penalmente rilevanti [183].

OLAF può svolgere indagini sia all'interno delle istituzioni comunitarie (cd. indagini interne) sia all'esterno di esse, su tutto il territorio dell'Unione europea e anche in Paesi, previa sottoscrizione di accordi (cd. indagini esterne). Fornisce inoltre assistenza alle autorità giudiziarie nazionali nello svolgimento delle attività d'indagine relative a fatti penalmente rilevanti, ricorrenti nella propria sfera di competenza [184].

L'Ufficio Antifrode ha poteri investigativi nei confronti degli operatori economici, sospettati di irregolarità di bilancio e frodi al bilancio comunitario ed ha poteri d'inchiesta nei confronti dei funzionari delle istituzioni comunitarie per fatti di frode, corruzione e gravi inadempienze professionali[185].

Le indagini sono avviate con decisione del Direttore dell'Ufficio, di propria iniziativa o su richiesta di uno Stato interessato, nel caso di quelle esterne e di propria iniziativa o su richiesta dell'istituzione, dell'organo o organismo a cui dovranno rivolgersi, nel caso di quelle interne. Il Direttore dirige l'esecuzione delle indagini [186].

Poiché l'OLAF opera nella verifica di illeciti penali, ha come interlocutori principali le autorità investigative degli Stati membri con cui coopera e a cui trasmette immediatamente le informazioni raccolte.

L'ulteriore collaborazione con le autorità giudiziarie dei Paesi avviene al termine delle operazioni, al momento della redazione della relazione finale, tenuto conto delle prescrizioni di procedura previste nella legislazione interna dello Stato membro coinvolto[187].

Tali relazioni hanno non solo valenza endo-procedimentale, potendo essere pienamente utilizzate nella fase delle indagini preliminari dal pubblico ministero per l'accertamento delle fattispecie di rilevanza penale, ma anche in senso processuale, potendo essere introdotto al dibattimento [188].

L'OLAF è diventato un tavolo operativo dove pubblici ministeri, ufficiali delle forze di polizia dei Paesi membri e dei Paesi Terzi, funzionari delle dogane e di altri servizi amministrativi si ritrovano per scambiare le

[183] Art. 2 Regolamento 1073/1999.
[184] Cfr C. M. PAOLUCCI *op.cit.,* pag. 437.
[185] Cfr A. PAGOTTO *op.cit.*
[186] Cfr artt. 5 e 6 Regolamento 1073/1999.
[187] Cfr art. 9 Regolamento 1073/1999.
[188] Cfr C. M. PAOLUCCI *op.cit.,* pagg. 440-441.

informazioni, concordare iniziative comuni per combattere fenomeni criminosi che hanno ramificazioni in diversi Stati.

Questo Ufficio interagisce necessariamente con tutte le autorità coinvolte nelle indagini in un determinato caso e con Eurojust.

L'OLAF dispone di limitati strumenti investigativi quali controlli e verifiche, ispezioni preso le sedi di operatori sospetti ma anche di terzi. L'Ufficio può contare sull'assistenza delle autorità locali per superare eventuali resistenze opposte dagli operatori. Nelle indagini interne è di rilievo la facoltà di OLAF di accedere senza preavviso ai locali delle istituzioni nonché ad ogni documentazione ivi presente[189].

Le indagini dell'Ufficio Antifrode, di durata potenzialmente illimitata, devono essere condotte nel pieno rispetto dei diritti dell'uomo e delle libertà fondamentali ed in particolare del principio di equità, del diritto della persona coinvolta a esprimersi sui fatti che lo riguardano e del diritto che la conclusione delle indagini si fondi unicamente su elementi aventi valore probatorio[190].

[189] Cfr A. PERDUCA *Le indagini dell'ufficio europeo per la lotta antifrode (OLAF) ed i rapporti con le autorità giudiziarie* in *Cassazione penale,* 12, 2006, pagg. 4242-4251.
[190] Così il Tribunale di I grado, 6 aprile 2006, causa Manuel Camos Grau c. Commissione europea.

CAPITOLO SECONDO

La prova digitale

SOMMARIO: 1. Ricognizione delle fonti per una nozione comune e comunitaria di prova digitale – 1.1 Il dato come elemento costitutivo della prova digitale – 1.2 Il problema della genuinità – 2. La prova digitale: distinzione tra supporto e contenuto della prova - 3. La direttiva sulla *privacy* e le leggi di attuazione

1. *Ricognizione delle fonti per una nozione comune e comunitaria di prova digitale*

Per ricostruire il concetto di prova digitale, prima ancora di analizzare le fonti normative, è necessario fare un breve *excursus* dell'evoluzione scientifico-tecnologica che ha caratterizzato la Società moderna, specie a partire dalla fine degli Anni Ottanta. Da questo fenomeno ha tratto origine e sviluppo il rapporto di parziale dipendenza tra informatica e diritto [191].

L'uso dei moderni mezzi di comunicazione ha prodotto un aumento considerevole di informazioni e dati in formato digitale: si sta assistendo ad uno storico passaggio alla società dell'informazione, della comunicazione e della digitalizzazione[192].

---

[191] L'interconnessione tra *information and communication technology* e diritto risale ad un periodo posteriore rispetto alla nascita degli *hard disk*, il cui primo è stato prodotto da IBM già nel 1952. La *computer forensics*, però, quale scienza rappresentativa del processo di neovascolarizzazione informatica, si sviluppa appieno contestualmente al progresso degli *home* e *personal computers* e con la diffusione di questi nel tessuto sociale. Più genericamente, il concetto di *digital forensics* (ovvero la scienza che studia il dato digitale), di *network forensics* (ovvero la scienza che si interessa della rete), di *mobile forensics* (ovvero lo studio dei dispositivi mobili) sono frutto di un'evoluzione scientifica e tecnologica i cui studi trovano origine nel contesto statunitense, fra i cui studiosi merita una particolare attenzione l'opera scientifica di E. CASEY *Network traffic as a source of evidence: tool strenghts, weaknesses and future needs in Digital investigation*, 2004, 1, pagg. 28-43; E. CASEY *Digital evidence and computer crime: forensic scienc, computers and the internet, Elsevier*, 2004. Sul tema si veda anche G. ZICCARDI – L. LUPARIA *Investigazione penale e tecnologia informatica*, Giuffré 2007, pagg. 4 ss; R.G. MASSA *Le vere origini della computer forensics in ComputerLaw Informatica e Diritto* all'indirizzo http://www.computerlaw.it/entry.asp?entry_ID=200 (consultato in data 29 maggio 2010).

[192] Il proliferare di tecnologie dell'informazione e della comunicazione e la loro diffusione capillare nel tessuto sociale ha generato un incremento spesso incontrollato di dati ed informazioni. Questo perché le economie globali, se ci riferiamo ai macro sistemi, ma anche gli individui singolarmente intesi sono ormai "dipendenti" (da intendersi non solo in accezione negativa) dai mezzi comunicativi: computer, rete *internet, blog, social network*, VoIP, telefoni cellulari di nuova generazione, tablet e tutto ciò che ogni giorni offre il mercato della tecnologia.

Questa ed altre "rivoluzioni" sociali e tecnologiche[193] hanno portato alla nascita della cd. prova scientifica, fino a pochi anni fa considerata un *novum* nel processo penale, ed oggi divenuta una realtà con cui ogni giorno si confrontano gli operatori del diritto, dal pubblico ministero alla polizia giudiziaria, dal difensore al giudice.

L'avvento della prova scientifica ha creato non pochi problemi applicativi, in conseguenza dello squilibrio tra lo sviluppo delle tecnologie e la lentezza delle risposte legislative. Per prova scientifica, si deve intendere una congerie di operazioni d'indagine innovative e diversificate, nuove quanto al processo di acquisizione, di ammissione, di assunzione e di valutazione, in cui sono utilizzati strumenti propri della scienza e della tecnica, secondo principi e metodologie scientifiche e tecnologiche che richiedono delle competenze specifiche[194].

Questo stato di fatto può costituire un valido strumento per la piena realizzazione di un processo di democratizzazione ma, come nota acutamente Pietro Citrella, esperto di ICT, *"l'uso delle tecnologie della comunicazione può semplificare e favorire i processi democratici ma non li risolve completamente perché sarà comunque necessario utilizzare i tradizionali spazi attraverso cui la vita democratica di un paese si manifesta"*.

La citazione è tratta da S. MARTELLO *Sulla partecipazione e sulla comunicazione nella Rete: riflessioni operative e giuridiche* in *Ciberspazio e Diritto*, 10, 2009, pag. 33, nota 14.

[193] Si pensi, in tal senso, a titolo esemplificativo, alle nuove scoperte in campo medico ed in specie nel campo degli studi genetici, accompagnati parallelamente dallo sviluppo tecnologico e quindi degli strumenti utilizzati

[194] La nozione di prova scientifica qui ricostruita si deve al considerevole lavoro scientifico di O. DOMINIONI *La prova penale scientifica*, Giuffré 2005, pag. 12. Invero l'intero testo è degno di nota e di attenzione per quanto ivi ricostruito e per le problematiche concrete affrontate. La prova esperta, come detto, richiede delle specializzazioni da parte del personale interessato, le cui conoscenze sono poi oggetto di utilizzazione in sede processuale, come già insegna la più risalente esperienza giuridica statunitense, ove si tratta del cd. *expert witness testimony*, quale prova dichiarativa del giudizio. Per un approfondimento in ordine ai problemi di utilizzazione di questo mezzo di prova, si rinvia a A. DONDI *Problemi di utilizzazione di conoscenze esperte, come export witness testimony nell'ordinamento statunitense* in *Riv. Trim. dir. Proc. Civ,* 2001, pagg. 1133 ss.

Ci si limita qui a ricostruire i passaggi essenziali dell'elaborazione statunitense delle regole di ammissione della prova scientifica. Per lungo tempo è stato utilizzato il *commercial marketplace test*, inteso a rilevare il grado di competenza e quindi di affidabilità di un *expert witness*, con il solo riferimento alle qualifiche possedute dall'esperto di cui si procedeva ad escutere testimonianza. Da un salto concettuale tra una visione prospettica di tipo pragmatico ad una epistemologica, nel 1923 la Circuit Court del Distretto di Columbia, nel caso Frye v. United States ha formulato il concetto di *general acceptance test*, per cui il grado di scientificità di un testimone esperto deve essere valutato in base all'approvazione che nella comunità scientifica di riferimento viene dato dell'operato di questi, più in generale subordinando l'affidabilità di una prova ad un consenso in ordine ai principi scientifici applicati, alle tecniche e procedure impiegate, alla funzionalità degli strumenti adottati, al corretto uso delle procedure riconosciute nel campo d'indagine, alla qualifica delle persone impiegate. Il cd. Frye test, però, è entrato presto in crisi, poiché gli operatori del diritto hanno valutato negativamente l'affidamento completo ad un criterio di accettazione che coinvolgesse il solo mondo scientifico , precludendo le valutazioni sull'affidabilità e sulla validità della prova dedotta agli organi giudiziari. La rimeditazione dell'inadeguatezza epistemologica di questo metodo ha avuto seguito anche nella decisione del caso Coppolino v. State (223 So.2d 68, 75 – Fla. Dist. Ct. App. 1969), in cui è stato affrontato in modo particolare il problema legato alla concezione statica ed assolutizzante della scienza,

In questo ampio contesto semantico si inserisce il concetto di prova digitale per la cui acquisizione è necessaria una conoscenza tecnica specifica che trascende il patrimonio cognitivo dell'uomo medio, secondo un'analisi non tanto delle componenti tecniche utilizzate in fase di assunzione bensì del procedimento logico-inferenziale di formazione del libero convincimento del giudice[195]. La cd. *computer forensics*, quale metodo di analisi forense applicabile nelle indagini informatiche, infatti, rappresenta un ambito di studio specialistico, rivolto ad estendere l'applicazione di teorie, principi e prassi della scienza forense al contesto dell'informatica e delle nuove tecnologie, cercando di estrapolare un rapporto di significanza tra il dato contenuto in un supporto informatico o telematico ed il contesto sociale e giuridico [196].

Il ritardo nel mettere a punti i congegni processuali e procedurali mediante i quali rendere praticabili le nuove risorse scientifico-tecniche nella funzione probatoria, con la necessaria affidabilità, rende ancora più complesso il rapporto con la prova digitale, la quale già di per sé è caratterizzata da intrinseca fragilità ed immaterialità della fonte e del dato, che non sempre

---

senza lasciare aperta la possibilità e la via a invalidazioni ed evoluzioni coltivate e coltivabili assieme allo sviluppo di condizioni e fattori scientifici nuovi e diversi con il trascorrere del tempo e lo sviluppo dei saperi. Da qui si sono sviluppati diversi filoni giurisprudenziali di rifiuto di aprioristiche valutazioni positive o negative di metodologie e conoscenze scientifiche applicate, parallelamente all'evoluzione legislativa in materia di prove, fino all'emanazione delle Federal Rules of Evidence nel 1975. Questo testo normativo ha avuto il pregio di elaborare dei criteri di base per il controllo della correttezza epistemologica della prova scientifica, accostando il sapere all'operatività tecnologica, senza chiusure entro i confini di preconcetti. La ricostruzione sintetica di cui sopra non esaurisce la cascata di confutazioni giurisprudenziali del *Frye test*, fino al considerevole punto di svolta intervenuto con la decisione della Suprema Corte Federale nel caso Daubert v. Merrel-Dow Pharmaceutical Inc. (509 U.S. 576 – 1993). Sulla scorta delle ultime innovazioni e scoperte scientifiche, i giudici dell'Alta Corte Federale si sono fatti carico di un nuovo inquadramento ispirato all'empirismo critico, riaffermando la centralità del ruolo del giudice nella valutazione della prova scientifica e definendo criteri generali di ammissibilità di tale prova, sulla scorta dei requisiti già enucleati nelle *Federal Rules of Evidence*. La Suprema Corte Federale statunitense non si è fermata alle affermazioni attestate nella menzionata decisione, infatti la dottrina riconduce le dispute intorno alla prova scientifica ad una trilogia Daubert-Joiner-Kumho ovvero ad un trittico di decisioni che, in un crescendo di chiarificazione e precisione, riproduce un'evoluzione nei metodi di valutazione della scientificità.
Per un approfondimento sul rapporto tra novel science e processo nell'ordinamento statunitense si rinvia a O. DOMINIONI *op. cit*., pagg. 115 ss. Più in generale, quanto all'ampio e dibattuto tema della prova scientifica, si possono annoverare molti lavori scientifici prodotti da autorevoli studiosi, oltre alla già citata opera di Dominioni, tra cui L. DE CATALDO NEUBURGER *La prova scientifica nel processo penale*, Cedam 2007; AA.VV. *Prova penale e metodo scientifico*, Utet, 2009.

[195] Questa impostazione di categorizzazione la si deve a O.DOMINIONI, *op. cit.,* pagg. 38-39. L'Autore precisa che una tale considerazione richiede un approccio di ampio orizzonte verso il fenomeno probatorio, in cui l'angolo visuale si deve aprire ad una nozione di scientificità che considera l'operazione probatoria a tutto tondo, in ogni aspetto del proprio sviluppo e della propria manifestazione nella realtà empirica di cui al *factum probans*.

[196] La nozione di *computer forensics* riportata si deve a Ziccardi in G. ZICCARDI – L. LUPARIA *op. cit.*, pagg. 6-11.

permettono una corretta e completa identificazione della sorgente originaria, a causa del costante e continuo mutamento nel tempo.

Per affrontare in maniera compiuto queste criticità e, contestualmente, apprezzare il valore giuridico e giudiziario della prova digitale, è necessario però fissarne i confini semantici e concettuali individuati nelle fonti del diritto e nella prassi, indagando e ricercandone una definizione che possa essere il più possibile condivisa e comune.

Gli studi scientifici in materia traggono origine dagli Stati Uniti d'America, in particolare dalle assimilazioni e dagli scritti di Casey [197], da cui è possibile trarre spunti di riflessione ed elaborazione di una accurata definizione.

Non esiste, ad oggi, una definizione comunemente riconosciuta di prova digitale, specie per quanto attiene l'ordinamento comunitario e di riflesso gli ordinamenti degli Stati membri.

L'unico dato certo ed incontrovertibile riguarda l'aumento considerevole di *cybercrimes* intesi in senso stretto e in senso lato, quali crimini, rispettivamente, commessi mediante l'uso del mezzo informativo-telematico e crimini agevolati dall'utilizzo degli strumenti di nuova tecnologia.

La dottrina nordamericana si è concentrata sullo studio e sulla ricerca delle caratteristiche proprie di ogni fonte di prova digitale da cui poter giungere, secondo un ragionamento logico-deduttivo, ad una definizione della prova ad esse connessa.

Questa "evidenza" richiede, in prima istanza, un'azione delicata e complessa di *tracing*, ovvero un iter ricostruttivo a ritroso fino ad individuare e riferire un fatto ad una persona nota, superando le possibili anonimizzazioni o sostituzioni di identità da parte dei soggetti agenti. Quindi è necessario circoscrivere e comprendere il fatto compiuto, specialmente mostrando ed analizzando la natura dell'evento dannoso prodotto. A seguire, gli elementi di prova digitale devono essere filtrati con precisione, al fine di circoscrivere le aree di sistema potenzialmente rilevanti ed i dati meritevoli di elaborazione per i fini correlati al *factum probans*. La potenziale prova digitale, così circoscritta, è spesso soggetta a modificazioni e contaminazioni o ad eliminazione, data la natura intrinsecamente fragile che, pertanto, richiede una gestione da parte di soggetti specializzati, mediante l'applicazione delle *best practices* di *computer forensics*.

Per estrapolare una prova digitale da un computer o da un sistema di reti o da qualsiasi altro supporto informatico-telematico, è necessario approcciare allo strumento tecnologico in un'ottica differente, ponendosi nella prospettiva di chi svolge un'attività investigativa che presenta rilevanti differenze rispetto all'operazione usuale ricerca di elementi di prova "fisica".

[197] Cfr E. CASEY *opp. citt.*

A partire dalla ricostruzione di queste procedure d'intervento e recuperando alcuni studi compiuti in seno a gruppi di lavoro negli Stati Uniti, Casey ha sviluppato una definizione di prova digitale secondo la quale questa è "*un qualsiasi dato memorizzato o trasmesso usando un computer che supporta o respinge una teoria su come è avvenuto un fatto offensivo o che individua elementi critici dell'offesa come l'intenzionalità o l'alibi*".

A corollario, lo studioso statunitense richiama anche altre tre diverse (generiche) definizioni: *digital evidence* come un qualsiasi dato che serva a stabilire se un crimine è stato commesso, chi lo ha commesso, che collegamento vi sia tra il crimine e la vittima; *digital evidence* come ogni informazione con un valore probatorio, memorizzata o trasmessa in forma digitale; la prova digitale come l'informazione trasmessa o memorizzata in formato binario ed utilizzabile in giudizio[198].

Secondo Casey, però, queste definizioni sono particolarmente limitative perché sono legate profondamente alla sola valenza probatoria della prova digitale, senza nulla riferire nella prospettiva dell'investigazione.

La definizione principale data dallo studioso nordamericano trova, invece, conferma ed accoglimento in elaborazioni dottrinali italiane in cui, nel più ampio contesto di un'analisi del concetto di *forensic computing*, la prova digitale viene intesa quale "*prova legale ottenuta attraverso sistemi digitali*"[199] e, secondo una visione datocentrica, il dato viene posto come fine ultimo dell'indagine di *computer forensics* in quanto elemento costitutivo dell'evidenza che solo può coadiuvare ovvero portare alla definizione di un fatto di reato [200].

La *section 69* del *Police and Criminal Evidence Act* inglese del 1984, così come modificata dai lavori della *Law Commission* inglese del 1995, collega il concetto di prova informatica ad ogni operazione di memorizzazione di dati da un computer o da altri supporti informatici [201].

Sempre restando nel mondo anglosassone, un intervento normativo rilevante è rappresentato dalle *Maryland Rules of Practice and Procedure*, con particolare riferimento alla *rule 2.504,3,* introdotta a seguito di un intervento della *Court of appeal del Maryland* nel 1998, dedicata specificamente alla *computer generated evidence*. Questa tipologia di prova attiene alla ricostruzione di un avvenimento o di un oggetto derivato da un computer, il cui risultato è

[198] Cfr E. CASEY opp. citt.
[199] Cfr M. MATTIUCCI – G. DELFINIS *Forensic Computing* in *Rassegna dell'Arma dei Carabinieri,* 2006, 2, pag. 54.
[200] In questi termini, conformemente a quanto espresso e sostenuto da Mattiucci e Delfinis, A. GHIRARDINI – G. FAGGIOLI *Computer forensics*, Giuffré, 2007.
[201] Il riferimento è alla regola 1001-3 del Police and Criminal Evidence Act inglese del 1984.

presentato in forma orale, visiva o in una qualsiasi altra modalità sensorialmente percepibile[202].

Non sfugge al legislatore americano che una delle caratteristiche proprie delle prove elettroniche è la volatilità dei dati, connessa alla immaterialità, quindi la modificabilità ed il rischio di dispersione totale dell'evide nza.

L'ordinamento comunitario ed anche i singoli ordinamenti nazionali degli Stati Membri non si sono dotati di una nozione definita e comune di prova digitale, pur utilizzando tale locuzione in più circostanze e pur conoscendone la diffusione, correlata all'incremento dei crimini informatici.

Nemmeno nel testo della Convenzione del Consiglio d'Europa, stipulata a Budapest nel 2001, meglio nota come Convenzione sul *cybercrime*, si trova una definizione di prova digitale.

Eppure la necessità di fornirne una descrizione certa e condivisa non nasce da un mero spirito di concettualismo ma si ricollega a finalità strettamente pratiche. Questa nuova categoria di prove si caratterizza per la presenza di elementi nuovi e diversi rispetto alle tipologie di prova tradizionalmente note agli ordinamenti giuridici moderni degli Stati UE. Pertanto, solo definendo i contorni del concetto di prova digitale è possibile focalizzare l'attenzione sulle disposizioni normative vigenti ad essa applicabili e, allo stesso tempo, individuare i vuoti normativi, ai fini dello sviluppo di una disciplina *ad hoc*, ove necessario.

La Convenzione di Budapest, ponendosi come finalità precipua l'armonizzazione delle legislazioni nazionali e l'avvicinamento tra i singoli ordinamenti, fornisce all'art. 1 la definizione di sistema informatico, di dati informatici, di fornitori di servizi, di dati relativi al traffico, relativi al contenuto e agli abbonati, ma nulla dice con riferimento specifico alla prova digitale. Solo l'art. 14, contenente le disposizioni processuali, fa riferimento alla raccolta di prove in forma elettronica per un qualunque tipo di reato, dando per assunto (o per pleonastica) la nozione di prova digitale.

Diversamente, si trovano dei riferimenti normativi nell'ordinamento comunitario e in quelli nazionali, quanto alla disciplina specifica di molteplici attività ed operazioni tipiche della fase accertativa d'indagine come le ispezioni, perquisizioni, sequestri, intercettazioni, con particolare riferimento all'ambito informatico ed elettronico, le cui risultanze sono definibili come *genera* della *species* prova digitale.

Il Consiglio d'Europa, nello svolgimento della sua attività, si è interessato da lungo tempo alla prevenzione e repressione della criminalità informatica,

[202] Sul punto si rinvia alla lettura di A. TZOUMAS *Maryland sets new standard for computer-generated evidence admissibility in Inside Litigation*, 4, 1998, pagg. 18 ss.; G.R. CARBIN – L. McLAIN *Does computer-generated evidences need its own Rules? Maryland adopts standards for animations simulations in Computer Law Strategist*, 2, 1998.

tanto da creare un Comitato *ad hoc* negli Anni '90, composto da un numero ristretto di esperti in materia di diritto processuale penale e di tecnologie dell'informazione. All'esito dei lavori di questo Comitato è stato preparato il testo della Raccomandazione R(95)13 adottata successivamente dal Comitato dei Ministri del Consiglio d'Europa l'11 settembre 1995. Nel preambolo di questo testo è fatto un chiaro riferimento alla necessità di adattare i mezzi legali a disposizione delle autorità titolari dell'attività d'indagine al carattere specifico delle inchieste svolte su sistemi elettronici e delle attività di raccolta delle prove elettroniche (o prove digitali). Questa Raccomandazione suggeriva[203] ai Paesi membri del Consiglio d'Europa di riformare la legislazione interna per uniformarsi ai principi lì enucleati, specialmente rendendo edotte le Autorità incaricate per le indagini.

Da questo si può desumere con certezza che, almeno dal momento dell'emanazione e divulgazione della menzionata Raccomandazione, gli Stati siano venuti a conoscenza e abbiano così iniziato ad analizzare il problema del contrasto alla criminalità informatica, intesa in senso ampio, oltre ad interrogarsi sul concetto e sulla categoria di prova elettronica o prova digitale.

L'uso continuo ed espanso dei nuovi mezzi di comunicazione elettronica e digitale, diffuso in tutto il tessuto sociale a livello internazionale, ha portato, anche un po' forzosamente, ad una presa d'atto dell'evoluzione generata in materia di criminalità, anche a causa della creazione di infiniti dati e di plurime informazioni in formato elettronico e digitale. Non stupisce, pertanto, trovare dei riferimenti alla prova digitale così nei testi dottrinari come nelle normative interne, comunitarie ed internazionali, negli atti difensivi e dell'accusa e nelle sentenze emesse dall'organo giudicante.

Nonostante ciò, non esiste una definizione codificata di cosa sia una traccia elettronica o informatica e di cosa si debba intendere per prova digitale.

L'approccio digitale alla prova si può distinguere preliminarmente in due processi differenti: la sostituzione della prova tradizionale con una prova in forma digitale; l'introduzione di una prova elettronica addizionale rispetto a quella tradizionale.

La *e-evidence* influenza non solo le procedure dinnanzi alle autorità giudiziarie, ma anche l'architettura delle aule ove si svolgono le udienze, anche

[203] Si vuole qui sottolineare l'adeguatezza del verbo utilizzato, in considerazione del valore non vincolante della Raccomandazione quale fonte del diritto internazionale. Come noto, infatti, le raccomandazioni non sono altro che degli inviti, delle esortazioni, degli ammonimenti rivolti agli Stati senza che da ciò ne derivi alcun obbligo di ottemperanza o adeguamento da parte degli ordinamenti giuridici nazionali. La raccomandazione produce semplicemente un effetto di liceità, ovvero uno Stato che volesse seguire il contegno proposto dal testo dall'organismo internazionale non incorrerebbe in alcuna illiceità anche qualora, facendo ciò, disattenda ad impegni assunti con un precedente accordo oppure ad obblighi derivanti dal diritto internazionale consuetudinario.
Per un approfondimento sul punto si rinvia alla consultazione di testi in materia di diritto internazionale e fra questi si indica B. CONFORTI *Diritto internazionale*, Edizione Scientifica, 2002.

al fine di permettere l'ingresso effettivo di tale forma probatoria. Un motivo dell'incremento della prova digitale è dettato dallo sviluppo dei numero di documenti digitali e dal decremento dei costi per l'archiviazione di quantità di MB di dati[204].

Questo aspetto è tanto più chiaro se si considera che ogni attività compiuta con un qualsiasi supporto informatico o mediante la rete internet è tracciato e registrato.

In base all'analisi dello stato della prassi e del contenuto delle fonti ivi ricostruiti, è possibile delineare un substrato comune e condiviso tra le diverse nozioni ed i vari riferimenti alla *digital evidence,* convenzionalmente si può definire come l'evidenza costituita da informazioni e dati creati, conservati o trasmessi da apparecchiature digitali o nella rete telematica [205].

1.1 Il dato come elemento costitutivo della prova digitale

Dalla ricostruzione del concetto di prova digitale è emersa una visione, per così dire, datocentrica che riconosce il dato come elemento costitutivo di questa tipologia di prova.

Gli studiosi, i tecnici e gli operatori del diritto riconducono l'attività di ricerca di tracce elettroniche al recupero, all'analisi, alla conservazione, alla documentazione e alla validazione di informazioni e di dati informatici, dotati di un fondamento di immaterialità ed alterabilità[206]: il riferimento concreto è all'attività di *computer forensics*, intesa come la materia che si occupa dell'utilizzo di principi, prassi e mezzi tecnici tipici dell'ambito scientifico, al fine di recuperare gli elementi di prova digitale all'interno di un supporto informatico e telematico.

---

[204] Questi rilievi si devono all'intervento effettuato da M. GERCKE in occasione del seminario di studi tenutosi a Barcellona il 27-28 maggio 2011 dal titolo "*The use of new technologies in criminal proceedings*".
Il relatore, inoltre, ha indicato dei dati significativi che attestano inconfutabilmente l'incremento smisurato di produzione di dati in formato elettronico. In particolare, nel 1981 si riscontrava una media di circa 10 MB di dati archiviati, nel 1990 di 676 MB, nel 1996 di 10.000.000 MB, nel 2000 di 70.000.000 MB e nel 2009 di 2.000.000.000 MB.
Sicuramente oggi è molto più economico copiare una quantità ingente di dati in formato digitale, piuttosto che su supporto fisico.

[205] Tale nozione viene qui indicata concordemente con quanto sostenuto da G. COSTABILE *Scena criminis*, *documento informatico e formazione della prova penale* in *Diritto dell'Informazione e dell'Informatica*, 2005, pag. 532.

[206] Conformemente a quanto espresso si vedano le fonti bibliografiche già citate in nota nel paragrafo 1 e, più specificamente, si rinvia alla lettura di S. ATERNO *La computer forensics tra teoria e prassi: elaborazioni dottrinali e strategie processuali*.

L'acquisizione delle impronte elettroniche ha come oggetto principale il flusso dei dati in formato digitale[207]. La prova digitale, come meglio precisato dalla dottrina nordamericana, può riguardare i dati contenuti in un computer statico e quelli presenti in un ambiente dinamico quale la rete.

La Convenzione di Budapest del 2001, all'art. 1, definisce la nozione di *dati informatici* come "*ogni rappresentazione di fatti, di informazioni, di concetti in una forma che si presta a un trattamento informatico, incluso un programma adatto a far sì che un sistema informatico esegua una funzione*".

In questa più ampia e generale cornice semantica s'inseriscono la nozione di *dati relativi al traffico*, quali dati inerenti una comunicazione attraverso un sistema informatico e relativi all'origine, alla destinazione, all'itinerari o, all'ora, alla data, alla misura, alla durata della comunicazione o al tipo di servizio sotteso; nonché la nozione di *dati relativi al contenuto della comunicazione* e di *dati relativi agli abbonati*[208].

Il dato digitale è costituito da una successione di 0 e 1 che, qualora trasferita su una base cartacea, è soggetta ad una operazione di codifica ASCII o di altro tipo. Questa attività è caratterizzata da un procedimento che convenzionalmente associa ad una successione di 0 e 1 un simbolo da riportare su un supporto.

Quando si analizza la *digital evidence* si pone l'attenzione sui dati conservati o trasmessi dalle cosiddette apparecchiature digitali, in base al fenomeno sociale dell'era moderna che ha portato ad un irreversibile passaggio dalla carta ai bits[209].

La Corte di Cassazione penale italiana, in una sentenza risalente al 1999, ha chiarito, in estrema sintesi, il collegamento tra tecnologia informatica, tra dato e informazione, precisando che i supporti informativi di nuova tecnologia sono caratterizzati "*dalla registrazione (o memorizzazione), per mezzo di impulsi elettronici, su supporti adeguati, di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit) numerici (…) in combinazione diversa: tali dati, elaborati automaticamente dalla macchina, generano le informazioni, costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l'utente*"[210].

Il collegamento e l'accostamento dei dati, secondo il volere del soggetto che li genera, determinano il significato di una informazione oppure di una comunicazione.

Secondo la definizione data all'art. 2 della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, in tema di tra ttamento

[207] Si veda L. CUOMO – R. RAZZANTE *La disciplina dei reati informatici*, Giappichelli, 2007.
[208] Il riferimento, per queste definizioni, è all'art. 1 della Convenzione di Budapest.
[209] In questi termini G. COSTABILE *op.cit.*, pag. 532.
[210] Il riferimento è alla sentenza della Corte di Cassazione, 14 dicembre 1999, n. 3067.

dei dati personali e di tutela della vita privata nel settore delle comunicazioni elettroniche, per comunicazione si deve intendere "*ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico*"[211].

In Francia, pur non esistendo una definizione ufficiale di prova elettronica, esiste una definizione dell'aggettivo "digitale" (*numérique*) che spesso viene utilizzato per descrivere anche l'*e-evidence*, presente in un regolamento del 22 dicembre 1981 e che così recita: "in contrapposizione con il termine analogico, questo termine si riferisce alla rappresentazione di dati o quantità fisiche per mezzo di caratteri – generalmente numerici – come di sistemi, supporti o metodi che utilizzano questo mezzo di rappresentazione. Lo stesso testo definisce il dato come una rappresentazione di un'informazione in una forma convenzionale al fine di permettere la facilitazione del trattamento.[212]

Il concetto stesso di prova digitale racchiude in sé una pluralità di forme di rappresentazione, dai dati (come i dati relativi all'indirizzo IP, al mittente, al destinatario, all'oggetto, al dato esterno di traffico, alla data e all'ora di trasmissione, al tempo di trasmissione o di durata della comunicazione, alle celle di geolocalizzazione) ai documenti, dalle immagini alla videoconferenza, dalle intercettazioni ai filmati.

Il primo ostacolo che deve affrontare l'autorità investigativa, in questo coacervo di dati e supporti digitali, è proprio la scelta e il sezionamento soltanto del materiale utile e pertinente.

Indipendentemente dalla forma che può assumere una prova elettronica, quello che interessa è che la prova sia stata raccolta e archiviata ritualmente, sia genuina e dunque utilizzabile nel processo penale ai fini della decisione.

---

[211] L'art. 2 della menzionata Direttiva definisce, assieme al concetto di comunicazione, quello di utente, di dati relativi al traffico, di dati relativi all'ubicazione, di chiamata, di consenso, di servizio a valore aggiunto, di posta elettronica. Questa Direttiva si pone lo scopo espresso al secondo considerando di rispettare i diritti fondamentali, con specifico riferimento alle garanzie offerte dagli art. 7 e 8 della Carta dei Diritti Fondamentali dell'Unione europea, preso atto dello sconvolgimento sociale generato dall'introduzione e sviluppo della rete Internet, fornitrice un'infrastruttura mondiale comune, e dall'accresciuta capacità di memorizzazione e trattamento dei dati delle nuove tecnologie.
Per completezza di definizione, la Direttiva 2002/21/CE del Parlamento europeo e del Consiglio del 7 marzo 2002 che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, all'art. 2 fornisce la definizione della locuzione "servizio di comunicazione elettronica", circoscrivendolo ad ogni servizio fornito a pagamento, consistente esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi servizi di telecomunicazioni e servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva.

[212] Il regolamento del 22 dicembre 1981 è relativo all'arricchimento del vocabolario dell'informatica, pubblicato sul *Journal officiel* in data 17 gennaio 1982 ed è consultabile all'indirizzo internet: http://www.culture.gouv.fr:80/culture/dglf/terminologie/repertoireJO220900/A2200004.htm (consultato in data 28 maggio 2011).

1.2 Il problema della genuinità

Dall'analisi che precede, è emerso che ai fini della ricerca e della raccolta della prova digitale sono necessarie delle competenze e delle conoscenze specifiche in materia di *computer forensics,* proprie del *forenser* e trascendenti il sapere dell'uomo medio.

Non è sufficiente riuscire ad ottenere delle tracce elettroniche ad ogni costo, ma è necessario che i dati raccolti siano utilizzabili in sede processuale perché rispettano la caratteristica dell'integrità, cioè siano privi di indebite alterazioni intervenute in un momento successivo alla creazione, alla trasmissione o all'allocazione di questi su di un supporto autorizzato [213].

Il problema della genuinità della prova si sostanzia nella valutazione dell'*iter* seguito dai tecnici e delle metodologie utilizzate nello svolgimento delle operazioni di ricerca ed acquisizione.

Non esiste nessuna norma che definisca compitamente quali siano le migliori pratiche scientifiche da applicare nelle indagini informatico-telematiche. E' lasciato così aperto un varco di discrezionalità per l'organo giudicante il quale può, entro una cornice ampia e dai contorni fumosi, valutare liberamente la genuinità dei risultati dell'attività di *computer forensics* in riferimento al *thema probandum*[214].

Sia le norme sia la giurisprudenza offrono un riferimento generico alla necessità dell'utilizzo delle metodologie tecnico-scientifiche in grado di garantire la genuinità dei dati raccolti mediante attività di *computer forensics,* senza fornire delle direttive precise sulle *best practices* da applicare da parte dei *computer forensers*.

Già la comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato Economico e Sociale e al Comitato delle Regioni del 26 gennaio 2001, COM(2000) 890 final, relativa al progetto eEurope2002 per la creazione di una Società dell'Informazione più sicura, attraverso l'incremento della sicurezza delle infrastrutture informative e per combattere i crimini

---

[213] La menzionata nozione di "genuinità" è data da G. COSTABILE – D. RASETTI *Scena criminis, tracce informatiche e formazione della prova* in *Ciberspazio e Diritto*, 2003, n. 3/4. Ne accoglie e sostiene il contenuto anche il contributo di A . GHIRARDINI – G. FAGGIOLI *Computer forensics: il panorama giuridico italiano* in *Ciberspazio e Diritto*, 2007, n. 3/4, pagg. 365-366

[214] Sul punto, solo a titolo esemplificativo, si ricordano alcune rilevanti decisioni emessi dai giudici nazionali italiani: Tribunale di Bologna, sentenza del 22 dicembre 2005, ha stabilito che "dal compimento di investigazioni informatiche che si discostano dalla migliore pratica scientifica non discende un'automatica inutilizzabilità del materiale raccolto. Spetta infatti alla difesa l'onere di dimostrare in che modo la metodologia utilizzata ha concretamente alterato i dati ottenuti", conformemente a quanto già sostenuto dai giudici bolognesi in una precedente sentenza del 21 luglio 2005 nel cd. caso Vierika. Rileva in quest'ambito anche la recente sentenza del Tribunale di Vigevano, relativa al famoso caso di Garlasco, del ove i giudicanti hanno valutato molto liberamente le prove digitali raccolte, nonostante i dubbi sorti in relazione alla genuinità delle prove digitali raccolte e assunte in dibattimento.

informatici, al punto 5.6 sottolinea l'importanza che le autorità di *law enforcement* possano ritenere e autenticare i dati informatici a cui hanno accesso e che "*sembrano costituire una prova penale*"[215]. La Commissione rileva la complessità di tale attività, considerata la volatilità, la manipolabilità, la falsificabilità, la distruttibilità dati elettronici. Pertanto, l'invito è quello all'utilizzo di una pratica di intervento che segua i migliori protocolli scientifici dell'attività di *computer forensics*, da applicare nelle procedure di ricerca, analisi e garanzia di autenticità dei dati.

A breve distanza dalla menzionata Comunicazione, è stata firmata la Convenzione di Budapest[216] la quale, ponendo l'accento sulla raccolta ed analisi dei dati informatici, in particolare all'art. 19 rubricato "Ricerca e sequestro di dati informatici", invita gli Stati membri del Consiglio d'Europa, ratificatori della convenzione, a disciplinare le misure necessarie per assicurare la ritenzione dei dati elettronici, acquisirne una copia, mantenerne l'integrità, renderli inaccessibili o rimuoverli dai supporti in cui sono contenuti [217].

La genericità di queste statuizioni permette soltanto di collegare la nozione di genuinità dei dati, e quindi della prova digitale, a quella di integrità degli stessi. L'integrità può essere garantita solo mediante l'impiego di protocolli scientifici specifici da parte dei *computer forensers*.

Non si trova traccia, in ambito europeo, di specifiche indicazioni riguardanti le attività che le autorità sono tenute a seguire al fine di poter attestare, unanimemente ed oggettivamente, l'integrità dei dati e dunque la genuinità della prova e l'utilizzabilità ai fini della decisione.

Dal testo della Convenzione di Budapest ci si attendeva maggiore rigore e completezza poichè, avendo ad oggetto proprio la prevenzione e repressione dei crimini informatici, avrebbe dovuto prevedere dei riferimenti specifici a protocolli d'indagine di *computer forensic*. Invece è stato lasciato questo compito al Legislatore nazionale degli Stati ratificatori, in sede di adeguamento interno alle direttrici segnate dal Consiglio d'Europa nel testo della Convenzione.

Appare chiaro che, così stando, gli organi investigativi sono tenuti ad adoperarsi per acquisire la prova digitale senza modificare il sistema informatico su cui si trovano ad operare; sono tenuti a garantire che la corretta applicazione della *chain of custody* permetta il trasferimento da un supporto all'altro di una copia identica all'originale; devono analizzare i dati senza apportare alcuna alterazione che produca una falsificazione del risultato.

Su questi binari prende le mosse una procedura investigativa in grado di generare una prova elettronica genuina.

---

[215] Il riferimento è al testo in inglese il quale recita: "*law enforcement authorities have accessed computer data which seem to be criminal evidence*".
[216] La Convenzione di Budapest sul cybercrime è stata firmata, infatti, il 23 novembre 2001.
[217] Il testo dell'art. 19 della Convenzione sul *cybercrime* è molto più articolato.

Per dare contenuto a questa necessità è opportuno palesare e rendere vincolanti dei protocolli standardizzati di intervento nelle indagini elettroniche.

Dal punto di vista strettamente operativo, l'attività del *forenser*, sinteticamente individuata, richiede l'individuazione, l'analisi e la valutazione dei flussi in formato digitale. Più compiutamente, le esigenze sottese alle procedure di *computer forensics* riguardano l'acquisizione della prova senza modificare il sistema informatico ove sono inserite; la garanzia nel trasferimento da un supporto all'altro, mantenendo la perfetta uguaglianza rispetto all'originale; l'analisi dei dati senza apportare alcuna alterazione dei contenuti[218].

Le attività investigative in ambito informatico-telematico richiedono la duplicazione bit a bit (cd. *bitstream image*) dell'intero disco rigido del supporto informatico, compresi gli spazi non ancora allocati o apparentemente inutilizzati[219]. Ogni operazione deve essere dettagliatamente verbalizzata ed i dati sono scritti su cd rom o dvd in modalità di sola scrittura, così da evitare che possano subire delle modifiche o delle alterazioni. L'intero processo di acquisizione spesso è filmato per assicurarne la completezza della documentazione. Terminate le operazioni è essenziale predisporre dei locali appositamente adibiti alla conservazione dei reperti elettronici, per proteggerli dall'azione di agenti fisici esterni dannosi.

Nel mondo anglosassone, specie statunitense, ove l'attenzione e la sensibilità in materia di indagini informatiche è decisamente più risalente ed avanzata, è possibile rilevare una previsione dettagliata delle migliori pratiche in materia di indagini informatiche, al fine di oggettivare la distinzione tra prove digitali genuine (ovvero quelle acquisite secondo tali protocolli di intervento) e non genuine.

Gli studiosi degli Stati Uniti sono attenti sia all'introduzione di un criterio oggettivo e metodologico sia all'introduzione di un parametro di valutazione soggettiva. Non è determinante soltanto l'effettuazione di una copia corretta dei dati digitali raccolti, ma è altrettanto utile un controllo delle effettive capacità di chi opera e dei mezzi utilizzati[220]. Proprio sulla base di una valutazione di questi elementi di riferimento, Casey, studioso statunitense, propone una scala di graduazione di certezza della prova che coadiuva l'individuazione dei possibili errori nelle operazioni di *computer forensics*. In

---

[218] La riportata ricostruzione schematica dell'attività di investigazione informatiche e delle esigenze ad essa connesse la si deve a L. CUOMO – R. RAZZANTE *La disciplina dei reati informatici*, Giappichelli, 2007, pagg. 50 ss.

[219] Questo spazio, infatti, spesso contiene un notevole numero di *files* utili ai fini delle indagini, cancellati in precedenza o che non sono stati più sovrascritti. Ancora, possono essere registrati documenti integri, *directory*, *file* temporanei o programmi rilevanti

[220] Cfr E. CASEY *opp.citt.;* G. ZICCARDI *Informatica, comportamenti e diritto*, *op. cit*., pagg. 436-445.

particolare, per prima cosa è necessario considerare i metodi utilizzati dagli investigatori per assicurare l'affidabilità della prova in tal modo raccolta, secondo una *certainty scale*, cioè una graduatoria di certezza che si caratterizza per parametri differenziati secondo il tipo di prova, al fine di mettere in evidenza le possibili fonti di errore che producono, di conseguenza, una non genuinità intrinseca del dato e della prova. In questo contesto è essenziale l'individuazione di protocolli operativi standardizzati, messi in opera dai *forensers* dotati di certificazioni che attestino la specializzazione degli operanti.

Il Gruppo ad Alta Tecnologia del G8 ha elaborato una serie di principi di massima da seguire nell'estrazione di elementi di prova dai sistemi digitali. In primo luogo è necessario minimizzare l'interazione tra i reperti e i non esperti eventualmente presenti sulla scena criminis, utilizzare un buon metodo di reperta mento ed imballaggio, conservare i reperti in luoghi adeguati e documentare qualsiasi fatto anomalo riguardante il trasporto o la detenzione dei reperti; quindi è essenziale che i soggetti che manipolano questi elementi al fine di trarne delle prove siano esperti ed opportunamente formati per lo svolgimento di simili operazioni; da ultimo, bisogna documentare ogni passaggio ed ogni attività compiuta e individuare una persona che, venendo a contatto con i dati acquisiti ed essendo addetto alle analisi di laboratorio, sia indicata come responsabile dell'operazione[221].

Il manuale del Dipartimento di Giustizia degli Stati Uniti d'America, aggiornato per l'ultima volta nel 2002, contiene le linee guida di *search and seizure* e specifica che, in taluni casi, gli operatori devono eseguire una copia di livello fisico o *bitstream image* dell'unità del supporto in analisi ed in altri casi le circostanze richiedono, invece, di procedere al sequestro del computer (o altro supporto) per eseguire un'analisi lontano dal luogo.

Una volta creata un'immagine perfetta del contenuto del supporto informatico in analisi, nell'immediatezza è fatta una copia del *file system* e del contenuto di una partizione logica.

Massima attenzione deve essere dedicata alla catena di custodia (*chain of custody*), ovvero alla metodologia di conservazione e trasporto, sia fisico sia virtuale, delle *digital evidence*[222].

Altrettanto importante è l'attività prodromica di messa in sicurezza dell'ambiente in cui si muovono gli operanti per la ricerca ed acquisizione della prova, essendo necessario procedere all'isolamento totale al fine di evitare

---

[221] Queste linee guida sono riportate da M. MATTIUCCI in *www.marcomattiucci.it/principi.php* (consultato il 3 marzo 2010)

[222] Molti studiosi anche italiani si sono interessati al tema della correttezza ed attenzione nelle operazioni riferite alla catena di custodia. Ex multis, F. BRUGALETTA – F.M. LANDOLFI *Il diritto nel cyberspazio*, Simone, 1999; L. CHIRIZZI *Computer Forensics, il reperimento della fonte di prova informatica*, Laurus Robuffo, 2006.

intrusioni di soggetti persona fisica ma anche contrasti con campi elettromagnetici circostanti.

Di particolare interesse sono anche le linee guida per l'analisi forense elaborate da IACIS, un'associazione di investigatori ed ex investigatori appartenenti alle Forze dell'Ordine.

In esse si precisa che la documentazione delle operazioni di computer forensics dovrebbe comprendere una descrizione fisica e un'annotazione dettagliata di ogni irregolarità, particolarità, mediante l'utilizzo di segni numerici o segni di identificazione; che bisognerebbe evitare l'esame dell'originale del media di prova e che si dovrebbe procedere, invece, ad una preparazione curata di copie per evitare che si verifichi una commistione di dati da casi differenti; che dovrebbe essere sempre tenuta aggiornata una idonea documentazione delle operazioni compiute[223].

Non si deve dimenticare che la disciplina della computer forensics ha origine in ambienti giuridici di *common law* ad alta evoluzione tecnologica come gli Stati Uniti, già nel 1984, quando il laboratorio scientifico dell'FBI e altre agenzie investigative americane iniziarono a sviluppare programmi da utilizzare nell'esame dei dati presenti nei computer. Nello stesso anno, per rispondere alla crescente richiesta di investigazioni in ambito informatico, fu creato, all'interno dell'FBI, il *Computer Analysis and Response Team* (CART) con il compito fondamentale di procedere nei casi in cui si rende necessaria l'analisi di un computer e la Gran Bretagna e ha visto sorgere numerose agenzie specializzate che non solo fornisco servizi di informatica forense ma offrono anche formazione e in qualche caso vendono il *computer forensics tool kit*, valigetta virtuale analoga a quella che l'anatomo-patologo usa per acquisire materiali da utilizzare nelle perizie di medicina legale.

Nel documento *Good Practice Guide for Computer based Electronic Evidence*, elaborato dalla *Association of Chief Police Officers*, si trova una guida elaborata da NHTCU in collaborazione con la *National Hi-Tech Crime Unit for Scotland* e il *Police Service for Northern Ireland* che fornisce interessanti spunti per assicurare pratiche corrette nella raccolta di prove digitali da un computer.

In particolare, in caso di indagini informatiche, gli agenti non devono modificare i dati contenuti sui supporti, deve intervenire soltanto personale esperto, deve essere tenuta traccia di tutti i processi applicati e la persona incaricata ha la responsabilità generale di assicurare la correttezza delle operazioni compiute[224].

---

[223] Per un approfondimento e per i dettagli delle linee guida di computer forensics di IACIS, nonché per visionare l'interessante settore dedicato alle certificazioni, si rinvia al sito internet: www.iacis.com.

[224] Sulle linee guida di computer forensics della Polizia inglese si rinvia a G. ZICCARDI – L. LUPARIA *op.cit.*, pagg. 115 ss.

A livello comunitario, l'E.N.F.S.I. (*European Network of Forensic Science Institute*), sta completando un complesso lavoro di armonizzazione delle procedure d'intervento previste nei singoli Stati finalizzato a migliorare, in termini di attendibilità probatoria, la qualità delle attività scientifiche, specie in sede di sopralluogo giudiziario[225].

Sono note anche le linee guida di computer forensics di cui si è dotato Olaf, per il migliore svolgimento delle attività di raccolta ed archiviazione di dati. In particolare Olaf informa tutti i suoi possibili interlocutori che qualora intervenisse un proprio esperto di computer forensics, costui, oltre ad essere un soggetto formato adeguatamente per lo svolgimento di queste attività, utilizzerà dei *tools* sicuri, sarà in grado di identificare i supporti ed i dati utili, sarà dotato di un kit specifico per queste operazioni e provvederà a fare una copia forense su di un disco di tutti i dati, secondo un codice *hash*. Questi dati raccolti non potranno essere così distrutti o cancellati e ne sarà assicurata l'integrità. Tutto il materiale verrà opportunamente archiviato e identificato mediante dei *keywords* che ne possano permettere la rapida identificazione. È garantita anche la catena di custodia dei dati estratti ed ogni analisi dei dati sarà effettuata non sull'originale ma su una copia della prova originale, proprio per preservarne l'integrità[226].

Dalla lettura delle norme europee e nazionali, dunque, non si riscontrano dei criteri generali e comunemente accolti che fungano da guida per le procedure di *computer forensics*, sebbene quasi tutte le forze di Polizia, gli esperti del mondo accademico, i consulenti e gli esperti informatici si siano dotati di strumenti idonei per l'attività d'indagine informatica.

Quasi tutte le autorità investigative nazionali e plurimi organismi, anche privati, si sono dotati di proprie *best practices* per le operazioni di *forensics*[227].

Questo vuoto normativo è imputabile anche ad uno sviluppo di queste attività avvenuto direttamente sul campo, mediante gli interventi degli addetti

---

[225] L'E.N.F.S.I. è un'organizzazione che riunisce gli istituti forensi europei di rilievo istituzionale e che si pone come principale ed autorevole riferimento per le discipline forensi sia a livello scientifico che a livello organizzativo e gestionale.

[226] Si invita a consultare il sito internet di Olaf: http://ec.europa.eu/anti_fraud/index_it.html.

[227] Quanto all'esperienza italiana si pensa, per esempio alle linee guida predisposte dall'Arma dei Carabinieri, dalla Polizia di Stato, dalla Guardia di Finanza e dal GATT della Guardia di Finanza, dalla Polizia Postale che si è dotata, già dal 1998, di un Nucleo apposito.
Una situazione simile si riscontra anche tra i *Bundeskriminalamt* tedeschi e così anche negli altri Stati europei.
Molto interessante è anche la versione ufficiale della *Good Practice Guide for Computer-Based Electronic Evidence* stilata dalla ACPO, la Polizia del Regno Unito, in collaborazione con *Safe Infromation Security*.
Vi sono aziende di servizi di sicurezza informatica che, fra le altre cose, forniscono anche servizi di *post incident analysis* di informatica forense, atti a fornire un servizio di prevenzione di futuri attacchi o malfunzionamenti, per evitare la perdita di dati rilevanti.

al lavoro, prima della previsione di rigorose regole metodologiche da parte della comunità scientifica[228].

Se da un lato è comprensibile la difficoltà che incontrano i tecnici, nella veste di investigatori informatici, nell'addentrarsi nei meandri del diritto e intendere le esigenze procedurale e processuali, d'altro lato anche il giurista non è in grado di trascendere oltremodo i limiti del proprio sapere e farsi portatore di una conoscenza tecnica avulsa dalla propria inclinazione di studio.

Pertanto è auspicabile che ciascun scienziato si metta a disposizione dell'altro, in un rapporto di interdisciplinarietà, per cercare i giusti bilanciamenti tra scienza e diritto, secondo un binomio sempre più presente (e problematico) negli ordinamenti giuridici moderni.

Lo sviluppo delle nuove tecnologie accresce l'esigenza di prevedere delle regole certe non solo strettamente legate ad un contesto nazionale ma anche applicabili in un ambito di respiro comunitario, in considerazione dell'incentivazione alla cooperazione di polizia e giudiziaria tra gli Stati Membri, per prevenire e reprimere crimini sempre meno legati ad uno spazio territoriale circoscritto[229].

Accanto alla *computer forensics*, a partire dagli anni Novanta, si è sviluppata sempre più la sensibilità verso la *computer ethics*, intesa come l'etica professionale volta allo sviluppo e all'avanzamento dello standard di buona pratica e dei codici di condotta per i professionisti del la materia[230].

Nonostante questo interesse verso la definizione di uno sforzo etico-professionale da parte degli operanti in ambito informatico-telematico, la lacuna generata dall'assenza di protocolli comunitari standardizzati di intervento fa in modo che i soggetti demandati allo svolgimento di queste attività si affidano sempre e solo sulle proprie conoscenze scientifiche e professionali[231].

La fase tecnica di *computer forensics* comprende delle operazioni di particolare delicatezza ed insieme di estrema rilevanza in ambito giuridico e giudiziario, riconducibili ad una serie di attività che iniziano dall'acquisizione del supporto, all'analisi dello stesso[232] e anche all'esposizione dei risultati

---

[228] Sul punto si concorda con quanto sostenuto da G. PALMER *Forensics Analysis in a Digital World* in *htttp://ijde.org/archives/gary_article.html"*; E. CASEY *opp.citt*.

[229] Quanto all'incremento della criminalità internazionale e transnazionale si rinvia alla lettura del cap. I e lo stesso vale a dirsi quanto all'incentivazione alla cooperazione di polizia e giudiziaria tra gli Stati Membri dell'Unione Europea, come indotto rispetto al mutato panorama di criminalità.

[230] Per un approfondimento in materia di *computer ethics* si invita alla lettura di G. ZICCARDI *Informatica, comportamenti e diritto: dalla computer ethics alla computer forensics* in *Ciberspazio e Diritto*, n. 4, 2008, pagg. 395-445; M. DURANTE *Il futuro del web: etica, diritto, decentramento,* Giappichelli, 2007.

[231] In questi termini si esprime L. CHIRIZZI *op.cit*., pagg. 464-465.

[232] L'analisi dei dati digitali raccolti, oltre ad essere un'operazione necessaria ai fini dell'effettivo utilizzo dei contenuti ed anche prodromica ad una successiva esplicazione scritta o orale di quanto

raggiunti: la disponibilità e lo studio del fascicolo e di tutti i suoi contenuti (compresi i dati digitali) è un elemento altrettanto importante dell'attività d'indagine informatica. Non di meno è importante soffermare l'attenzione, anche al fine di una futura e auspicabile regolamentazione, sulle operazioni di rimozione e spostamento dei supporti in cui sono contenuti dei dati digitali considerati rilevanti ai fini delle indagini, come altresì sull'attività di distruzione totale e definitiva di quanto non pertinente, non rilevante, acquisito illegalmente o illegittimamente o non utilizzabile.

Il problema della genuinità della prova digitale non è di poco conto se visto nel contesto di un incremento dei processi ove questa tipologia di prova entra a far parte del giudizio, rivestendo spesso un ruolo determinante ai fini dell'indagine prima e della conclusione del processo poi.

Finché permarrà un generale stato di incertezza intorno alla prova elettronica si potrà andare incontro a esiti processuali falsati o comunque diversi da quelli che si potrebbero ottenere in un clima di certezza delle operazioni di indagine istruttoria[233].

È auspicabile almeno la sola previsione di protocolli d'indagine informatica a livello di regole generali poiché, invero, ogni scena del crimine ed ogni supporto informatico richiede un approccio specifico e differenziato che i tecnici, dunque, devono avere l'accortezza di conoscere e sviluppare.

2. *La prova digitale: distinzione tra supporto e contenuto della prova*

La ricostruzione ed analisi della definizione di prova digitale ha fatto emergere la stretta connessione che lega questa al dato, come suo elemento costitutivo. È risultato altresì che il dato elettronico e, più nello specifico, i dati combinati ed accostati secondo un certo ordine, producono il risultato di una comunicazione e/o di una informazione.

---

raccolto e dei risultati raggiunti, è anche utile al fine di valutare se vi siano state delle forme di alterazione o manipolazione. Si sta infatti diffondendo, per esempio, specie negli Stati Uniti d'America, una pratica illegale connessa alla manipolazione dei fotogrammi , attraverso una ricombinazione delle immagini e dei segmenti sonori in uno spazio morfologico (*morph space*) ad alta dimensione, attraverso il semplice uso di programmi e software di un personal computer. L'utilizzo di queste pratica può portare alla falsificazione anche di fonti o elementi di prova digitale sebbene le non ancora sofisticate tecnologie applicabili renda più facilmente riconoscibile la "non genuinità".
Per un approfondimento sul tema si invita alla lettura di L. LEONE *La manipolazione digitale dei fotogrammi* in *Ciberspazio e Diritto*, n. 3/4, 2007, pagg. 289-308.

[233] Il timore di un sempre maggiore allontanamento dalla tensione alla verità processuale che può ancor più facilmente concretizzarsi per le incertezze delle operazioni di computer forensics è condiviso con A. GHIRARDINI – G. FAGGIOLI *op.cit.*, pag. 381.

I dati digitali sono, per definizioni, degli elementi immateriali (e per tali motivo volatili, fuggevoli e mutevoli) che possono essere appresi su di un supporto ovvero possono essere trasferiti da un supporto all'altro secondo le procedure di *computer forensics*.

Da un punto di vista strettamente tecnico-operativo, tra le principali attività compiute nella fase delle indagini informatiche si annoverano i sequestri, la copia delle informazioni e l'intercettazione di flusso.

L'investigatore può, se necessario e rilevante ai fini delle indagini, sequestrare, cioè prendere fisicamente il supporto su cui risiede il dato oppure può limitarsi ad eseguire una copia attraverso la quale il supporto originale viene acquisito indirettamente, sottoforma di duplicazione dei dati ivi contenuti, per essere poi riportati su di un altro e diverso supporto.

Ancora, è possibile che sia eseguita un'intercettazione del flusso di informazioni elettroniche e telematiche durante la trasmissione tra due sistemi. La lettura e l'analisi delle informazioni così acquisite non avviene, dunque, dal supporto di memorizzazione dove il dato risiede ma direttamente dal *medium* utilizzato per i flussi.

Si consideri anche che, in una ipotetica *scena criminis*, è possibile venire in contatto con una pluralità di supporti informatico-telematici, a volte difficili da vedere e riconoscere perché nascosti o confusi in involucri fuorvianti [234].

Il proliferare di *devices* crea prima ancora che un problema di gestione di una quantità di dati, anche un problema di formazione tecnica specifica degli esperti che intervengono [235].

Emerge così chiaramente la distinzione tra il dato ed il supporto che lo contiene.

Anche il trattamento di un computer o di un qualsiasi *device* elettronico è di estrema importanza per garantire che le informazioni ivi estrapolate siano genuine.

Secondo Casey, nel caso per esempio di un'indagine riguardante un *personal computer* è auspicabile procedere nel seguente modo:

---

[234] Si pensi, per esempio, che una chiavetta USB si può nascondere dentro un portachiavi o in un gioiello

[235] Sono gli stessi forenser ad insegnare che le procedure di intervento da seguire per garantire la genuinità dei dati raccolti, dipendono molto dal device su cui si opera.
A titolo esemplificativo, si rinvia a M. EPIFANI *Analisi di telefoni cellulari in ambito giuridico* in *Ciberspazio e Diritto*, vol. 10, 2009, pagg. 83-98; A. GHIRARDINI – G. FAGGIOLI *Computer forensics: il panorama giuridico italiano* in *Ciberspazio e Diritto,* n. 3-4, 2007, pagg. 324-384; C. AQUILA *La computer forensics aziendale: alcune problematiche preliminari* in *Ciberspazio e Diritto*, n. 2, 2008, pagg. 123-131.
In questo stesso contesto, l'ulteriore problematiche è legata proprio alla ricerca di percorsi di formazione ad hoc per i *forenser*. Sul punto si rinvia a M. EPIFANI *Computer forensics: percorsi formativi in Italia e certificazioni internazionali* in *Ciberspazio e Diritto*, n. 3-4, 2009, pagg. 311-324.

1. staccare dal computer i cavi di rete e il modem ed eventualmente verificare se vi siano delle connessioni attive;
2. fotografare il supporto ed il contesto di quanto lo circonda;
3. verificare se vi siano delle impronte digitali;
4. se il computer è acceso, è utile registrare le informazioni di sistema non solo del pc ma anche dei supporti collegati;
5. spegnere il computer.

Sempre secondo la ricostruzione di Casey, nei casi di sequestro del materiale informatico, è necessario etichettare i cavi e le porte, mettere un disco di protezione in ogni drive, impacchettare tutto, sigillare ed evitare l'esposizione ad agenti dannosi.

Ogni dispositivo deve essere trattato dall'investigatore in modo specifico e differenziato, secondo la miglior prassi della scienza che ogni tecnico deve conoscere ed approfondire.

L'attività di *computer forensics* pone l'accento anche sulla nozione di documento informatico, da intendere come la rappresentazione di atti, fatti e dati rilevanti in ambito giuridico.

Il supporto contenente quei dati digitali, idonei a divenire prova nel processo penale, diviene così oggetto di interesse e di studio.

Il documento informatico è sicuramente il supporto più diffuso ove risiedono e vengono riprodotti i dati digitali, ma non è certo l'unico.

La nozione di documento informatico ha influenzato la teoria generale nazionale del documento e ha richiesto una rivalutazione delle normative sulla base del contenuto garantista del principio del giusto processo, riconosciuto e tutelato dall'art. 6 Convenzione Europea dei Diritti dell'Uomo, recepito nelle normative nazionali almeno dagli Stati membri dell'Unione europea.

Il punto di partenza è rappresentato da una generale e tradizionale definizione di documento come supporto fisico (nozione mutuata dall'ambito civile) in cui risiede il dato digitale, oggetto rilevante per i fini della giustizia penale.

La tendenza attuale è alla parificazione dell'informatica alla scrittura, assimilando così il documento digitale al documento scritto, entrambi quali mezzi di rappresentazione di fatti, persone o qualsiasi altra cosa.

Più precisamente e nello specifico, il documento non solo rappresenta un qualcosa ma incorpora in sé un elemento immateriale (il dato) su di una base materiale. Ciò che viene inserito su di un supporto è una rappresentazione sottoforma di parole, immagini, suoni o gesti. Quando tale attività è compiuta con il metodo digitale e su di un supporto informatico, allora siamo di fronte ad un documento informatico, nelle altre ipotesi siamo di fronte ad documento, come tradizionalmente noto.

Una rappresentazione, dunque, potrà avvenire con uno scritto o con un *file*; il file, a sua volta, potrà risiedere su di un CD, su di un *pen drive* ovvero su di un altro e diverso supporto, pur non modificandosi il contenuto. L'unica differenza che sussiste tra una forma di incorporamento analogico ed una digitale si sostanzia nel fatto che nel primo caso ha luogo un incorporamento materiale, in cui la rappresentazione non esiste senza il suo supporto fisico; nel secondo caso, invece, l'incorporamento è immateriale poiché la rappresentazione esiste indipendentemente dal supporto informatico scelto, facilmente trasferibile dall'uno all'altro. Da questo si comprende meglio il motivo per cui il dato digitale è caratterizzato dalla fragilità.

L'attività d'indagine informatica, volta alla conservazione della genuinità del dato ricercato ed acquisito, si caratterizza, tra le altre operazioni, per l'esecuzione di una copia *bit* per *bit* della memoria del supporto informatico in analisi. I *files* così acquisiti sono trasferiti su di un certo supporto, quale un cd-rom o un dvd-rom completamente libero, al fine di ricreare le condizioni di partenza. I supporti sono fruibili in modalità di sola lettura e pertanto non permettono che i contenuti che vi risiedono possano subire alterazioni e modificazioni. Questo perché i casi in cui è legittimo procedere al sequestro di un intero supporto informatico sono eccezionali: oltrepassando questo limite, si rischia di incorrere in un'attività oltremodo invasiva e passibile di sanzioni per violazione di diritti fondamentali dell'individuo.

Sussiste, dunque, un *favor* verso l'attività di assicurazione delle prove informatiche avente ad oggetto non tanto il contenitore, quanto il contenuto di informazioni e dati, i quali formano il vero oggetto di prova digitale.

Il supporto può essere un elemento di prova determinante nei casi in cui è utilizzato unicamente o comunque in maniera principale per compiere delle attività illecite, viceversa rappresenta solo un mezzo materiale ove vengono creati, risiedono e possono essere trasferiti i dati digitali che interessano ai fini delle indagini.

L'ablazione del bene è giustificata dalla necessità di cristallizzare la condotta e fornire un'approfondita descrizione tecnica, di preservare l'organizzazione logica dei dati, di evitare la dispersione dei dati e delle informazioni per estrema volatilità, nonché per ragioni di urgenza di estrazione della copia del disco rigido al fine della prosecuzione rapida delle indagini, oltre che per l'espletamento di altre analisi tecniche d'ufficio o di parte.

Questo perché deve essere contemporaneamente tutelato il diritto alla proprietà privata dell'individuo che potrebbe risultare leso mediante le operazioni indiscriminate di sequestro dei supporti informatici.

Il supporto su cui risiede un dato digitale può, in taluni casi, rappresentare una chiave di volta per le indagini se, dall'analisi, si possa coadiuvare le operazioni di acquisizione di conoscenza sui fatti o sul soggetto

agente, ovvero si possano rilevare tracce o effetti del reato per cui si procede, mediante la procedura dell'ispezione.

Lo strumento fisico in cui sono appresi i dati e le informazione acquisisce un ruolo essenziale nelle procedure di intercettazione: per captare un flusso di dati tra o di sistemi informatici o telematici, coperto dalla segretezza e riservatezza, è necessario l'impiego di un supporto tecnologico adatto che, dunque, diventa il mezzo essenziale per acquisire le comunicazioni *bit a bit*. In particolare, nelle intercettazioni telematiche sono impiegati degli apparecchi tecnologici specifici, in grado di cogliere gli impulsi elettronici non immediatamente comprensibili e convertirli in una forma intellegibile.

3. *La direttiva sulla privacy e le leggi di attuazione*

La *privacy* è un concetto tanto nebuloso quanto metamorfico, flessibile e modificabile anche in base alle esigenze del progresso tecnologico e del mutato contesto di garanzia rivendicata.

Il diritto alla *privacy* è stato definito , fin dai primordi, "*right to be let alone*"[236] e, ad oggi, si è tanto diffuso fino a inglobare nuovi e diversi significati che abbracciano, tra l'altro, la possibilità del singolo di conoscere, controllare, indirizzare ed interrompere il flusso di informazioni che lo riguardano. Queste ulteriori esigenze di tutela sono state ravvisate, in particolare, per l'avvento delle nuove tecnologie in campo biomedico, in considerazione del carattere di dato sensibile riferibile ad ogni informazione di natura genetica acquisita con l'uso di tali mezzi.

Nuovi interrogativi sul contenuto del diritto alla *privacy* sono sorti anche a causa delle allarmanti minacce terroristiche che preoccupano e sensibilizzano l'intero globo. In particolare, si è reso (e si rende) necessario valutare quale possa essere il giusto equilibrio tra due opposte esigenze: il rispetto del diritto alla riservatezza da un lato e la necessità di tutelare l'incolumità e la sicurezza della collettività dall'altro lato[237].

---

[236] La nota definizione è frutto degli studi degli americani Warren e Brandeis ai quali va riconosciuto il merito di aver prodotto il primo vero scritto di teoria generale della tutela della provaci già sul finire del secolo XIX.
Cfr S.D. WARREN – L.D. BRANDEIS *The right to privacy* in *Harvard Law Review,* n. 4, 1890, pagg. 193 ss.
Questo pamphlet si contraddistingue per avere innovato il concetto di *diritto alla privacy,* passando da un pensiero che legava strettamente tale diritto al diritto alla proprietà privata per giungere, invece, ad un nucleo centrale portato sull'idea dell'inviolabilità dei diritti della personalità.

[237] Lo sforzo concettuale volto ad una ricostruzione ed introduzione ai problemi legati al diritto alla privacy si devono a C. SARTORETTI *Contributo allo studio del diritto alla privacy nell'ordinamento costituzionale. Riflessioni sul modello francese,* Giappichelli, 2008, pagg. 7 ss.; U. PAGALLO *La tutela della privacy negli Stati Uniti d'America e in Europa,* Giuffré, 2008, pagg. 109-156.

La forte dinamicità della *privacy* non permette di circoscrivere e cristallizzare una formula e una definizione, proprio perché gli sviluppi tecnologici che caratterizzano giornalmente la nostra epoca incidono sulle dinamiche della riservatezza creando delle situazioni giuridiche nuove [238].

La pluralità contenutistica di questo concetto ha portato la dottrina a ritenere che la *privacy* non costituisca un diritto singolo ed autonomo, bensì una costellazione di diritti[239], per questo refrattaria ad un qualsiasi congelamento in carte costituzionali o documenti normativi statici.

La nozione di *privacy* è il prodotto del sentire socio-culturale dell'epoca contemporanea e degli sviluppi del sapere e delle scienze, da collocare sempre nel contesto storico specifico di riferimento.

In una società civile come quella odierna, caratterizzata dalla crisi della territorialità dello Stato, i problemi e le soluzioni acquisiscono una dimensione sovranazionale.

Ciò vale anche per il catalogo dei diritti e, in particolare, per il diritto alla *privacy*.

Nella Carta dei Diritti dell'Unione europea, già nel Preambolo si legge che l'Unione europea "*si basa sui principi di democrazia e dello stato di diritto*", e "*pone la persona al centro della sua azione*" creando "*uno spazio di libertà, sicurezza e giustizia*" ove vengono tutelati in particolare i diritti "*derivanti in particolare dalle tradizioni costituzionali e dagli obblighi internazionali comuni agli Stati membri, dal Trattato dell'Unione europea e dai trattati comunitari, dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, dalle carte sociali adottate dalla Comunità e dal Consiglio d'Europa, nonché i diritti riconosciuti dalla giurisprudenza della Corte di giustizia delle Comunità europee e da quella della Corte europea dei diritti dell'uomo*".

In questo contesto di garanzie s'inserisce anche il diritto alla *privacy* che, tra i molteplici aspetti, si caratterizza per il *data protection,* da intendersi come tutela del diritto all'*habeas data*[240].

La *privacy*, quale proiezione del nucleo sensibile e della sfera esclusivamente personale e indisponibile dell'individuo [241], è da lungo tempo al

---

[238] La bibliografia in materia di privacy è molto vasta, proprio per via della trasversalità della materia che tocca molti rami del diritto, dal diritto costituzionale al diritto civile, il diritto penale ed il diritto dell'Unione europea.
Si segnalano, *ex multis:* S. RODOTA' *Tecnologie e diritti,* Il Mulino, 1996; A. CERRI *Riservatezza (voce)* in *Enciclopedia Giuridica Treccani,* Istituto Poligrafico e Zecca dello Stato, 1991; P. CONTI (a cura di) *Intervista su privacy e libertà,* Laterza, 2005

[239] L'espressione riportata è di F. MODUGNO *I "nuovi" diritti nella Giurisprudenza costituzionale,* Giappichelli, 1995, pag. 20.

[240] Cfr C. SARTORETTI *op.cit.*, pag. 21.

[241] In questi termini si esprime A. FERRARA *Premesse ad uno studio sulle banche dati della pubblica amministrazione: fra regole della concorrenza e tutela della persona* in *Diritto amministrativo,* 1997, pagg. 555 ss.

centro della tutela da parte della Comunità, in particolare a partire dalla Direttiva 95/46/CE del 24 ottobre 1995, in materia di trattamento dei dati personali e libera circolazione[242].

Come si legge nel Preambolo, la Direttiva nasce da una presa di coscienza del notevole incremento del trattamento e dello scambio dei dati, a motivo del continuo progresso delle tecnologie; nonché dalla presa d'atto dell'agevolazione del flusso transfrontaliero dei dati personali attuato mediante l'integrazione economica e sociale di cui all'art. 7A del Trattato UE.

Nel *considerandum 8,* in particolare, è enucleata la *rat*io dell'intera Direttiva secondo cui, per eliminare gli ostacoli alla circolazione dei dati personali, è necessario riconoscere un livello di tutela dei diritti e delle libertà delle persone relativamente al trattamento dei dati personali equivalente in tutti gli Stati, che può trovare attuazione solo mediante un intervento della Comunità volto al ravvicinamento delle legislazioni nazionali[243].

La Direttiva si ispira, come esplicitato, sia all'art. 7A del Trattato, sia all'art. 8 Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, sia alla Convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale[244].

La Direttiva *privacy* è applicabile al trattamento di tutti i dati personali, anche quelli in forma di suoni e immagini, relativi a persone fisiche, compiuto parzialmente o interamente mediante l'uso di mezzi automatizzati ovvero senza l'uso di tali mezzi ma riguardante dati personali contenuti o destinati a figurare in archivi[245].

I "*dati personali*" sono tutte le informazioni concernenti una persona fisica identificata o identificabile, direttamente o indirettamente, in particolare mediante il riferimento ad uno o più elementi specifici e caratteristici. Per "trattamento dei dati" si intende ogni operazione svolta con o senza l'ausilio di mezzi automatizzati, applicata ai dati personali quali la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto, l'interconnessione, il congelamento, la cancellazione, la distruzione. Un "*archivio di dati personali*" è

---

[242] La cd. Direttiva Privacy è stata pubblica in Gazzetta Ufficiale CE n. 281 del 23 novembre 1995, impegnando gli Stati Membri, quali destinatari del testo, a recepirla mediante la previsione di disposizioni legislative, regolamentari ed amministrative necessarie per conformar visi, al più tardi nel terzo anno successivo all'adozione (art. 32 Direttiva).

[243] L'obiettivo, dunque, non è solo quello di approntare un livello minimo di protezione individuale ma, come ben esposto dalla Corte europea di giustizia sin dal caso Lindqvist del 2003, di garantire in questo modo una tutela generale della privacy.
Il menzionato caso Lindqvist è stato deciso il 6 novembre 2003, causa C-101/01.

[244] In particolare, il riferimento esplicito ai menzionati testi è fatto nei *consideranda* 8, 10 e 11.

[245] Si vedano, in particolare, i *consideranda 12, 14, 15* nonché l'art. 3 rubricato "Campo d'applicazione".

un insieme strutturato di dati personali accessibili, secondo criteri determinati, indipendentemente dal fatto che sia organizzato mediante un sistema centralizzato, decentralizzato o ripartito in modo funzionale o geografico [246].

L'art. 7, inserito nella sezione dei principi relativi alla legittimazione dei dati, specifica che "*Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando: a)la persona interessata ha manifestato il proprio consenso in maniera inequivocabile; b)è necessario per l'esecuzione del contratto concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta di tale persona; c)è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento; d)è necessario per la salvaguardia dell'interesse vitale della persona interessata; e)è necessario per l'esecuzione di un compito d'interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati; f)è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata*".

L'art. 13 concede la previsione di deroghe e di restrizioni da parte degli Stati membri per motivi di sicurezza dello Stato, di difesa, di pubblica sicurezza, di prevenzione, ricerca, accertamento e perseguimento di infrazioni penali o di violazioni della deontologia professionale, per un rilevante interesse economico o finanziario di uno Stato o dell'Unione europea, per operazioni di controllo, ispezione *et similia.*

L'art. 17 si concentra sul tema della sicurezza nel trattamento dei dati che deve essere offerta con un livello appropriato da parte degli Stati, anche in considerazione della natura dei dati da proteggere da distruzione, perdita, alterazione, illecita diffusione, accessi non giustificati, specie nelle ipotesi di trasferimento all'interno di una rete ma non solo.

In base al disposto dell'art. 20, gli Stati membri sono tenuti a precisare i trattamenti di dati che presentano particolari rischi per i diritti e le libertà degli individui, prevedendo per questi dei controlli preliminari prima della messa in opera[247].

La Direttiva del 1995 è stata oggetto di modifica ed integrazione in una successiva Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, sempre relativa al trattamento dei dati personali e alla tutela della vita privata, ma specificamente dedicata al settore delle comunicazioni

[246] L'art. 2 della Direttiva enuclea le riportate definizioni, oltre alla definizioni di "*responsabile del trattamento*", di "*incaricato del trattamento*", di "*terzi*", di "*destinatario*" e di "*consenso della persona interessata*".

[247] All'art. 20 si precisa che tale esame preliminare è effettuato dall'autorità di controllo a seguito della notifica del responsabile del trattamento o della persona incaricata della protezione dei dati, previa consultazione dell'autorità di controllo.

elettroniche[248]. La *ratio* anche di questa Direttiva attiene alla volontà di armonizzazione delle disposizioni legislative, regolamentari e amministrative degli Stati membri proprio in materia di tutela dei dati personali e della vita privata[249].

La Direttiva del 2002 si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico perché appoggiati su reti pubbliche[250].

In particolare, il Parlamento ed il Consiglio richiedono ai fornitori di servizi di comunicazione elettronica accessibili al pubblico di adottare le misure tecniche idonee per garantire la sicurezza dell'utente della rete, secondo il livello offerto dallo stato dell'arte in rapporto alle esigenze riscontrate in ogni diverso contesto[251].

I dati interessati dall'applicazione di questa Direttiva sono i dati di traffico, i dati relativi all'ubicazione, i dati relativi all'identificazione della linea chiamante e collegata, nonché l'elenco degli abbonati[252].

La Direttiva del 2002 è stata oggetto di modifica per il tramite della Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione[253].

Nel *considerandum 6* della Direttiva del 2006 è esplicitata la presa d'atto di una realtà giuridica europea in cui sussistono delle differenze teoriche e tecniche tra le disposizioni nazionali relative alla conservazione dei dati ai fini della prevenzione, dell'indagine, dell'accertamento e del perseguimento dei reati, ciò determinando un ostacolo al libero mercato delle comunicazioni elettroniche, giacché ogni fornitore è tenuto a salvaguardare, conservare e trattare i dati secondo dei livelli obbligatori di tutela molto differenti.

Già il Consiglio Giustizia e affari interni del 19 dicembre 2002 aveva concluso sottolineando il considerevole aumento delle possibilità di comunicazioni elettroniche, i cui dati ad esse afferenti costituiscono uno

---

[248] La Direttiva è stata pubblicata in Gazzetta Ufficiale CE del 31 luglio 2002.

[249] Il riferimento, in particolare è al *considerandum 8* e all'art. 1 rubricato "*Finalità e campo d'applicazione*".

[250] In questi termini l'art. 3 della Direttiva 2002/58/CE rubricato "*Servizi interessati*".

[251] Il riferimento è all'art. 4 della Direttiva rubricato "*Sicurezza*". Tale articolo precisa, altresì, che qualora esistano dei rischi particolari di violazione della sicurezza della rete, il gestore ha l'obbligo di informare chiaramente l'utente indicando che tali rischi sono fuori dal campo delle applicazioni delle misure adottate.

[252] Il testo della Direttiva fornisce una definizione chiara dei diversi tipi di dati in particolare all'art. 2. Nel corpo centrale, poi, si trovano le disposizioni specifiche riferite ai dati di traffico (art. 6), all'identificazione della linea chiamata e collegata (art. 8), ai dati relativi all'ubicazione (art. 9), all'elenco degli abbonati (art. 12).

[253] La Direttiva 2006/24/CE è stata pubblicata in Gazzetta Ufficiale CE in data 13 aprile 2006.

strumento importante per la prevenzione, indagine, accertamento e perseguimento dei reati, in particolare della criminalità organizzata [254].

La necessità di armonizzare le misure sulla conservazione dei dati relativi alle telecomunicazioni è stata ancora più sentita in seguito agli attacchi terroristici di Londra, come ribadito anche dal Consiglio nella seduta del 13 luglio 2005[255].

L'art. 5, elencando le categorie di dati da conservare, fa riferimento specifico alle seguenti: i dati necessari per rintracciare ed identificare la fonte di una comunicazione, quali il numero telefonico chiamante, nome e indirizzo dell'abbonato o dell'utente registrato ovvero il suo identificativo, l'assegnazione dell'indirizzo di protocollo Internet (IP); i dati necessari per rintracciare e identificare la destinazione di una comunicazione, quali il numero digitato o chiamato, l'eventuale uso dei servizi di inoltro o trasferimento di chiamata ed i numeri a cui la chiamata è trasmessa, nome e indirizzo dell'abbonato o dell'utente registrato, identificativi dell'utente o numero telefonico del presunto destinatario (sia essa una chiamata telefonica o Internet); i dati necessari per determinare la data, l'ora e la durata di una comunicazione, compresi i dati di *log-in* e *log-off*; i dati necessari per determinare il tipo di comunicazione; i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le attrezzature utilizzate; i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile, quali il Cell ID (o etichetta di comunicazione iniziale).

Sono esclusi dall'applicazione della Direttiva del 2006 i dati relativi al contenuto delle comunicazioni[256].

Tutti questi dati, una volta raccolti, possono essere trasferiti alle autorità competenti su loro richiesta[257].

Tali dati, inoltre, secondo l'art. 7, devono essere conservati secondo elevati standard di sicurezza, mediante l'utilizzo di adeguate strumentazioni tecniche e di un'organizzazione che possano limitare il più possibile i rischi di distruzione, alterazione, perdita, accesso e divulgazione illeciti e non autorizzati[258].

---

[254] Le riportate conclusioni del Consiglio Giustizia e affari interni del 19 dicembre 2002 sono riassunte nel *considerandum 7* della Direttiva 2006/24/CE.

[255] Ciò è ribadito anche nella Direttiva 2006/24/CE al *considerandum 10*.

[256] Il riferimento è all'art. 5 nella sua completezza di contenuto, ove viene fatta un'elencazione dettagliata delle diverse categorie di dati. Nel successivo art. 6 è esplicitato che tali dati debbano essere conservati per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione. Secondo il disposto dell'art. 9, ogni Stato designa una o più autorità pubbliche di controllo dell'applicazione della Direttiva del 2006.

[257] Cfr art. 8 Direttiva 2006/24/CE.

[258] L'art. 15 della Direttiva prevedeva espressamente la data del 15 settembre 2007 quale termine ultimo per il recepimento. Alcuni Stati hanno da subito presentato delle dichiarazioni per chiedere una proroga:

Le leggi nazionali europee, con particolare riferimento agli ordinamenti italiano, francese e tedesco, hanno recepito la normativa comunitaria in maniera sostanzialmente comune, salvo alcune peculiarità di ciascun modello ordina mentale.

In Italia il diritto alla *privacy* è stato per lungo tempo misconosciuto, almeno a livello normativo, se non dalla dottrina e da lla giurisprudenza.

Il primo approdo legislativo è rappresentato dalla Legge n. 675 del 1996 in materia di protezione dei dati personali, successivamente modificata dal D.Lgs 196/2003, sempre al fine del recepimento delle già menzionate Direttive comunitarie del 1995 e del 2002[259].

La Costituzione italiana, però, a tutt'oggi tace sul diritto alla riservatezza, prevedendo espressamente soltanto delle altre forme di libertà che possono essere comprese nel concetto di *privacy*, quale la libertà di domicilio (art. 14 Cost.), la libertà e segretezza della corrispondenza (art. 15 Cost.), oltre al generale art. 2 Cost. che riguarda la garanzia ed il riconoscimento dei diritti inviolabili dell'uomo, come clausola omnicomprensiva anche dei diritti di nuova generazione.

Il codice della *privacy* italiano definisce, all'art. 4.1 lett. B), i "*dati personali*" come qualsiasi tipo di informazione che rende identificabile una persona fisica o giuridica, mediante il riferimento ad un numero o ad uno o più elementi specifici, caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale[260]. Per "*trattamento*", la legge italiana intende qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, regis trati in banche dati o non registrati[261].

Al soggetto interessato è riconosciuto il diritto di accedere ai dati personali, nonché di ottenere la conferma della loro esistenza o meno, anche al fine di esercitare su di essi i diritti di aggiornamento, rettifica, cancellazione, anonimizzazione, blocco e quanto previsto *ex lege*[262].

---

tra questi la Germania, limitatamente alla conservazione dei dati concernenti l'accesso Internet, la telefonia via Internet e la posta elettronica su Internet, chiedendo una proroga di 18 mesi e negli stessi termini anche il Granducato di Lussemburgo, senza però indicare un termine ulteriore specifico.

[259] Per alcuni spunti di approfondimento sulle origini storiche del quadro giuridico italiano in materia di privacy e protezione dei dati personali si veda C. SARTORETTI, *op.cit.*, pagg. 38 ss.

[260] La differenza della legge sulla privacy italiana rispetto alla direttiva europea attiene al fatto che l'ordinamento europeo non fa nessun riferimento alle persone giuridiche ma solo alle persone fisiche.

[261] La definizione di "*trattamento*" è contenuta all'art. 4.1, lett. A) del Codice Privacy.

[262] L'art. 7 del D.Lgs 196/2003 disciplina ed elenca in modo specifico e dettagliato tutti i diritti esercitabili dal singolo individuo in relazione ai dati personali che lo interessano. I successivi articoli 8 e 9, poi, regolamentano i modi e le forme di esercizio di tali diritti e l'art. 10 riconosco il diritto al soggetto

I dati personali devono essere trattati in modo lecito e secondo correttezza; devono essere raccolti e registrati per scopi espliciti e legittimi e devono essere corretti ed aggiornati. Tali dati devono essere pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e quindi trattati; devono essere conservati in una forma che consente l'identificazione dell'interessato per un periodo non superiore al raggiungimento degli scopi prefissati.

La violazione delle regole sul trattamento dei dati personali rende questi non utilizzabili[263].

All'atto della cessazione del trattamento, secondo quanto disposto dall'art. 16, i dati devono essere distrutti, ceduti ad altro titolare se destinati ad un trattamento compatibile, conservati per fini meramente personali o per scopi di scienza e conoscenza.

I dati sensibili possono essere trattati da parte di soggetti pubblici solo se vi è una espressa disposizione di legge e per perseguire finalità di interesse pubblico, diversamente è necessario ottenere un'autorizzazione preventiva del Garante[264]. Lo stesso vale a dirsi per il trattamento di dati giudiziari da parte di soggetti pubblici[265].

Regole ulteriori sono previste per i privati e gli enti pubblici economici, quanto al trattamento dei dati sensibili e giudiziari.

I dati sensibili possono essere oggetto di trattamento solo previo consenso dell'interessato o su autorizzazione del Garante e comunque entro i limiti stabiliti dalle disposizioni del D.Lgs 196/03[266].

Quanto ai dati giudiziari, invece, questi possono essere trattati solo previo consenso dell'interessato ovvero a seguito di autorizzazione del Garante, con specificazione delle rilevanti finalità di interesse pubblico [267].

Per "*dati sensibili*" si intendono tutte quelle informazioni idonee a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche e politiche, l'adesione a gruppi organizzati di qualsiasi natura, nonché i dati idonei a rivelare lo stato di salute e la vita sessuale. Sono "*dati giudiziari*" tutti quei dati idonei a rivelare i provvedimenti propri dei casellari giudiziari, quelli riferiti a

---

di ottenere un riscontro da parte del responsabile del trattamento, mediante la trasmissione di dati, comunicazioni ed informazioni intelligibili.

[263] Cfr art. 11 Codice Privacy.

[264] Cfr art. 20 Codice Privacy.

[265] Cfr art. 21 Codice Privacy.

Sia in ipotesi di trattamento di dati sensibili sia di trattamento di dati giudiziari, ai soggetti titolari del trattamento sono richieste particolari attività di controllo preventivo e di verifiche successive, nel corso delle operazioni (art. 22).

[266] L'art. 26 regolamenta le garanzie dei dati sensibili nelle operazioni di trattamento, specificandone gli oggetti di riferimento e le modalità da seguire in maniera puntuale e dettagliata.

[267] Cfr art. 27 Codice Privacy.

sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti o la qualità di imputato o indagato[268].

Le disposizioni del Codice Privacy, secondo una finalità esplicitata, non devono essere d'ostacolo alla libera circolazione dei dati personali tra Stati membri dell'Unione europea[269].

I trattamenti effettuati per motivi di giustizia, cioè direttamente correlati alla trattazione di affari giudiziari o che hanno una diretta incidenza sullo svolgimento dell'attività giurisdizionale, sono soggetti a deroghe rispetto ai limiti previsti per il trattamento delle altre categorie di dati [270].

Le forze di polizia e i dipartimenti di pubblica sicurezza sono sottoposti a regole diverse per il trattamento ed il flusso di dati. Costoro possono acquisire dati, informazioni, atti e documenti anche per via telematica, avvalendosi di convenzioni per l'implementazione di reti di comunicazioni elettroniche tra uffici ed organi, in cui allocare pubblici registri, elenchi, schedari e banche dati[271]. Ulteriori regole derogatorie rispetto al sistema generale di trattamento dei dati sono previste per finalità di difesa o di sicurezza dello Stato[272].

L'intero Titolo X, in conformità alla Direttiva del 2002, è dedicato alle comunicazioni elettroniche.

È vietato utilizzare una rete pubblica di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, al fine di memorizzare le informazioni o monitorare le operazioni dell'utente[273].

Le disposizioni del Codice Privacy distinguono il trattamento possibile per i dati relativi al traffico, per la fatturazione dettagliata, per l'identificazione della linea, per i dati relativi all'ubicazione, per il registro delle chiamate di disturbo e di emergenza, per i dati relativi al trasferimento automatico della chiamata, per i dati relativi all'elenco degli abbonati e alle comunicazioni indesiderate[274].

L'art. 132 del D.Lgs 196/03 in tema di conservazione di dati di traffico "*per altre finalità*"[275], ha subito una pluralità di modifiche e integrazioni nel corso degli anni. Già il D.L. 155/05, meglio noto come pacchetto sicurezza Pisanu, ha inciso profondamente sul contenuto del menzionato articolo,

---

[268] Queste definizioni si trovano nell'art. 4 rispettivamente lett. D) e lett. E).

[269] Cfr art. 42 Codice Privacy. Il successivo art. 42 disciplina, invece, le ipotesi in cui è consentito il trasferimento dei dati in Paesi terzi.

[270] Cfr art. 47 Codice Privacy. Di assoluto interesse anche il successivo art. 48 il quale disciplina, secondo strutture generale, la formazione e il funzionamento delle banche dati di uffici giudiziari.

[271] Per un'analisi più approfondita e dettagliata sul trattamento dei dati da parte delle forze di polizia è necessario scorrere tutte le disposizioni del Codice Privacy inserite nel Titolo II, dall'art. 53 all'art. 57

[272] Sul punto si veda il Titolo III, art. 58.

[273] Cfr artt. 121 e 122 Codice Privacy.

[274] Cfr artt. 123-131 Codice Privacy.

[275] Questa è la dicitura utilizzata nella rubrica dell'articolo in analisi.

ricomprendendo i dati relativi al traffico telematico nel novero dei dati da trattare e da conservare, ponendo fine ad un vuoto legislativo che inficiava la fruttuosità delle indagini informatiche[276].

Successive modifiche ed integrazioni sono state effettuate ad opera del D.Lgs n. 109 del 2008, poi convertito nella Legge n. 48 del 2008 di recepimento della Convenzione di Budapest.

L'art. 132 prevede che il fornitore conservi i dati relativi al traffico telefonico per ventiquattro mesi dalla data della comunicazione, qualora sussistano le finalità di accertamento e repressione dei reati mentre, per le medesime finalità, i dati relativi al traffico telematico, sono conservati dal fornitore per dodici mesi dalla data della comunicazione. In entrambi i casi sono esclusi i contenuti delle comunicazioni.

I dati relativi alle chiamate senza risposta, invece, sono conservati per trenta giorni.

Il Ministro dell'Interno, i responsabili degli uffici centrali specialistici in materia informatica e telematica possono ordinare ai fornitori di servizi informatici o telematici di conservare i dati, se perviene una richiesta in tal senso da parte di un'autorità investigativa estera, per un periodo non superiore ai novanta giorni. Tale termine, che si riferisce comunque ai soli dati esterni e non ai contenuti delle comunicazioni, può essere prorogato, per motivate esigenze, per un periodo non superiore ai sei mesi e solo in riferimento a specifici reati per cui si procede[277].

Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e all'attività svolta su mandato dell'autorità, viceversa incorre in una violazione penalmente rilevante[278].

Il trattamento dei dati per finalità di accertamento e repressione dei reati deve essere effettuato garantendo l'interessato e proteggendo i dati, affinché mantengano i requisiti di qualità, sicurezza e protezione in rete, prevedendo anche delle forme di autenticazione informatica e indicando sempre le modalità tecniche per la periodica distruzione dei dati, allo spirare dei termini previsti dalla legge[279].

---

[276] Il pacchetto Pisanu non è stato però immune da critiche per la limitatezza dei contenuti affrontati, specie per quanto attiene la vastità delle attività d'indagine informatica. Per un approfondimento sulle modifiche della L. 155/05 si rinvia a G. BRAGHO' *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa* in *Diritto dell'Informazione e dell'Informatica,* 2005, fasc. 3, pag. 517 ss.

[277] Il riferimento generico a "*specifici reati*" non è meglio precisato nel testo dell'art. 132 e nemmeno desumibile dal contesto normativo. Si può presumere che, certamente, possa essere prevista una tale proroga dei termini di conservazione dei dati qualora si stia procedendo per reati di particolare allarme sociale e gravità, quale il reato di terrorismo.

[278] Cfr art. 132, comma 4-quater, Codice Privacy.

[279] Cfr art. 132, comma 4-quinquies e 5, Codice Privacy.

Anche in Francia il concetto di *privacy* si è sviluppato prima in dottrina, in un secondo momento in giurisprudenza e solo più tardi a livello normativo[280].

Il diritto alla riservatezza, è un diritto di origine pretorile, un'autentica *creation pretorienne.*

Una rilevante modifica legislativa del codice civile nel 1970 ha portato alla consacrazione del diritto al rispetto della vita privata[281]. E' merito del *Conseil constitutionel* di aver elevato la *vie privée* a diritto di rango costituzionale attraverso una minuziosa operazione ermeneutica.

La Francia ha adottato la prima normativa in tema di protezione dei dati personali nel 1978, con ciò dimostrando di avere elaborato una risposta tempestiva alle esigenze del progresso tecnologico, specie relativamente all'informatica, alle schedature e alle libertà[282].

La legge del 1978, correttamente riveduta e integrata per dare piena attuazione alle Direttive comunitarie del 1995 e del 2002, è stata sostanzialmente trasposta nella Legge n. 801 del 2004, nel cui testo sono identificati in modo chiaro i valori tutelati ed anche la dimensione della tecnologia informatica con tutte le potenzialità ad essa correlate.

Nessun testo normativo, però, definisce compiutamente il concetto di *droit au respect de la vie privéè.*

Il giudice costituzionale francese, con la sentenza 2 marzo 2004, n. 2004-492 ha affermato che l'art. 2 della Dichiarazione del 1789 implica il rispetto della vita privata e, pertanto, nel novero delle libertà costituzionali questa deve figurare come bene giuridico oggetto di tutela e garanzia[283].

La nuova legge francese sulla protezione dei dati del 2004 è stata promulgata all'esito del parere favorevole reso dal Consiglio costituzionale. Questa norma è il frutto di una lunga gestazione e di lavori parlamentari durati più di due anni prima che fosse licenziato il testo definitivo approvato.

La Legge 801 del 2004 ha introdotto l'obbligo di sottoporre all'autorizzazione preventiva della CNIL i trattamenti di dati "a rischio" per la vita privata, introducendo un regime più gravoso. Se ad eseguire il trattamento è un ente statale, l'obbligatorio parere preventivo del CNIL deve essere reso di dominio pubblico. Inoltre è stata introdotta la possibilità per i soggetti che operano per la tutela del diritto d'autore di creare e gestire un database in cui

---

[280] Per un'approfondita ricognizione della giurisprudenza francese in materia di privacy si rinvia alla lettura di P. KAIESER *Le secret de la vie privée,* Dalloz, 1965; S. CIPRIANI *La protezione penale della riservatezza in diritto comparato italiano e francese* in *Riv. it. dir. proc. pen,,* 1997, pag. 86 ss.

[281] La novella legislativa è stata operata dalla Legge del 17 luglio 1970, n. 643 che, modificando l'art. 9 del Codice civile, ha garantito un valore preminente ai concetti di "*vita privata*" e "*intimità della vita privata*".

[282] Così A. GRUBER *Il sistema francese di tutela dei dati personali* in G.F. FERRARI (a cura di) *La legge sulla privacy dieci anni dopo,* Egea, 2008, pagg. 83-85.

[283] Per un approfondimento sull'evoluzione del concetto di *privacy* nell'ordinamento giuridico francese si rinvia a C. SARTORETTI *op.cit.*

inserire le segnalazioni di ipotetici reati di falsificazione, da sottoporre comunque all'autorizzazione preventiva del CNIL.

Sono previste delle eccezioni riguardo i dati nominativi definiti "*sensibili*", che non possono essere raccolti per principio, salvo delle eccezioni a beneficio delle autorità pubbliche e giurisdizionali e qualora il trattamento sia necessario per la salvaguardia della vita umana, dell'individuo o di terzi o qualora si riferiscano a dati resi pubblici dall'interessato o alla cui diffusione lo stesso abbia prestato il consenso.

Ogni titolare del trattamento deve nominare un referente per la protezione dei dati personali (*correspondants à la protection des données*) incaricati di vigilare sul rispetto della normativa da parte dei singoli titolari [284]. La legge prevede che questi soggetti devono godere di effettiva indipendenza ed essere in possesso di determinate qualifiche.

Le sanzioni previste dal Codice penale nelle ipotesi di violazione della Legge n. 801 del 2004 sono state inasprite, prevedendo, per talune ipotesi, anche la pena della reclusione fino a 5 anni e dell'ammenda fino a Euro 300.000,00. Anche le persone giuridiche possono essere responsabili penalmente per queste violazioni, con possibilità di dichiararne l'interdizione.

La legge francese prevede il principio del consenso dell'interessato per il trattamento dei dati che lo riguardano all'art. 7, integrato da cinque condizioni alternative.

Nel caso di raccolta di dati personali, l'interessato debba essere informato relativamente alla obbligatorietà o facoltatività delle risposte nonché delle conseguenze dell'eventuale rifiuto di fornire i dati. Inoltre, l'interessato deve ricevere informazioni sui soggetti che avranno accesso ai dati personali e sul diritto di accesso e di rettifica che la stessa legge gli attribuisce. Infine, chi effettua il trattamento dei dati deve informare l'interessato delle finalità solo ove questi lo richieda, e non in generale, sempre prima di raccogliere i dati personali o effettuare qualsiasi trattamento. Le finalità del trattamento devono essere comunicate esclusivamente al CNIL.

La legge si applica indipendente dalla circostanza che il trattamento venga effettuato da soggetti francesi o stranieri, essendo l'applicazione stessa basata su un principio di territorialità, adottato anche dalla legge 675/96. In base a tale principio, l'applicazione della legge dipende dalla circostanza che il trattamento venga effettuato nel territorio dello Stato, indipendentemente, dunque, dalla nazionalità dei soggetti coinvolti in detto trattamento.

La legge francese si applica anche agli archivi manuali, ma sole ove gli stessi siano in qualche modo connessi ad archivi automatizzati. Essa inoltre non si applica ai dati personali relativi alle persone giuridiche.

[284] La previsione della figura del referente nasce proprio in applicazione dell'art. 18(2) della Direttiva 95/46.

Quanto al ruolo del CNIL nel caso di trasferimento all'estero di dati personali, qualora il trasferimento di dati sia indirizzato verso Paesi che hanno una propria legislazione in materia di protezione dei dati personali, è sufficiente notificare preventivamente al CNIL l'intenzione di procedere al trasferimento. Nel caso in cui, invece, il Paese destinatario dei dati og getto di trasferimento sia sprovvisto di tale legislazione, la legge francese richiede che colui che effettua il trasferimento debba concludere un contratto con l'utilizzatore di tali dati nel Paese destinatario, nel quale quest'ultimo si impegni a garantire una tutela dei dati trasferiti equivalente a quella fornita dalla legislazione francese. Quest'ultima previsione è particolarmente interessante se si considera che la legge francese fornisce addirittura modelli per la conclusione di tale accordo[285].

La legge tedesca sulla *privacy*, il *Bundesdatenschutzgesetz* del 18 maggio 2001[286] (entrato in vigore il 23 maggio 2001), si caratterizza per l'assoluto rigore e severità politica di contenuto.

Non sembra un caso che l'origine dell'indagine su *Google Street View* abbia preso le mosse dalle segnalazioni dei garanti della *privacy* tedeschi.

Il governo tedesco si è sempre dimostrato attento agli aspetti con cui le nuove tecnologie entrano nella vita dei cittadini[287]. L'ultimo esempio è la recente richiesta, da parte del Ministro alla Tutela dei Consumatori, Ilse Aigner, di istituire un codice di condotta specifico per le società che operano in rete, onde evitare che internet diventi la gogna del XXI secolo.

Anche l'esperienza tedesca, come quella francese ed italiana, si caratterizza per l'importante ruolo assunto dalla giurisprudenza costituzionale che, in armonia con spunti già provenienti dalla dottrina, ha cercato di dare un fondamento costituzionale al diritto alla tutela della *privacy*[288]. La Corte costituzionale tedesca ha anche affermato il principio di necessità del trattamento dei dati personali, nei cui casi il diritto alla difesa della sfera privata dei singoli è subordinato all'interesse pubblico, secondo un criterio di proporzionalità.

---

[285] Per un'analisi completa e dettagliata della legge francese sulla privacy si rinvia al testo normativo che è visionabile in rete all'indirizzo web del CNIL: www.cnil.fr.

[286] Il testo del Bundesdatenschutzgesetz del 2001 è consultabile in rete all'indirizzo www.privireal.org/content/dp/germany.php (consultato in data 4 febbraio 2011).

[287] La Germania, a partire dagli Anni Settanta, si è data un'ampia disciplina legislativa in materia di privacy e, segnatamente, di diritto al trattamento dei dati. Dopo sette anni di attività, è stato varato dal Parlamento federale il primo Bundesdatenschutzgesetz già nel 1977 e cui è succeduta una legge nel 1990 e quindi il BDSG del 2001. Va però osservato che, prima ancora della normativa federali del 1977, alcuni Lander avevano già disciplinato il diritto al segreto dei dati, in particolare l'Assia nel 1970 e la Renania-Palatinato nel 1974.

[288] Per un approfondimento sull'esperienza tedesca in materia di privacy e protezione dei dati personali si rinvia, *ex multis,* a C. SARTORETTI *op.cit.,* pag. 44 ss; S. PANUNZIO (a cura di) *I diritti fondamentali e le Corti in Europa,* Jovene, 2005.

Anche la Germania, come la Francia, ha presto dato corpo normativo alla protezione dei dati personali, recependone l'esigenza ben presto rispetto agli altri Stati dell'Unione.

Prima ancora della Legge federale del 1977, poi riformata nel 1990 e nel 2001, alcuni *Lander* hanno introdotto una norma sulla protezione dei dati personali.

Nella relazione annuale del Garante della *privacy* tedesco del 2003[289], il bilancio delineato sulla Legge del 2001 presenta luci e ombre: da un lato è aumentata la sensibilità per le tematiche di protezione dati a livello politico, amministrativo e sociale; dall'altro, le esigenze di *privacy* non ricevono ancora tutta l'attenzione che meritano, e sussistono molti pregiudizi difficili da eliminare, quali l'inconciliabilità tra sicurezza pubblica e *privacy* e gli ostacoli che la privacy oppone al libero dispiegamento dell'attività economica. Il Garante ha da subito rappresentato le problematiche più urgenti quali l'assenza di norme sulla registrazione e la diffusione delle immagini e l'aumento smisurato di intercettazioni telefoniche senza motivazioni chiare e/o sufficienti.

Il *Bundesdatenschutzgesetz* è applicabile al settore pubblico ed anche al settore privato, quanto alle attività di raccolta mediante mezzi informatici e telematici di dati personali.

Ogni registrazione, archiviazione e trattamento di dati è permesso solo se conforme alle disposizioni di legge o se l'interessato ha prestato il proprio consenso.

La Legge sulla privacy tedesca regola il trasferimento dei dati all'estero. Se il trasferimento di una categoria di dati è permessa all'interno del territorio tedesco allora lo è anche in territorio estero. Se il Paese richiedente è membro dell'Unione europea non è necessaria alcuna restrizione particolare, oltre i limiti già posti dalla normativa tedesca, se invece la richiesta proviene da un Paese extra UE la Germania può escludere il trasferimento dei dati solo a fronte di una motivazione coerente e comunque deve essere garantita una protezione dei dati equivalente a quella nazionale.

Ogni trasferimento di dati medianti mezzi automatizzati deve essere soggetto a registrazione prima di essere effettivamente eseguito. Questo non vale per i casi in cui il responsabile del trattamento provveda a istituire un ufficio apposito per la protezione dei dati o, ad alcune condizioni, se il responsabile del trattamento provveda alla raccolta, al trattamento e all'uso dei dati personali solo per i propri scopi.

Ogni autorità coinvolta in attività di trattamento dei dati personali è tenuta a prevedere delle idonee misure di protezione dei dati e degli strumenti

[289] Il testo della relazione è visionabile nel web all'indirizzo www.consulentiprivacy.it/Relazione_Germania2002.htm (consultato in data 15 gennaio 2011).

tecnici adeguati a tal fine, i quali devono essere testati e valutati da soggetti esperti indipendenti.

La violazione delle disposizioni della legge sulla privacy è sanzionata penalmente mediante la previsione di pena detentive e pene pecuniarie.

Il BDSG regola, inoltre, le condizioni per la videosorveglianza dei luoghi pubblici, anche da parte di privati, la quale è subordinata ad un'autorizzazione. L'autorizzazione viene rilasciata solo in particolari circostanze e subordinatamente a determinate condizioni previste dalla legge[290].

Una particolare attenzione per la scurezza e la tutela dei dati deve essere assicurata nell'uso di strumenti mobili di memorizzazione e trattamento dei dati quali le *smart cards*[291].

L'intero testo normativo tedesco sulla *privacy* è incentrato sull'incremento degli *standard* di protezione dei dati.

Le informazioni memorizzate devono essere utilizzate solo nei limiti e secondo i fini per cui sono stati acquisiti; il soggetto interessato deve essere avvisato qualora i suoi dati personali siano utilizzato per scopi pubblicitari o commerciali. Un surplus di tutela viene garantito nelle attività di memorizzazione, trasferimento e trattamento dei dati sensibili.

Non è necessario il consenso preventivo all'acquisizione e memorizzazione dei dati personali in particolari circostanze previste *ex lege*.

Il settore privato è soggetto ad un maggior numero di restrizioni e limitazioni quanto alle operazioni di raccolta, memorizzazione e trattamento dei dati rispetto al settore pubblico.

[290] Cfr paragrafo 6 BDSG.
[291] Cfr paragrafo 6c BDSG.

CAPITOLO SECONDO

SEZIONE I

Il contenuto della prova digitale nell'ambito della cooperazione nello spazio giudiziario europeo

SOMMARIO: 4. Il catalogo dei reati che coinvolgono la prova digitale e la sua circolazione: le ipotesi di *cyber terrorism* nazionale e transnazionale; 5. Le garanzie nella circolazione della prova digitale e la sicurezza delle infrastrutture; 5.1 Il rapporto pubblico-privato per lo sviluppo delle infrastrutture: un incontro tra esigenze di pubblica sicurezza e di sviluppo economico; 5.2 Un progetto di regole comuni per la catalogazione e indicizzazione delle prove: l'individuazione di termini e tecniche di scelta condivisa; 5.3 Le forme di controllo delle richieste di trasmissione di prove digitali e dei soggetti richiedenti: un intervento preventivo contro gli eccessi e gli abusi; 5.4 La formazione del personale coinvolto nelle procedure di cooperazione e di circolazione della prova digitale: una specializzazione necessaria per l'incremento della responsabilizzazione dei singoli

4. *Il catalogo dei reati che coinvolgono la prova digitale e la sua circolazione*[292]*: le ipotesi di cyber terrorism nazionale e transnazionale*

La Direttiva 96/9/CE del Parlamento e del Consiglio europeo del 11 marzo 1996 contiene le regole di tutela giuridica delle banche dati. L'art. 7, rubricato "*oggetto della tutela*", prevede che "*Gli Stati membri attribuiscono al costitutore di una banca dati il diritto di vietare operazioni di estrazione e/o reimpiego della totalità o di una parte sostanziale del contenuto della stessa, valutata in termini quantitativi, qualora il conseguimento, la verifica e la presentazione di tale contenuto attestino un investimento rilevante sotto il profilo qualitativo o quantitativo*". Per

[292] Il paragrafo si prefigge lo scopo di offrire un primo quadro di riferimento dei reati che coinvolgono la prova digitale e la sua circolazione. Gli approfondimenti e le analisi più approfondite si lasciano agli studiosi esperti di diritto penale sostanziale.
Si rinvia ad una serie di testi sul diritto penale dell'informatica, quali C. PECORELLA *Diritto penale dell'informatica*, Cedam, 2000; V.S. DESTITO – G. DEZZANI – C. SANTORIELLO *Il diritto penale delle nuove tecnologie*, Cedam, 2007; C. SARZANA DI SANT'IPPOLITO *Informatica, internet e diritto penale*, Giuffré, 2010.

estrazione, come precisato nello stesso articolo, si intende il trasferimento permanente o temporaneo della totalità o di una parte rilevante di un contenuto di una banca dati su un altro supporto, con qualsiasi mezzo e attraverso qualsiasi forma.

Per *reimpiego* si intende una messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto di una banca dati mediante la distribuzione di copie, noleggio, trasmissione in linea o in altre forme. Il prestito pubblico non può essere configurato come una forma di estrazione o reimpiego. Sull'interpretazione di questa Direttiva ed in particolare del menzionato art. 7 è intervenuta la Corte di Giustizia delle Comunità europee con una interessante decisione della sez. IV, 9 ottobre 2008, nella causa C-304/07. Con questa sentenza i giudici hanno chiarito la nozione di "*estrazione*"[293] sostenendo, *in primis*, che non si possa limitare tale concezione alle sole operazioni che consistono nel riprodurre meccanicamente, senza adattamenti, il contenuto di una banca dati o di una parte di essa tramite un semplice processo di copia/incolla, né può circoscriversi alle operazione di trasferimento del contenuto di una banca dati tutelata o di una parte sostanziale di esso. Altrettanto certo è che le attività di consultazione delle banche dati esulino dalla previsione dell'art. 7 della Direttiva.

Questa sentenza della Corte di Giustizia è giunta quattro anni dopo le famose sentenze del 2004 che delimitavano la privativa attribuito al costitutore delle banche dati a mezzo del cd. diritto *sui generis*, concentrandosi questa volta però sulle operazioni di estrazione. La Corte ammette che si possa agire non solo contro il reimpiego parziale o totale dei dati contenuti nel *database* ma anche contro la semplice appropriazione, mediante estrazione dei dati. Già nel caso *British Horse Racing*, la Corte spiegava che l'accesso diretto al *database* non rappresentava un elemento essenziale perché si potesse integrare la fattispecie di estrazione. Si ammetteva, dunque, che l'acquisizione del contenuto attraverso una risorsa terza, che ne disponeva legittimamente, configurasse parimente un'ipotesi di estrazione anche se, di fatto, non era stata eseguita alcuna estrazione diretta di dati dalla banca dati.

La proposta di Decisione quadro COM(2002)173 definitivo, presentata dalla Commissione europea e avente ad oggetto gli attacchi contro i sistemi informatici, tende a garantire lo sviluppo delle interconnessioni tra i sistemi, allo scopo della piena realizzazione di uno spazio europeo di libertà, sicurezza e giustizia.

Questa proposta di Decisione quadro vuole essere un valido spunto ed un appoggio per realizzare il ravvicinamento delle normative penali degli Stati membri, almeno nel settore degli attacchi a sistemi informatici.

---

[293] Per un approfondimento sulla sentenza della Corte di Giustizia, si invita alla lettura del testo completo della decisione, consultando il sito http://curia.europa.eu.

La locuzione "*sistemi d'informazione*", come precisato nella relazione introduttiva alla proposta, deve intendersi nell'accezione più ampia, comprendendo quindi i personal computer stand alone, i *personal organizer* digitali, telefoni cellulari, *intranet*, *extranet*, le reti, i *server* e le altre infrastrutture di Internet.

La Commissione europea ha enucleato i tipi di minacce ai sistemi d'informazione:

1. accesso non autorizzato ai sistemi di informazione, mediante lo sfruttamento di informazioni interne agli attacchi più invasivi e alle intercettazioni di *password;*
2. interruzione del funzionamento dei sistemi d'informazione attraverso attacchi dolosi, quali il cd. *denial of service* consistente nella saturazione degli apparecchi con messaggi lunghi e ripetuti, cercando di sovraccaricare i *server web* o gli ISP;
3. esecuzione di *malicious software,* alcuni dei quali danneggiano il PC stesso, mentre altri utilizzano il *personal computer* per attaccare diverse componenti collegati in rete. Alcuni programmi rimangono inerti fino a che non si realizza un evento che li innesca, altri appaiono benigni ma se attivati determinano gravi alterazioni o distruzioni di dati. Un'altra tipologia è rappresentata da quei programmi che non infettano ma si auto duplicano in copie sempre più numerose da saturare il sistema;
4. intercettazione di comunicazioni;
5. usurpazione dell'identità di un individuo ed illecito utilizzo di essa.

Sugli stessi argomenti è stata predisposta la Decisione quadro 2005/222/GAI del 16 marzo 2005 che, in particolare nel *considerandum* 11, esplicita la necessità di giungere ad un approccio comune per la definizione di reati comuni di accesso illecito ad un sistema di informazioni, di interferenza illecita per quanto riguarda i sistemi e, in maniera distinta, per quanto riguarda i dati. Lo scopo espresso di questa Decisione, in base al contenuto del *considerandum* 17, è quello di fare in modo che gli attacchi ai danni di sistemi di informazione siano puniti effettivamente in tutti gli Stati membri per mezzo della previsione di sanzioni proporzionate ai fatti commessi ed ai danni provocati, così da dissuadere il potenziale criminale, incoraggiando e migliorando la cooperazione giudiziaria, eliminando le barriere di divisione tra i Paesi con la previsione di norme comuni e compatibili.

La Decisione Quadro 2005/222/GAI contiene non solo la previsione dell'illecito accesso a sistemi informatici ma anche l'interferenza illecita sempre nei sistemi, l'interferenza illecita per quanto riguarda i dati e l'istigazione, favoreggiamento, complicità e tentativo.

L'art. 3 dispone che gi Stati membri adottino le misure necessarie per sanzionare penalmente l'atto intenzionale, commesso dal non avente diritto, almeno nei casi più gravi, volto ad ostacolare gravemente o interrompere il funzionamento di un sistema informatico mediante l'immissione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione, la soppressione di dati informatici o rendendoli inaccessibili.

L'art. 4, invece, attiene la previsione di misure sanzionatorie penali, almeno per le ipotesi di maggiore allarme e potenziale offensivo, contro gli atti intenzionali diretti a cancellare, danneggiare, deteriorare, alterare, sopprimere o rendere inaccessibili dati informatici in un sistema di informazioni, commessi da soggetti che non ne hanno diritto.

L'art. 5 è una disposizione finale e di completamento che si riferisce tanto all'art 2, cioè all'accesso illecito a sistemi informatici, quanto agli articoli 3 e 4, prevedendo che siano puniti anche i fatti di istigazione, favoreggiamento, complicità e tentativo. Interessante notare la deroga prevista dal paragrafo 1 dell'articolo in analisi in cui si precisa che gli Stati membri hanno facoltà di non punire il tentativo, ma solo in relazione al tentato accesso illecito a sistemi informatici. Già il tenore di questa previsione facoltativa rende palese il minor grado di allarme e di pericolosità avvertito dal Parlamento e dal Consiglio europeo in relazione ai fatti di accesso illecito a sistemi di informazione.

Questo è ancora più chiaro dal contenuto dell'art. 6 della Decisione quadro, rubricato "*Sanzioni*", nel cui secondo paragrafo è prevista la soglia di pena massima detentiva, oltre la quale non è dato scendere, in particolare individuata tra uno e tre anni, solo per i fatti che integrano l'interferenza illecita per quanto riguarda i sistemi e per quanto riguarda i dati, nulla indicando nello specifico per le ipotesi di accesso illecito a sistemi di informazione.

L'art. 7 individua un diverso grado di pericolosità ed offensività del bene giuridico protetto avvertito per le ipotesi di cui all'art. 2 Decisione quadro, laddove prevede l'applicazione della circostanza aggravante per i fatti commessi nell'ambito di un'organizzazione criminale[294], in tutte le ipotesi di interferenza illecita per quanto riguarda i sistemi e i dati, mentre per l'accesso illecito a sistemi di informazione nei soli casi in cui la fattispecie sia stata

[294] Per la nozione di organizzazione criminale si rinvia al testo dell'Azione Comune 98/733/GAI del 21 dicembre 1998, adottata dal Consiglio sulla base dell'articolo K3 del Trattato sull'unione europea. L'art. 1 così recita: "*Ai fini della presente azione comune, per organizzazione criminale si intende l'associazione strutturata di più di due persone, stabilita da tempo, che agisce in modo concertato allo scopo di commettere reati punibili con una pena privativa della libertà o con una misura di sicurezza privativa della libertà non inferiore a quattro anni o con una pena più grave, reati che costituiscono un fine in sé ovvero un mezzo per ottenere profitti materiali e, se del caso, per influenzare indebitamente l'operato delle pubbliche autorità".*

integrata da un fatto commesso mediante la violazione delle misure di sicurezza. L'applicazione di suddetta circostanza aggravante è circoscritta ai soli comportamenti che abbiano provocato gravi danni o abbiano colpito interessi essenziali.

Le persone giuridiche rispondono dei reati previsti dagli articoli 2, 3, 4 e 5 della Decisione quadro, quando commessi per trarne un beneficio per sé a cura di soggetti individuali o organi riconducibili alla stessa persona giuridica. L'art. 8, inoltre, prevede una forma di responsabilità delle persone giuridiche anche nei casi in cui la commissione del fatto di reato sia stata resa possibile o comunque agevolata dall'omesso controllo o vigilanza da parte dei soggetti a ciò preposti. Il procedimento di riconoscimento della responsabilità penale della persona giuridica non esclude l'avvio di un *iter* giurisdizionale anche nei confronti dei soggetti, persona fisica, che risultano essere le parti attive del comportamento penalmente rilevante.

Nel quadro dello sviluppo delle politiche criminali per combattere la cibercriminalità, la Commissione ha presentato la comunicazione COM(2007) 267 definitivo al Parlamento, al Consiglio europeo e al Comitato delle Regioni.

La Commissione precisa che sulle reti elettroniche si possono commettere numerosissimi reati, quali in particolare le frodi, i furti d'identità, lo *spamming*, il *phishing*, l'intrusione di codici maligni. E' in crescita il numero di siti internet a contenuto illegale che diffondono materiali illegittimamente e anche il numero di attacchi ai sistemi d'informazione, da parte di organizzazioni o singoli individui (spesso attraverso i cosiddetti *botnets*) e alle infrastrutture critiche di informazione. Lo sviluppo continuo delle tecnologie informatico-telematiche, come precisato dalla Commissione, non permette una previsione di norme incriminatrici esaustive e complete di tutte le fattispecie di reato realizzabili e questo richiede una soglia di attenzione sempre crescente da parte del Legislatore comunitario, così come del Legislatore nazionale.

La Convenzione sul *cybercrime* fornisce un ulteriore catalogo di reati informatici che possono coinvolgere la prova digitale nella sua fase statica di apprensione e nella sua fase dinamica di circolazione fra gli Stati membri dell'Unione europea ma anche verso Stati Terzi.

Nel Preambolo alla Convenzione, il Consiglio d'Europa sottolinea la necessità e insieme la priorità di prevedere una politica criminale comune tra i Paesi, al fine di proteggere la società contro i crimini informatici, mediante l'adozione di una legislazione appropriata ma anche per mezzo del rafforzamento della cooperazione internazionale.

Il Consiglio d'Europa ha palesato la consapevolezza dei rilevanti cambiamenti attuati per mezzo della digitalizzazione e della continua globalizzazione dei *computer networks*, individuando i rischi del *computer network* e dell'informazione elettronica nel loro uso illecito per la commissione

di offese penalmente rilevanti e nella conseguente necessità di acquisire e poi trasferire le prove di questi fatti criminosi mediante la rete. La finalità della Convenzione di Budapest, espressa fin dal Preambolo, riguarda la prevenzione delle azione dirette contro la confidenzialità, integrità e funzionalità del sistema informatico, della rete e dei dati informatici e l'adozione dei poteri necessari e sufficienti per rendere effettiva la lotta a queste forme di criminalità in costante incremento, facilitando la prevenzione, le indagini e la repressione sia a livello nazionale sia a livello internazionale, anche mediante l'incentivazione di forme di cooperazione.

E' anche espressa la necessità di procedere ad un bilanciamento tra gli interessi delle autorità investigative e il rispetto dei diritti fondamentali previsti dal testo della Convenzione di Roma del 1950 del Consiglio d'Europa, dal Patto dei Diritti civili e politici delle Nazioni Unite del 1966 e da qualsiasi altro Trattato internazionale sui diritti umani che garantisca il diritto all'espressione delle proprie opinioni senza interferenze, il diritto alla libertà di espressione ed il diritto alla *privacy*. Tra i diritti fondamentali che necessitano di essere bilanciati con contrapposti interessi, nel Preambolo è fatto espresso riferimento anche al diritto alla protezione dei dati personali, conferente alla Convenzione del Consiglio d'Europa per la Protezione degli Individui con riguardo al trattamento automatizzato delle informazioni.

Il Consiglio d'Europa, preso atto delle procedure di cooperazione vigenti tra gli Stati, ritenendone essenziale lo sviluppo in termini di mezzi utilizzati e di velocizzazione delle operazioni, si pone lo scopo di intervenire in questo contesto, oltre che determinare una disciplina per rendere più efficaci le indagini ed effettivi i processi per le offese penali correlate ai sistemi informatici e ai dati, con particolare attenzione alla raccolta delle prove in formato elettronico.

La Convenzione di Budapest, nella sezione 1 del Capitolo II, affronta il tema della legge penale sostanziale, prevedendo una serie di offese penali alla confidenzialità, integrità e fruibilità dei dati e sistemi informatici, come misure di riferimento che devono trovare applicazione nelle norme nazionali degli Stati ratificatori della Convenzione.

Oltre al già menzionato art. 2 in materia di accesso illegale, l'art. 3 impone agli Stati di adottare una disciplina e delle misure idonee per le intercettazioni illegali, commesse intenzionalmente e senza averne diritto, mediante l'uso di mezzi tecnici, avverso trasmissioni non pubbliche di dati a, da o per mezzo di sistemi informatici.

L'art. 4 contiene la previsione di normative nazionali di sanzione per comportamenti intenzionali di danneggiamento, cancellazione, deterioramento, alterazione o soppressione di dati di un computer, senza diritto.

L'art. 5 tratta invece delle interferenze di sistema commesse intenzionalmente, quali atti che producano un serio danno al corretto funzionamento di un sistema informatico mediante introducendo, trasmettendo, asportando, deteriorando, alterando o sopprimendo dati informatici.

La Convenzione *cybercrime* prevede sanzioni per le attività di produzione, vendita, procuramento per l'uso, importazione, distribuzione o rendendo utilizzabili delle *devices*, compresi programmi informatici, costruite o adattate principalmente per agevolare la commissione delle fattispecie penali previste nel medesimo testo convenzionale ovvero anche le ipotesi di utilizzo di password, codici d'accesso o altri dati simili che in tutto o in parte permettono l'accesso ad un sistema informatico se commesso intenzionalmente ed al fine di integrare una delle fattispecie illecite previste nella Convenzione. Gli Stati sono liberi di sanzionare anche il mero possesso di un *item* riferito all'offesa appena menzionata, ma ciò è possibile se e solo se vi è l'intenzionalità di commettere uno dei fatti offensivi previsti dal Consiglio d'Europa e se il possesso di tali dati è ottenuto senza averne il diritto.

Il Titolo II della Convenzione di Budapest riguarda le offese correlate ad un computer: in particolare furti e frodi.

L'art. 7 prevede che ogni Stati sanzioni i comportamenti volontari e non autorizzati di *input*, alterazione, asportazione o soppressione di dati informatici, sia che si tratti di dati autentici o non autentici, indipendentemente dal fatto che il dato sia direttamente leggibile ed intellegibile. Ogni Stato è libero di prevedere delle misure preventive e dunque di sanzionare comportamenti diretti alla commissione delle categorie di fatti previste dall'art. 7.

L'art. 8, riguardante i comportamenti fraudolenti, punisce i fatti commessi intenzionalmente, senza averne diritto, che causano la perdita della proprietà di un soggetto mediante input, alterazioni, asportazioni o soppressioni di dati informatici ovvero mediante forme di interferenza al buon funzionamento di un sistema informatico, inequivocabilmente diretti a procurare un ingiusto beneficio economico a sé o ad altri.

Il Titolo IV della Convenzione, composto dall'unico (lungo) art. 10, prevede la sanzione per i comportamenti atti a violare il diritto d'autore ed i diritti a questo connessi, commessi per il mezzo informatico. Quanto alla nozione di diritto d'autore, di diritti connessi e l'individuazione dei confini di garanzia e tutela già previsti e comunemente condivisi, la Convenzione rinvia *al Paris Act* del 1971, all'Accordo sugli aspetti correlati al commercio dei diritti della proprietà intellettuale e il *WIPO Copyright Treaty*.

Come precisato dall'art. 12 della Convenzione, tutte le tipologie di offese richiedono una sanzioni da parte degli Stati ratificatori, non solo nel caso in cui

siano commesse da una persona fisica ma anche quando poste in essere da un organo di una persona giuridica ovvero da componenti di essi con posizioni apicali, con poteri di rappresentanza, poteri decisori e di controllo.

In relazione ai tipi sanzionatori, l'art. 13 della Convenzione lascia liberi i legislatori nazionali di scegliere la forma più idonea e proporzionata per i fini punitivi e dissuasivi, che possono comprendere anche la privazione della libertà e la previsione di sanzioni in denaro.

Il furto di identità digitale è una forma di reato particolarmente diffusa e che, secondo le statistiche, genera un forte allarme sociale, tale per cui la popolazione avverte forte la necessità di ricevere informazioni chiare e complete sui comportamenti da tenere per prevenire e reprimere questo crimine.

L'interesse verso i reati informatici è visibile in tutto il contesto internazionale, in seno alle Nazioni Unite, all'OECD e al G8.

Ne sono ulteriore prova le varie Raccomandazioni emanante dal Consiglio dei Ministri, quali N. R (85) 10 sulle modalità di applicazione della Convenzione europea sulla mutua assistenza in materia penale, nel rispetto della disciplina delle intercettazioni di comunicazioni; N. R (88) 2 sulla pirateria nel campo delle violazioni del diritto d'autore e dei diritti affini; N. R (95) 4 sulla protezione dei dati personali nell'ambito dei servizi di telecomunicazione, con particolare riferimento ai servizi di telefonia; N. R (89) 9 in materia di crimini informatici, prevedendo delle linee guida per orientare i legislatori nazionali nella definizione dei *cybercrime;* N. R (95) 13 sulle problematiche procedurali correlate alle tecnologie dell'informazione.

La Commissione Europea, nel *Forum on the prevention of organised crime,* ha analizzato la legislazione vigente e le attività d'indagine poste in essere da ciascuno Stato membro in materia di crimine organizzato per la commissione di furti d'identità. È emerso un quadro sconfortante di assoluta assenza di un pacchetto legislativo specifico. Gran parte degli Stati considerano il furto d'identità digitale come un mezzo per commettere altri reati o come mera circostanza aggravante.

Per *attacchi informatici all'identità elettronica* si intendono tutti quegli attacchi portati, tramite *software* eseguito da remoto, alle infrastrutture informatiche, finalizzati a carpire le credenziali dell'utente dei servizi.

Queste fattispecie di reato sono caratterizzate da una formulazione generale e generica che, volutamente, lascia ampio spazio di discrezionalità ai legislatori nazionali nella previsione di norme di attuazione. Ogni Stato, dunque, secondo le diverse realtà giuridiche e le scelte di politica criminale, bilancia le misure preventive e repressive preferibili, in relazione alle esperienze ed ai dati sulla criminalità corrente.

Da una valutazione generale che trascenda le singole particolarizzazioni, è possibile ritenere che tali forme di reato afferente i dati informatici, i sistemi informatici e le vicende ad essi correlate come la circolazione e lo scambio, sono idonee a realizzare una forma di *cyberterrorism*[295].

Secondo la definizione data dall'FBI, il *cyberterrorism* è caratterizzato da un'azione integratrice premeditata, un attacco motivato politicamente contro informazioni, sistemi informatici, programmi informatici e dati, quale risultato di una violenza perpetrata a danno di non combattenti da parte di gruppi nazionali o agenti clandestini. Gli autori del reato possono essere gruppi di dissidenti nazionali o internazionali che, in questo modo, fanno valere la propria causa o aggiungono queste forme alle più tradizionali forme di terrorismo.

Destrutturando il termine e quindi il concetto di *cyber* terrorismo o terrorismo informatico, si nota che tale parola composta contiene il richiamo al terrorismo con tutte le problematiche anche definitorie ad esso correlate[296],

[295] Per un approfondimento sul *cyberterrorism* si rinvia a D.E. DENNING *Cyberterrorism*, Georgetown University Press, 2000; N. PIRO *Cyberterrorismo*, Castelvecchi, 1998

[296] Il concetto di terrorismo è ancora oggi trattato in maniera critica da gran parte della dottrina. Esso coinvolge non solo profili giuridici ma anche socio-politici e psicologici. L'utilizzo dell'originario termine inglese si collega strettamente al concetto di paura, panico e ansia. Come noto, il cd. "*regime di terrore*" ha caratterizzato il 1798 e la Rivoluzione francese. A partire da tale data, il termine terrorismo è riferito ad un tipo di intimidazione fisica, violenta, destinata ad un determinato obiettivo. E' uno stile di violenza diretto a coartare le abitudini e distruggere la tranquillità e le certezze di una pluralità di soggetti. La disciplina normativa del fenomeno criminosa a finalità terroristica è contenuta nella Convenzione di Ginevra del 16 novembre 1937 e fu adottata su iniziativa della Società delle Nazioni in seguito all'attentato del 9 ottobre 1934, nel quale re Alessandro di Jugoslavia ed il Ministro degli Esteri francese Barthou furono assassinati dal terrorista croato Gueroguiev. La Convenzione di Ginevra del 16 novembre 1937 per la prevenzione e repressione del terrorismo ha contemplato, per la prima volta, fattispecie criminose a finalità terroristica allora sconosciuti quali gli attentati contro il capo dello stato o di governo, gli attentati contro edifici pubblici, i reati di pericolo comune. Le manifestazioni terroristiche venivano ad assumere rilievo internazionale allorchè travalicavano l'ambito di un singolo ordinamento statale.

Negli anni '60 la Comunità Internazionale si è trovata di fronte ad una pluralità di manifestazioni criminose, con prevalente finalità terroristica, fino ad allora ignote: pirateria aerea e navale, dirottamento di navi, sequestri di agenti diplomatici. Da lì si sono dunque resi necessari degli interventi normativi specifici, di natura particolare, per ciascuna delle menzionate fattispecie. Gli anni '70 sono stati caratterizzati da plurime azioni di sequestro di persone. Si pensi agli episodi relativi ai cittadini italiani Sallustro e Ruzzo, sequestrati in Argentina nel 1972-1973 e alla cattura di undici atleti israeliani durante le Olimpidadi di Monaco del 1972.

La Comunità Internazionale ha reagito con sufficiente prontezza al diffondersi di queste manifestazioni criminose anche elaborando degli strumenti pattizi ed agevolando la cooperazione interstatuale. Tutti gli atti normativi, indipendentemente dal carattere di applicazione settoriale o generale, si caratterizzano per i contenuti parzialmente generici, lasciando così ampio spazio di manovra e di coordinamento libero tra gli Stati nell'impegno alla prevenzione e repressione dei reati di stampo terroristico. Tutti gli accordi interstatuali si basano sul principio *aut dedere aut judicare* ed i crimini a finalità terroristica debbono essere considerati dagli stati contraenti come casi di estradizione.

Nel 1972 le Nazioni Unite, nell'intento di realizzare un concerto degli stati membri sul tema generale del terrorismo, ha adottato la risoluzione 3034/XXVIII, spostando il fulcro del problema dalla previsione di

misure di prevenzione e repressione allo studio e comprensione delle origine e delle cause del fenomeno. A seguire, sul piano regionale europeo, sono state varate la Convenzione di Strasburgo del 27 gennaio 1977 e l'Accordo di Dublino del 4 dicembre 1979.

La difficoltà nel dare una definizione generale e condivisa del termine "*terrorismo*" nasce sicuramente dalle differenze socio-politico-culturali degli Stati ma anche dalla varietà di manifestazioni del fenomeno. Non vi sono solo gruppi o individui che agiscono per fini propri e con le proprie risorse, ma anche organizzazioni spesso sponsorizzate e sostenute dai governi nazionali. Gli atti compiuti per i fini terroristici sono tanto vari e tanto diversi che è difficile anche indicarne dei denominatori comuni di riferimento.

La fattispecie criminosa con finalità terroristica, per tendenza, coinvolge una pluralità di Stati e ciò ha richiesto uno sviluppo delle procedure di scambio transnazionale di informazioni, privilegiando forme di coordinamento tra autorità inquirenti: la Raccomandazione dell'Ocde sulla gestione degli archivi e la Convenzione del Consiglio d'Europa del 1981, in particolare, si interessano del tema. Si sono, poi, susseguite una serie di Raccomandazioni, Risoluzioni e accordi bilaterali o multilaterali, ma il vero punto di svolta si è avuto in seno al Gruppo di Trevi, riunione informale dei ministri della Giustizia e degli Interni dei singoli stati della CEE.

L'*escalation* di manifestazioni di violenza organizzata con finalità di terrorismo che hanno scosso la società democratica dell'Europa occidentale, hanno posto il problema dell'adeguamento degli strumenti di reazione dello Stato, pur nel quadro giuridico della protezione delle libertà fondamentali rappresentato dalla Convenzione europea dei diritti dell'uomo. Non è risalente nel tempo la polemica e lo scandalo sollevati dalle modalità di esecuzione di pena e degli interrogatori al fine di estorcere delle confessioni e delle dichiarazioni nei confronti di terroristi (o presunti tali), specie di nazionalità islamica, nelle prigioni di *Guantanamo Bay*. Come ha ammonito Kofi Annan, Segretario Generale delle Nazioni Unite, nel corso di un messaggio espresso in occasione della Giornata mondiale delle libertà di stampa del 3 maggio 2002, « *nel nome dell'antiterrorismo, i principi ed i valori che sono stati sviluppati in decenni, perfino in secoli, possono essere messi a rischio* ».

La risposta al terrorismo si è fatta chiaramente più intensa a seguito dell'attacco alle Twin Towers e al Pentagono nell'11 settembre 2001. La svolta alle politiche di *counter terrorism* si è verificata con la Risoluzione del Consiglio di Sicurezza dell'ONU n. 1373 del 28 settembre 2001, la quale richiedeva agli Stati di prendere le necessarie misure per prevenire e reprimere atti e attività di natura terroristica. A questa Risoluzione ne sono seguite ulteriori, nonché accordi, Trattati e Convenzioni approvati in seno alle maggiori organizzazioni internazionali regionali, in primo luogo il Consiglio d'Europa, l'Unione Europea e l'OSCE.

La trattazione del concetto e del fenomeno di terrorismo conta una pluralità di contributi dottrinari di approfondimento. Tra gli altri, si rinvia a: A. MARINI *Il terrorismo internazionale oggi: brevi spunti di riflessione* in *Iustitia*, n. 2, 2009, pagg. 133-140; R. BARBERINI *Il giudice e il terrorista*, Einaudi, 2008; A. SIMONS – D. TUCKER *The Misleading Problem of Failed States: a socio-geography of terrorism in the post-9/11 era* in *Third World Quarterly*, n. 2, 2007, pagg. 387-401; M. E. BARTOLONI *Articolazione delle competenze e tutela dei diritti fondamentali nelle misure UE contro il terrorismo* in *Il Diritto dell'Unione Europea*, n.1, 2009, pagg. 134-162; J. R. PIOMBO *Terrorism and U.S. Counter-Terrorism Programs in Africa: an overview* in *www.centerforcontemporaryconflict.int*; A. SINCLAIR *An anatomy of terror*, Pan Books, 2003; AA.VV. *Enforcing International Law Norms Against Terorism*, Oxford and Portland Oregon, 2004; J. BAUDRILLARD *Lo spirito del terrorismo,* Raffaello Cortina Editore, 2002; A. LAUDATI *I delitti transnazionali:. Nuovi modelli di incriminazione e di procedimento all'interno dell'Unione europea* in *Diritto Penale e Processo*, n. 4, 2006, pagg. 401-405; A. SERRANO' *Le armi nazionali contro il terrorismo contemporaneo*, Giuffré, 2009; V. SCIARABBA *Misure antiterrorismo e diritti fondamentali: c'è un giudice a Lussmeburgo, ora anche due* (*intervenuta la Corte, il Tribunale si adegua*) in *Diritto pubblico comparato ed europeo*, n. 4, 2009, pagg. 201-207; G. INSOLERA *Reati associativi, delitto politico e terrorismo globale* in *Diritto Penale e Processo*, n. 11, 2004, pagg. 1325-1330; J. S. TUMAN *Communicating terror*, SAGE Publications, 2003; L. QUADARELLA *Il nuovo terrorismo internazionale come crimine contro l'umanità,* Editoriale Scientifica, 2006; G. ZICCARDI CAPALDO *Terrorismo internazionale e garanzie collettive*, Giuffré,

affiancato dal collegamento all'informatica e dunque alla categoria dei reati informatici, con tutto il precipitato di complessità e novità.

Il problema *cyber* terrorismo non è nato dopo l'11 settembre. Già molto tempo prima l'amministrazione USA, tra le altre, aveva espresso preoccupazioni al riguardo, pianificando degli investimenti[297].

In base agli studi americani del fenomeno, il reato di *cyberterrorism* è un contenitore di varie tipologie di reati, così individuabili:

1. *Virus*: assimilabili al concetto più noto nel campo della biologica ma applicabile anche all'informatica quanto al *genus* ed agli effetti. E' auto replicabile, fonte di danneggiamenti a programmi informatici o infetta altre applicazioni, non tutti i virus sono distruttivi;
2. *Worms*: sono simili ai virus, si autoriproducono, non necessitano di divenire parte integrante di un altro programma informatico. Gli effetti principali prodotti sono la cancellazione dei *files* dagli *host* oppure l'invio a parti terze di informazioni di sicurezza (come possono essere i codici di una carta di credito) degli *host*;
3. *Trojan Horses*: non attaccano altri *files* o programmi, non si autoriproducono e necessitano di essere trasferiti nello spazio ove poi provocano l'asportazione di *files* oppure la riconfigurazione dei *settings*;
4. *Spyware:* é un tipo di *trojan horse* che non attacca i *files* esistenti, non si autoriproduce. Quale effetto principale permette l'invio a fonti esterne di informazioni proprie dell'utente e può produrre anche la riconfigurazione di alcuni *settings* del computer. In linea generale si può dire che non provoca danni all'apparato informatico ma si insinua insidiosamente nelle maglie dello strumento senza che l'utente ne prenda coscienza e conoscenza;
5. *Spam*: genera scompensi al computer nel suo funzionamento, per esempio sovraffollando gli *in-boxes* oppure visualizzando continue finestre *pop-up* e allungando i tempi dell'utente per compiere una qualsiasi attività compiute con l'uso del computer.

Gli Stati Uniti d'America sono il Paese che più ha avuto esperienza di attacchi di *cyberterrorism* già a partire dagli Anni Novanta del secolo scorso: nel

---

1990; L. BAUCCIO *L'accertamento del fatto reato di terrorismo internazionale*, Giuffré, 2006; V. MUSACCHIO *Le strategie di lotta al terrorismo internazionale* in *Rivista Penale*, n. 3, 2006, pagg. 273-280; A. PECCIOLI *Il terrorismo quale settore chiave per l'armonizzazione del diritto penale* in *Diritto Penale e Processo*, n. 6, 2007, pagg. 801-807; F. VIGANO' *Terrorismo, guerra e sistema penale* in *Rivista Italiana di diritto e procedura penale*, 2006, pagg. 648-703; G. FLORA *Profili penali del terrorismo internazionale tra delirio di onnipotenza e sindrome di auto castrazione* in *Rivista Italiana di diritto e procedura penale*, 2008, pagg. 62-74.

[297] Si veda C. DI FEDE *Una valutazione dell'apporto della rete all'azione terroristica* in *Rivista trimestrale di Scienza dell'Amministrazione*, n. 3, 2004, pagg. 63-69.

1997 un *hacker* è riuscito a disabilitare la torre di controllo del *Mass Airport*, causando disservizi notevoli sebbene siano stati scongiurati miracolosamente gli incidenti tra velivoli; nel 1998 un altro *hacker* ha avuto accesso a dati ed informazioni personali contenuti presso i server del Dipartimento della Difesa americano; il 1998 è stato teatro anche di altri plurimi attacchi a sistemi informatici di università, della NASA, della Marina; nel 2001 si è verificato un accesso abusivo agli ID personali del sistema bancario del *Treasure Department*.

Il concetto stesso di terrorismo informatico è ritornato al centro dell'attenzione giuridica mondiale in particolar modo da quando si è avuta notizia di una informatizzazione dei membri della rete terroristica di Al-Qaeda, i quali, dunque, hanno cominciato a far circolare informazioni on-*line* e così acquisire proseliti ma anche organizzare attacchi. Pare infatti che, capofila di azioni terroristiche informatiche, sia tale Younis Tsouli, fautore di operazioni di intrusione in server, specie dello Stato USA, per postarvi materiale da diffondere, quale istruzioni per la costruzione di ordigni, video di addestramento e altri documenti di propaganda terroristica, nonché per pubblicare una lista di server vulnerabili, con indicazione del modo di accesso e pubblicazione di contenuti su tali sistemi non molto protetti.

Gli obiettivi informatici dei *cyberterrorist* vengono colpiti con attacchi distruttivi o semplicemente intrusivi, specie quando attengono ad infrastrutture critiche mirate per le quali si vuole ridurre l'efficacia e la funzionalità strutturale.

Un attacco ad un sistema può essere effettuato, in linea generale, secondo due differenti modalità d'azione: un attacco parzialmente informatico allorquando per effettuare l'intrusione si sia resa necessaria l'acquisizione di informazioni anche in ambiente fisico; un attacco solo digitale allorquando l'*hacker* terrorista opera solo all'interno delle reti telematiche.

Gabriel Weimann ha individuato almeno otto modi diversi in cui i terroristi fanno uso di internet per raggiungere i propri scopi: sfruttamento della potenzialità mediatica e dell'espansione territoriale di internet, creazione di siti web *ad hoc*, rapida modifica del *format* o immediata cancellazione dei siti, facile raggiungimento di nuovi adepti, come di nemici pubblici e dell'opinione pubblica internazionale sono le forme più tradizionali d'uso di internet da parte di singoli e gruppi terroristici.

I terroristi spesso combinano l'uso della rete a fini di propaganda con l'utilizzo delle tecnologie per generare il cd. *phsycological warfare*, amplificando lo stato di terrore dell'opinione pubblica mediante video, audio, CD-ROM, DVD, fotografie e annunci[298].

[298] Ne è prova il fatto che, a seguito dell'attacco alle Torri Gemelli l'11 settembre 2001, Al Quaeda, a mezzo internet, ha espresso la propria soddisfazione per l'azione compiuta non solo per i danni materiali causati ma anche e soprattutto per il generale panico e senso di terrore diffusosi tra la gente.

Altro modo di utilizzo della rete è il cd. *data mining*: in internet i terroristi trovano una pluralità di informazioni utili per la realizzazione delle loro azioni e dei loro fini come i sistemi di funzionamenti di servizi e infrastrutture statali critiche.

Anche i terroristi, come altre organizzazioni politiche, cercano i fondi in rete, chiedendo ai propri adepti di fare delle donazioni per la realizzazione degli scopi del gruppo ed inoltre mediante la rete organizzano attacchi, pianificano le attività, mantengono contatti tra membri delle stesse cellule o tra cellule diverse, scambiano e condividono informazioni.

Non bisogna però confondere ogni attività compiuta in internet da terroristi con la fattispecie di *cyberterrorism*.

La Decisione quadro del Consiglio europeo 2002/475/JHA, all'art. 2 definisce le offese che possono essere correlate ad un gruppo terrorista. In base a tale disposizione, un gruppo terrorista è configurabile come un gruppo strutturato e composto di più di due persone, stabilito da un certo periodo di tempo e che agisce in concertazione per realizzare degli atti offensivi criminali di stampo terroristico. Il gruppo quindi deve essere strutturato, cioè non formato per l'occasione nell'immediatezza della realizzazione dell'offesa, indipendentemente dalla presenza o meno di una definizione formale dei ruoli dei singoli membri stabili e continuativi dell'organizzazione.

Gli esperti Europol confermano l'assoluta carenza di una definizione comunemente accettata di *cyberterrorism* e offrono un primo appoggio in tal senso, con lo scopo precipuo di tracciare i contorni di una realtà ancora da studiare: « *cyberterrorism is the premeditated use of disruptive activities, or the torea thereof, against computer and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives* »[299].

In base agli studi effettuati dall'Agenzia di Polizia dell'Unione Europea sarebbero gli estremisti islamici ad essere i massimi utilizzatori della tecnologia informatica e telematica per il raggiungimento dei propri scopi criminali, specie per il rapporto tra i bassi costi nella gestione delle operazione e, allo stato, ancora uno *standard* di rischio minori rispetto alle tradizionali forme di offesa[300].

---

[299] Il riferimento è al testo redatto e pubblicato sul sito internet di Europol dal titolo "*high tech crimes within the eu: old crimes new tools, new crimes new tools. threat assessment 2007 - high tech crime centre*".

[300] Si invita alla lettura di G. OLIMPO La *testa del serpente. Tutti i segreti di Osama Bin Laden*, Nuovo Istituto Italiano d'Arti Grafiche, 2011. L'Autore, corrispondente de Il Corriere della Sera, ha seguito da vicino, a livello di attività giornalistica, le vicende che hanno coinvolto Al Qaeda, Osama Bin Laden e tutta l'organizzazione estremista islamica facente a lui capo. Nel raccontare, per immagini e suggestioni, nello stile che è proprio del giornalista, Guido Olimpo ricorda il crescente utilizzo dei mezzi di comunicazione di natura tecnologica da parte di Bin Laden e dei suoi Collaboratori, inviando messaggi

Non sempre gli utilizzatori della tecnologia sono membri dei gruppi terroristici o sono dei terroristi ma spesso sono semplicemente degli esperti assoldati per compiere una particolare e specifica attività illecita.

La rete internet, in particolare, è molto sfruttata dai terroristi informatici per la varietà di opportunità date ai fini del raggiungimento di uno considerevole numero di obiettivi differenti.

La realtà contemporanea, destinata a rappresentare non solo il presente ma anche e sempre di più il futuro, è caratterizzata da un incremento degli attacchi terroristici informatici, in tutte le diverse forme descritte.

I *cyberterrorists* utilizzano, in particolare, programmi per comunicazioni anonime come *FreeNet* o il *proxy server Tor* per *web browser*.

Così come la prevenzione e lotta al terrorismo sono una priorità nazionale, comunitaria e internazionale, il terrorismo informatico rappresenta una realtà allarmante che richiede delle strategie d'intervento ancora più complesse, poiché contiene non solo le potenzialità offensive di un attacco terroristico tradizionale ma anche le criticità proprie dei reati informatici, in continuo e costante sviluppo ed evoluzione.

5 *Le garanzie nella circolazione della prova digitale e la sicurezza delle infrastrutture*

Come si è già avuto modo di sottolineare, l'aumento della criminalità transfrontaliera è una realtà ed una costante nel diritto penale nazionale, comunitario e internazionale. Sempre più spesso le autorità investigative necessitano e richiedono l'intervento ausiliario di altre autorità presenti in un diverso territorio nazionale.

Questo può accadere perché un fatto criminale si è sviluppato oltre i confini nazionali dello Stato procedente ovvero semplicemente perché alcune prove utili ai fini dell'esercizio dell'azione penale sono collocate all'estero o sono acquisibili in terra straniera, oppure ancora perché un reato coinvolge soggetti di nazionalità diversa o che hanno lasciato una qualche traccia di sé un in altro Stato, utile per gli inquirenti.

In conseguenza di un tale scenario, un'autorità è chiamata a richiedere ad un'altra autorità, collocata geograficamente in un'altra zona, un intervento cooperativo nell'acquisizione della prova e quindi nella sua circolazione verso il soggetto richiedente.

Con stretto riferimento alla prova digitale, se preliminarmente è richiesto che essa sia acquisita secondo delle *best practices* di intervento, per evitare di

---

scritti e video messaggi in internet, ma anche celando informazioni riservate e istruzioni per la costruzione di bombe o per la realizzazione di attacchi terroristici mediante testi e immagini criptate.

minare alla integrità e genuinità, anche l'archiviazione e la circolazione della prova stessa deve avvenire per mezzo di strutture all'uopo istituite e secondo modalità che possano garantire massimamente una raccolta ed un transito sicuro dei dati.

La materia della sicurezza richiede, da parte dei tecnici specializzati, un continuo sforzo di studio e ricerca al fine di monitorare l'evoluzione dei modi e delle forme di aggressione alla struttura ed al funzionamento delle infrastrutture informatico-telematiche.

La crittografia, da intendersi come l'arte e la scienza delle scritture segrete[301], è diffusa nella *information security* come nel mondo criminale. In molti casi essa rappresenta l'unico modo per salvaguardare efficacemente l'informazione.

Una cifratura "*link by link*" assicura che la massa di informazioni circoli completamente cifrata[302].

Nel periodo del secondo dopoguerra, la crittografia rappresentava una tecnologia prettamente militare, per funzione ed applicazioni, ma il progresso dei mezzi di informazione e comunicazione ne ha determinato la diffusione anche in campo civile[303].

5.1 Il rapporto pubblico-privato per lo sviluppo delle infrastrutture: un incontro tra esigenze di pubblica sicurezza e di sviluppo economico

Lo sviluppo della sicurezza informatica prende corpo dalla presa di coscienza della necessità di proteggere i sistemi da attacchi che vanno a colpire le vulnerabilità delle infrastrutture di sistema , sia nel pubblico sia nel privato.

Basti considerare, a titolo di esempio, la crescente sensibilità sviluppata in Italia già agli inizi degli anni '90 a seguito della diffusione di analisi statistiche che riscontravano un *trend* in crescita degli attacchi informatico-telematici segnalati, in specie, al CERT-IT.

Negli USA la tensione è tanto più alta e sono registrati attacchi quotidiani di *worm*, *Trojan*, *virus*. L'*Institute for Security Technologies Studies* monitora

[301] Così C. GIUSTOZZI – A, MONTI – E. ZIMUEL, *Segreti, spie e codici cifrati*, Apogeo, 1999.

[302] Si registrano molti protocolli di cifratura, innovati periodicamente, afferenti sia la fase statica del dato che il trasporto, per facilitare comunicazioni sicure tra le parti nella rete.
Per un approfondimento sul tema della crittografia si rinvia a G. ZICCARDI *Crittografia e diritto*, Giappichelli 2003.

[303] La diffusione dei sistemi crittografici in campo civile è stata determinata anche da un alleggerimento dei controlli nell'industria e nell'esportazione di prodotti che utilizzano determinate chiavi non più lunghe di 40 bit. Così, G. ZICCARDI *op.cit,* pagg. 20-22.

costantemente queste manifestazioni criminose e ha dimostrato la correlazione fra conflitti militari e politici e l'incidenza del cyberterrorismo [304].

Le vulnerabilità delle infrastrutture tecnologiche richiedono la predisposizione di sistemi di prevenzione, oltre agli interventi per il ripristino della situazione antecedente all'attacco.

È necessario intervenire nell'investimento di pacchetti di programmi di sicurezza che possano proteggere il più possibile dagli assalti criminogeni.

Per approntare delle forme di prevenzioni sempre più efficaci e tempestive è necessario coniugare lo sforzo delle aziende e dei ricercatori che operano in questo particolare e delicato settore, ma è altresì necessario che la cifra nera dei reati che minano alla sicurezza si abbatta e che, quindi, il numero delle denunce cresca [305].

Spesso l'intervento delle autorità inquirenti ,con conseguente sequestro di *software* infetti e isolamento delle vulnerabilità [306], permette di evitare numerosi ulteriori incidenti, come la propagazione in larga scala dei virus.

L'argomento della sicurezza informatica, intesa come confidenzialità, integrità e disponibilità dei dati e delle risorse informatiche in generale, si è sviluppato di pari passo all'evoluzione dei modelli di *standard* per la sicurezza. Le tematiche principali attengono all'interoperabilità di sistema, alla corretta modellazione e strutturazione delle infrastrutture e delle applicazioni, oltre agli aspetti strettamente afferenti le garanzie della sicurezza.

Il maggiore o minore grado di intelleggibilità di dati e programmi dipendono dalle tecniche crittografiche utilizzate e sono queste stesse che permettono, pur in presenza di una fragilità dei contenuti di elaboratori elettronici, di ottenere il massimo grado di tutela dell'autenticità del documento, anche per non alternane la rilevanza giuridica.

La crittografia è una tecnica che permette, con l'aiuto di un algoritmo matematico, di trasformare un messaggio leggibile in una forma non leggibile, mediante l'applicazione di una chiave segreta. Con l'operazione inversa, applicando lo stesso algoritmo e la stessa chiave al messaggio cifrato, è possibile tornare al testo originale [307].

---

[304] Sul punto www.ists.org.

[305] È logico pensare che gli enti pubblici come le industrie private tendano a tenere nascoste le notizie che riguardano attacchi informatici, sottrazione, dispersione o cancellazione di dati anche per il risvolto negativo sull'opinione pubblica e sul comune senso di sicurezza e affidamento.

[306] Sul punto *EUROPOL high tech crimes Within the eu: old crimes new tools, new crimes new tools threat assessment 2007* in *www.europol.europa.eu.*

[307] Questa tecnica che appare così sofisticata, rappresenta un'evoluzione nei secoli di rudimentali applicazioni per ottenere messaggi cifrati, a partire dall'Antico Egitto. Lo sviluppo di questa tecnica bene rappresenta la tensione umana esistente fra chi inventa metodi sempre più sofisticati per trasmettere informazioni in modo intellegibile e chi fa tutto per violare questa segretezza, decriptando i testi per scoprirne il significato nascosto. La crittografia già rappresenta un secondo stadio evolutivo se messa in

L'uso della crittografia asimmetrica, parallelamente alla funzione di *hash*, sono utilizzate sul documento trasmesso, al fine di assicurarne la provenienza e di renderne accessibile il contenuto al destinatario finale, il quale soltanto possiede la chiave idonea a rendere leggibile il testo.

Per lo stesso fine soccorre la previsione delle cd. chiavi biometriche che regolano l'accesso a sistemi informatici mediante il riconoscimento personale di un dato, un dispositivo o una caratteristica fisica e comportamentale [308].

Queste possono essere applicate anche in combinato con le chiavi crittografiche, per ottenere una forma avanzata di sicurezza dei dati.

Le tecniche di cifratura, elaborate e sviluppate per proteggere dati e documenti informatici, specie durante la fase di trasmissione attraverso le reti telematiche rappresentato un valido supporto per assicurarne i contenuti e per permettere un valido utilizzo in sede giudiziaria [309].

Nell'ambito delle politiche di controllo della crittografia l'OECD (*Organisation for Economic Co-operation and Development*), dal 1996, ha messo a punto delle linee guida che, nel 1997, hanno ricevuto forma definitiva nella *Recommendation of the Council concerning Guidelines for Cryptography Policy*.

La crittografia non rappresenta l'unica fonte di sicurezza di dati e informazioni. Anche la steganografia, che si tende comunque a considerare come una tecnica ormai superata, in alcuni casi può risultare determinante, specie se utilizzata parallelamente alla criptazione [310].

Non basta, però, assicurare l'implementazione di determinate funzionalità ad un qualsiasi sistema informatico, come può essere anche una banca dati, ma è necessario garantirne l'invulnerabilità, in relazione all'utilizzo che ne viene fatto.

---

corrispondenza con la steganografia. Se quest'ultima, infatti, avevo lo scopo di nascondere il messaggio in sé, la criptazione si sostanzia invece nella non leggibilità del contenuto.
Così, S. SINGH *Codici & segreti*, BUR, 1999.

[308] Vi sono parecchi dispositivi in commercio che applicano il riconoscimento mediante il controllo della retina o dell'impronta digitale precedentemente registrata.

[309] Per la materia di cui ci si occupa in questa ricerca, è importante segnalare che nel testo dell'8 ottobre 1997, COM(1997) 53, già era indicato l'obiettivo di armonizzare le differenti legislazioni entro il 2000, al fine di assicurare il mutuo riconoscimento delle firme digitali.
Sul tema si rinvia a http://europa.eu.int/eur-lex/it/register2.html e http://www2.echo.lu (siti consultati in data 30 novembre 2010).

[310] Così la steganografia come la crittografia sono delle tecniche che, su altro versante, sono applicate per agevolare operazioni criminali. E' molto utilizzata anche la forma di manipolazione delle immagini, specie nei reati di pedopornografia, laddove il criminale nasconde delle foto pedopornografiche dietro ad altre apparentemente "lecite". Questa pratica risulta essere molto diffusa in Germania, tanto che la *German BKA* si è dotata di personale esperto nelle procedure di riconoscimento di questa manipolazione di fotografie che, in realtà, nascondono materiale pedopornografico.

Molti enti governativi hanno adottato dei criteri di valutazione e tutela della sicurezza[311] che rappresentavano nient'altro che delle regole di indirizzo, prive di valore normativo.

Per iniziativa della Comunità Europea si sono sviluppati dei gruppi di studio per la formulazione di *Common Criteria* che riguardano alcune funzionalità specifiche e le architetture di comunicazione generale: il riferimento, in particolare, è alla certificazione dei sistemi ISO[312].

Ancora troppo spesso l'investimento nella sicurezza delle infrastrutture informatico è considerato, erroneamente, uno spreco ingiustificato di denaro, così svalutandone gli enormi benefici che può generare nel breve o nel lungo periodo, quali un maggior senso di fiducia ed affidamento della società e, per quanto qui di interesse specifico, una circolazione di dati e prove integri e genuini.

Le misure di sicurezza in ambiente informatico sono gli unici mezzi attraverso cui creare una sorta di "*surrogato della perimetrazione muraria o della delimitazione spaziale connaturata al domicilio tradizionale* "[313] per i fini di protezione delle informazioni.

Questi parametri possono essere costituiti da chiavi metalliche per l'accensione dei computer e dei terminali; *badge* per l'autenticazione o identificazione dell'utente abilitato all'accesso; chiavi logiche per l'accesso agli archivi; sistemi biometrici di riconoscimento che abilitano all'accesso. È anche frequente l'impiego, nei sistemi ad elevata complessità, di livelli differenti di interdizione di area e funzione, ciascuno assistito da autonome misure di sicurezza[314].

La difficoltà maggiore nel proteggere i dati consiste nella valutazione di tutte le possibili situazioni che possono minare alla sicurezza delle infrastrutture, sebbene non è possibile prevedere ogni attacco.

---

[311] *Ibidem*.

[312] La norma ISO 27001 specifica i requisiti di sicurezza dei sistemi informativi che devono essere soddisfatti da ogni organizzazione che intenda dotarsi di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI).
L'applicazione di tali requisiti garantisce la riduzione dei fattori di rischio della sicurezza dei sistemi informativi e ne assicura l'affidabilità.
Lo standard ISO/IEC 27002 stabilisce che la sicurezza dell'informazione è caratterizzata da integrità, riservatezza e disponibilità. È stato emesso nel 2007 dall'Organizzazione internazionale per la normazione e dalla Commissione Elettrotecnica Internazionale, al termine di un lungo percorso di evoluzione iniziato con lo *standard* britannico BS7799 nel 1995, attraverso anche l'ISO/IEC 17799, ritirato in concomitanza con l'emissione del nuovo documento, meglio armonizzato con la serie ISO 27000 di *standard* sulla sicurezza delle informazioni.
La ISO 27037, la cui pubblicazione del testo è prevista per il 2012, prevede degli standard per alcune attività tipiche di computer forensics, in relazione alla raccolta di alcuni tipi di prove informatiche.

[313] Cfr L. CUOMO – R. RAZZANTE *La disciplina dei reati informatici*, Giappichelli, 2006.

[314] *Ibidem*.

Le tecniche di tutela della sicurezza informatica intervengono dal punto di vista fisico, per quanto attiene alla sicurezza dei terminali da cui nasce il dato e dal punto di vista procedurale, ovvero sulla regolamentazione da attuare per la protezione dei dati, dalla genesi all'archiviazione e alla circolazione.

I metodi matematici o informatici, dal punto di vista tecnico, garantiscono una serie di proprietà di sicurezza, rappresentate dalla disponibilità dei dati, dalla loro integrità e confidenzialità. Anche l'autenticazione è un'attività di sicurezza rilevante per individuare il mittente ed il destinatario legittimati., così come il principio non ripudio, cioè il metodo attraverso cui si garantisce la fonte da cui proviene una determinata informazione circolata.

Già la Direttiva 95/46/ CE sul trattamento dei dati personali e la libera circolazione, nel *considerandum* 25, evidenzia l'importanza della garanzia della sicurezza tecnica per la tutela delle informazioni apprese, archiviate e trattati. Lo stesso riferimento si trova anche nella Direttiva 2002/58/ CE del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, in particolare al punto 9.

Il regolamento CE 45/2001 all'art. 22 analizza in modo specifico e dettagliato i possibili rischi e le misure di sicurezza da adottare nel trattamento dei dati. E' necessario valutare le criticità del singolo caso per adattare la tutela dei rischi alla natura dei dati personali da proteggere. La finalità da perseguire è quella di evitare la divulgazione o l'accesso non autorizzati, la distruzione accidentale o illecita o la perdita accidentale o l'alterazione dei dati, nonché impedire qualsiasi altra forma illecita di trattamento. In particolare, in caso di trattamento automatizzato dei dati personali devono essere adottate le misure idonee per evitare che i soggetti non autorizzati accedano ai sistemi informatici utilizzati per il trattamento; evitare forme non autorizzate di lettura, riproduzione, alterazione o rimozione dei supporti di memorizzazione; evitare immissioni non autorizzate di dati di memoria nonché ogni divulgazione, alterazione o cancellazione; evitare che persone non autorizzate utilizzino i sistemi di trattamento dei dati avvalendosi di infrastrutture destinate alla trasmissione dei dati; assicurare che le persone accedano soltanto ai dati per cui sono autorizzati; registrare i dati che sono stati comunicati, in quale momento e a chi; assicurare che nel corso della procedura di comunicazione di dati personale e nel corso del loro trasferimento i dati non possano essere letti, copia, alterati, cancellati; strutturare organismi e istituzioni in modo da soddisfare le esigenze di protezione dei dati.

Come sottolineato nella Comunicazione della Commissione al Parlamento europeo, al Consiglio e al Comitato delle Regioni, COM(2007) 267

definitivo, la sicurezza delle infrastrutture informatiche è centrale per la lotta alla cibercriminalità.

Questa Comunicazione rafforza e consolida la comunicazione del 2001 « *creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica* » (COM(2000)890 definitivo) che proponeva l'adozione di disposizioni di diritto penale sostanziale e procedurale adeguate per contrastare le attività criminali transnazionali e nazionali. A tale comunicazione ha fatto seguito la previsione di una decisione quadro 2005/222/GAI relativa agli attacchi contro i sistemi d'informazione[315].

La Comunità europea si è fatta portatrice di un progetto unitario di sfida per la garanzia della sicurezza delle reti e dell'informazione che si articola nella lotta alla cibercriminalità, nella previsione di misure specifiche per la sicurezza delle reti e delle informazioni, in un quadro normativo di tutela delle comunicazioni elettroniche.

Questa politica è stata oggetto di un crescente sviluppo in ambito comunitario non solo con la già menzionata Direttiva 2002/58/CE ma anche mediante l'adozione della Comunicazione COM(2001)298 dal titolo "*Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*", della Comunicazione COM(2006) 251 in tema di "*Strategia per una società dell'informazione sicura*", della Comunicazione COM(2006) 688 sulla lotta contro le comunicazioni commerciali indesiderate, i programmi spia e i *software* maligni, del Regolamento CE 460/2004 del Parlamento e del Consiglio, del 10 marzo 2004, che costituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.

Le tecnologie dell'informazione e delle comunicazioni e la loro sicurezza figurano tra gli obiettivi del Settimo programma quadro di ricerca dell'UE, operativo dal 2007 al 2013, come elemento essenziale per la lotta alla cibercriminalità.

Il programma finanziario della Commissione europea "*prevenzione e lotta contro la criminalità*", tra gli altri progetti finanzia l'avviamento di azioni pubblico/privato che sensibilizzino ai costi e ai pericoli della cibercriminalità, concentrandosi su una descrizione degli aspetti negativi dell'assenza di sicurezza delle infrastrutture e delle comunicazioni. È agevolato lo studio e l'esame, da parte della Commissione assieme agli Stati membri, del fenomeno degli attacchi coordinati e su larga scala contro le infrastrutture di informazioni statali, al fine di prevenirli e combatterli, anche con risposte coordinate e

[315] Sono seguite l'adozione di decisioni quadro in alcune materie specifiche, riferite a particolari forme di criminalità informatica quali la decisione quadro 2001/413/GAI relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti; decisione quadro 2004/68/GAI relativa alla lotta allo sfruttamento sessuale dei bambini e la pornografia infantile.

condividendo le informazioni e le migliori pratiche utilizzate o sviluppate. La Commissione promuove e finanzia la conclusione di accordi volontari e convenzioni a livello comunitario tra autorità pubbliche e operatori privati, in particolare ISP, sulle procedure di prevenzione e repressione delle forme di criminalità legate alla circolazione di dati ottenuti illegalmente.

Il Consiglio europeo, riunitosi l'11 e 12 dicembre 2008, ha rinnovato la volontà di imprimere un nuovo impulso alla politica europea di sicurezza e di difesa, per rispondere alle nuove sfide dello sviluppo della criminalità transfrontaliera. Preliminarmente il Consiglio ha riaffermato la centralità del Trattato di Lisbona laddove contribuisce ad un funzionamento più efficace, democratico ed efficiente dell'Unione europea, specie in seguito all'allargamento agli Stati dell'Europa dell'Est. Il Trattato di Lisbona, che modifica il Trattato sull'Unione europea e il Trattato che istituisce la Comunità europea, pone come obiettivo primario dell'Unione la creazione di uno spazio di libertà, sicurezza e giustizia per i cittadini, contribuendo alla pace, alla sicurezza e alla tutela dei diritti umani (art. 2 e art. 6). Tali obiettivi sono stati reiterati nelle conclusioni della succitata riunione del Consiglio, nell'ambito della quale è stata rinnovato il progetto di sviluppo della politica europea di sicurezza.

In maniera conforme, il Programma di Stoccolma del 2 dicembre 2009 incentiva l'evoluzione degli strumenti di sicurezza interna ed esterna, al fine di creare quella che viene qualificata dal Consiglio europeo come "*A Europe that protects*", "*Un'Europa che protegge*". La lettera del punto 2.5 del citato Programma evidenzia un'attenzione particolare alla protezione della *privacy* e dei dati personali, in osservanza alle disposizioni della Carta dei Diritti Fondamentali dell'Unione.

L'UE è chiamata a rispondere alle esigenze legate all' intensificazione (necessaria) della circolazione e dello scambio di dati e di informazioni all'interno dello spazio giudiziario comunitario ed extracomunitario. Essa promuove l'applicazione degli strumenti comunitari di protezione dei dati e la conformità alle Carte e alle Convenzioni che tutelano il diritto alla riservatezza delle informazioni.

Il Consiglio europeo, come precisato nel Programma di Stoccolma, ritiene che lo sviluppo tecnologico rappresenti una sfida da affrontare per incrementare la protezione dei dati personali. Tra i principi basilari individuati in questo contesto vi è la necessità di introdurre limitazioni, di monitorare la proporzionalità, la legittimazione e i limiti temporali di raccolta ed archiviazione dei dati, nel rispetto dei diritti di ogni singolo individuo. Il diritto alla protezione dei dati può essere meglio tutelato dallo sviluppo di nuove tecnologie che si adeguino all'evoluzione della cibercriminalità, agevolando la

cooperazione tra settore pubblico e settore privato, specie nell'ambito della ricerca.

Il piano di azione del Programma di Stoccolma 2010-2014 prevede delle tappe di sviluppo coerente di tutti i sistemi d'informazione presenti e futuri [316].

La Commissione europea ha affrontato nuovamente il tema dell'evoluzione degli *standard* di sicurezza delle infrastrutture, come fine per la maggiore protezione dei dati personali, mediante una Comunicazione rivolta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni del 4 novembre 2010, COM(2010) 609 definitivo. Al punto 2.4.2 di tale atto è ribadita l'importanza di promuovere dei principi fondamentali e di consolidare il ruolo trainante dell'Unione europea per la formazione di regole giuridiche e tecniche per la protezione dei dati personali, da applicare in ambito internazionale. La Commissione invita a seguire con particolare attenzione lo sviluppo delle norme tecniche internazionali messe a punto dagli organismi come il CEN e l'ISO per verificare concretamente la loro efficacia giuridica e l'effettività sul piano operativo di protezione di dati.

Il Gruppo di lavoro articolo 29 può assumere un ruolo determinante nell'espletamento delle sue funzioni consultive, ma anche contribuendo all'applicazione uniforme negli Stati membri delle norme di protezione dei dati personali.

Nella Comunicazione COM(2010) 609 definitivo, la Commissione si è proposta di mettere a punto misure non legislative, attraverso lo studio di fattibilità della promozione di marchi europei di certificazione.

In questo contesto sono stati compiuti passi importanti, come la costituzione di un gruppo multilaterale di aziende, organizzazioni della società civile (comprendenti associazioni per i diritti umani e per la libertà di stampa), investitori e accademici che hanno stretto una collaborazione allo scopo di proteggere e far progredire la libertà di espressione e la tutela della vita privata nel settore delle TIC, dando vita alla *Global Network Initiative* (GNI) nell'ottobre del 2008[317], come ne dà atto la Raccomandazione del Parlamento europeo del 26 marzo 2009 sul rafforzamento della sicurezza e delle libertà fondamentali su Internet.

---

[316] Si veda il punto 5 rubricato Garantire la sicurezza in Europa.

[317] Si veda il sito http://www.globalnetworkinitiative.org/index.php. La menzionata iniziativa riguarda *All over the world – from the Americas to Europe to the Middle East to Africa and Asia – companies in the Information & Communications Technology (ICT) sector face increasing government pressure to comply with domestic laws and policies in ways that may conflict with the internationally recognized human rights of freedom of expression and privacy. In response, a multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics spent two years negotiating and creating a collaborative approach to protect and advance freedom of expression and privacy in the ICT sector, and have formed an Initiative to take this work forward.*

5.2 *Un progetto di regole comuni per la catalogazione e indicizzazione delle prove: l'individuazione di termini e tecniche di scelta condivisa*

Il Sostituto Procuratore della Repubblica presso il Tribunale di Trieste, dott. Federico Frezza, in un intervento ad un incontro di studi[318] ha così apprezzabilmente concluso: "*Solo andando a raccogliere prove all'estero e, corrispettivamente, fornendo agli altri Stati le nostre prove, si otterranno due risultati: in primo luogo si capiranno fenomeni dei quali, altrimenti, quasi neppure si sospetterebbe l'esistenza, e si raccoglieranno prove sull'intera catena criminale (…); in secondo luogo, quale effetto collaterale, l'azione repressiva avrà maggiore efficacia, in quanto gli Stati interessati, che vengono messi al corrente delle nostre indagini, agiranno direttamente nei confronti dei reati commessi nel loro territorio*".

Pur condividendo nella sostanza il pensiero espresso dal Pubblico Ministero, lo scenario che si vorrebbe realizzare non è tanto quello secondo cui ogni autorità inquirente si debba recare all'estero per raccogliere direttamente la prova, quanto una realtà in cui il buon funzionamento delle procedure di cooperazione tra forze di polizia permetta la circolazione rapida e, prima ancora, una comune catalogazione ed indicizzazione, dei dati, così da permetterne il riconoscimento all'accesso in un sistema di archivi e banche dati predisposte all'uopo.

Il fenomeno della criminalità transfrontaliera richiede, prima di tutto, un approccio comparatistico volto all'individuazione di modi, termini e soggetti legittimati ad avanzare una richiesta ad un'autorità straniera, con attenzione alla disciplina armonizzatrice del diritto comunitario. Non ogni Stato conosce e categorizza i medesimi tipi di prova, non ogni Stato riconosce e legittima le stesse forme di acquisizione della prova, non ogni Stato richiede le stesse garanzie nella formazione della prova. Oltre a questo, un ulteriore limite è posto dalla cd. babele delle lingue nazionali e, più ancora, dei microlinguaggi giuridici che costituiscono un ostacolo alla piena comprensione reciproca..

Le prove raccolte in un diverso Stato possono essere catalogate in formato elettronico, in archivi e banche dati nazionali accessibili da soggetti esterni legittimati. La forma scelta da ciascuno Stato per l'archiviazione e l'indicizzazione di questi dati incide sul grado di fruibilità e sul tempo impiegato per la visualizzazione, l'inoltro della richiesta e il recapito dei contenuti utili al destinatario richiedente.

La realizzazione del principio di disponibilità nell'ordinamento dell'Unione europea è ancora *in fieri,* sebbene era prevista già come obiettivo

[318] Cfr F. FREZZA 6/8 giugno 2005 intervenuto nell'incontro di studio sul tema "*Criminalità organizzata transnazionale: strumenti di contrasto e forme di cooperazione giudiziari"a* pag. 175-176 di F. CAJANi – G. COSTABILE – G. MAZZARACO *Phishing e furto d'identità digitale*, Giuffrè 2008.

del Programma dell'Aia, in materia di rafforzamento della libertà, della sicurezza e della giustizia e ancora più specificamente nell'Allegato II della Proposta di Decisione quadro del Consiglio europeo sullo scambio d'informazioni (COM(2005) 490 definitivo). Vi è traccia di questo principio anche nel testo della Convenzione di Strasburgo dell'8 novembre 1990 in materia di riciclaggio, nell'art. 30.1 della Convenzione di applicazione dell'Accordo di Schengen, nella Convenzione di Bruxelles del 2000 e nel Trattato di Prum del 27 maggio 2005 (a livello internazionale si segnala il riferimento al principio di disponibilità delle informazioni nella Convenzione di Palermo).

Il principio di disponibilità si basa sul mutuo riconoscimento in materia penale e mira a creare un *network*, composto dagli archivi nazionali e consultabile da tutti i soggetti che partecipano alla realizzazione di questo sistema, rendendo pienamente fruibili le informazioni utili alla prevenzione dei reati e alle indagini su fatti punibili[319].

La rete telematica può favorire, come supporto infrastrutturale, la raccolta e la circolazione di dati e prove giuridiche soltanto se sono applicati sistemi e tecniche valide per sfruttare al massimo la potenzialità della rete e facilitare la consultazione degli spazi telematici[320].

Già nel Programma di Tampere prendeva forma l'obiettivo dell'Unione europea di rilanciare l'integrazione comunitaria mediante l'evoluzione della cooperazione informativa. Nel Programma, più specificamente il Consiglio ha sancito il canone della libera circolazione delle informazioni, tracciando le direttrici per darvi attuazione.

Tra le linee principali d'intervento, il Consiglio ha auspicato un oculato investimento sulle tecnologie e sullo sviluppo di sistemi informativi centralizzati. Una gestione di tal sorta è caratterizzata da una struttura radiale, sorretta da una banca dati centrale (diretta da un organismo sovranazionale), collegata a plurime unità nazionali dislocate nei singoli Paesi UE. Accanto alla forma di cooperazione centralizzata o canalizzata, si colloca un diverso paradigma ispirato ad una logica di maggiore diffusività, cioè di scambio o accesso immediato e capillare ai dati. Questa differente strategia di condivisione è rintracciabile, sia pure in nuce, nella Convenzione sull'assistenza giudiziaria in materia penale, adottata dal Consiglio dell'Unione in data 29 maggio 2000, nel chiaro intento di sviluppare le forme cooperative accennate dalla Convenzione di Strasburgo del 20 aprile 1959.

---

[319] Cfr N. PARISI *Diritto processuale penale e profili internazionali* in *Studi in onore di Mario Pisani*, La Tribuna, 2010, pagg. 470 ss.

[320] Si veda P. SAMMARCO *Circolazione, contaminazione e armonizzazione nella disciplina delle nuove tecnologie della comunicazione* in *Diritto dell'informazione dell'informatica*, 2008, pag. 711 ss.

Risulta evidente il divario che intercorre tra queste direttrici pros pettiche e quella diretta ad una centralizzazione della raccolta e dell'analisi del dato, la quale risponde alla logica secondo cui i dati appartengono anzitutto all'autorità nazionale che li raccoglie e detiene, collocandosi in un momento successivo ed eventuale l'inserimento di questi in un sistema informativo transnazionale.

La Commissione europea, il 10 maggio 2005, ha rivolto una Comunicazione al Consiglio e al Parlamento europeo (COM(2005) 184 definitivo) per l'attuazione organica del Programma dell'Aia, predisponendo un documento allegato con l'elencazione delle misure e delle azioni concrete per i successivi cinque anni. Gli Stati sono stati sollecitati a rispettare scrupolosamente il principio di finalità limitata[321] e a distinguere le informazioni in categorie, a seconda dei diversi livelli di accuratezza del trattamento e di affidabilità delle fonti, nonché a provvedere affinché i dati raccolti risultino chiaramente distinguibili in ragione dello *status* dei soggetti a cui afferiscono[322]. La Commissione sposa, infatti, la logica della differenziazione per fare in modo che le informazioni archiviate seguano un certo ordine logico.

Nell'ottobre 2005 la Commissione ha preso una seconda iniziativa (COM(2005) 490 definitivo) ispirata al paradigma dello sviluppo della cooperazione informativa all'interno del territorio dell'Unione europea, permettendo la consultazione integrale e diretta *on-line* dei dati oppure assicurando l'accesso *on-line* ai soli dati di indice, cui potrà seguire una richiesta di trasmissione delle informazioni correlate. La proposta in analisi non è attenta soltanto alla *visibility* ma anche alla *readability* delle informazioni, facilitando con ciò una conoscenza effettiva e completa dell'informazione archiviata.

Il Trattato di Prum (Decisione Quadro 2008/615/GAI), avente l'obiettivo prioritario e pionieristico di raggiungere un elevato livello di cooperazione di polizia e giudiziaria, con particolare riferimento ai dati di DNA e all'immatricolazione di veicoli, ha fatto emergere una strategia di scambio di informazione di tutto rilievo. Ciascuno Stato ha l'obbligo di mantenere tre archivi nazionali centralizzati, contenenti il primo i profili DNA archiviati, il secondo le impronte digitali catalogate, il terzo le informazioni sui veicoli immatricolati. L'*information sharing* viene effettuato mediante l'accesso

[321] Secondo tale principio i dati dovranno essere rilevati per finalità determinate, esplicite e legittime nonché, successivamente, trattati non in modo incompatibile con tali finalità. V.S. CIAMPI *Principio di disponibilità e protezione dei dati personali nel terzo pilastro dell'Unione europea* in *Cooperazione informativa e giustizia penale nell'Unione europea*, a cura di Francesco Peroni e Mitja Gialuz, Fondazione CRTrieste, 2009.

[322] Ad esempio saranno distinte le persone sospettate di aver commesso un reato, dalle persone condannate in sede penale, dalle persone che danno adito a ritenere che commetteranno un reato perché sono state acquisite pregresse notizie di reato a loro carico.

automatizzato a certe categorie di informazioni disponibili *on-line* (in genere i soli dati di indice) o mediante il trasferimento delle informazioni richieste, a seguito di una domanda dettagliata avanzata da un'autorità di contrasto al proprio omologo di oltre confine. L'indice associa al profilo di DNA oggetto della ricerca un numero di riferimento utilizzabile per accedere alle ulteriori informazioni archiviate. L'accesso *on-line* alla banca dati DNA avviene alternativamente per consultazione o comparazione.

Il generale meccanismo applicato, incentrato sulla domanda-risposta e non sull'accesso diretto *on-line*, non traduce in atto i profili di maggiore originalità insiti nel Programma dell'Aia, quanto alle direttive sull'accesso reciproco e l'interoperabilità tra le basi di dati nazionali. L'accesso diretto *on-line* è sinonimo di disponibilità pura e trova ostacolo attuativo nel sentimento di gelosia degli Stati membri e nella mancanza di una piena fiducia reciproca.

Non si manca di considerare un altro problema rilevante. La cooperazione tra gli Stati e la libera circolazione delle prove non possono trovare piena applicazione in assenza delle infrastrutture idonee all'individuazione del *locus* corretto dove avanzare la richiesta. Questo limite è stato rilevato nel testo del Libro Bianco del 2005, in particolare in tema di accesso alle informazioni del casellario sulle condanne all'estero. È nata l'idea della costruzione di un archivio centralizzato per ovviare ai menzionati ostacoli.

Sotto il profilo delle modalità di comunicazione, è auspicabile l'applicazione (come del resto avviene, per esempio, per il sistema del casellario) dell'interconnessione mediante un'infrastruttura che permetta la trasmissione delle informazioni, ove possibili, in via telematica [323].

L'esempio della libera circolazione delle informazioni estratte dai casellari nazionali è sicuramente un buon paradigma di riferimento perché attua un canone di mutuo riconoscimento e di fiducia reciproca che può soddisfare dal punto di vista strettamente tecnico, relativamente alle modalità di catalogazione e per il modello *hit/no hit* di accesso ai dati, seppure ancora carente dal punto di vista della protezione dei dati personali e dell'armonizzazione delle garanzie processuali.

Nel già menzionato Libro Bianco del 2005 in tema di casellario europeo, è emerso un ulteriore e rilevante limite della banca dati sulle condanne penali che, più in generale, è un limite che affligge l'ordinamento comunitario, anche in materia penale e che pone un freno all'attuazione piena della cooperazione di polizia e giudiziaria. Questo riguarda le difficoltà di comunicazione e scambio allorché i dati, le informazioni, le prove restano espresse nella forma linguistica dello Stato da cui provengono.

[323] Il sistema TESTA - *Trans-European services for telematics between Administrations* - è già utilizzato e testato dalla Commissione europea.

L'Unione europea, nel contesto del progetto di armonizzazione delle legislazioni degli Stati membri, ha iniziato ad occuparsi più da vicino del problema del linguaggio.

Le istituzioni comunitarie hanno da sempre un ufficio che coinvolge linguisti e giuristi di ciascun Paese dell'Unione europea [324].

Attualmente le lingue ufficiali dell'Unione sono ventitre[325] ed ogni atto, sebbene i lavori si svolgano in lingua inglese, francese o tedesca,sono tradotti in ciascuna lingua.

L'Europa da sempre incoraggia il multilinguismo, lo studio e la conoscenza di tutte le lingue ufficiali, anche mediante la destinazione di fondi a tale scopo, poiché il linguaggio è considerato, prima di tutto, lo specchio di una cultura che deve essere salvaguardata come patrimonio nazionale e dell'intera umanità e come segno tangibile dell'identità di un popolo[326]. Per motivi di tempo e di risorse finanziarie è invece limitato il numero dei documenti di lavoro tradotti in tutte le lingue. La Commissione europea ha adottato l'inglese, il francese e il tedesco come lingue procedurali, mentre il Parlamento europeo fa tradurre i suoi documenti a seconda delle necessità dei parlamentari [327].

---

[324] Si veda in particolare il Servizio giuridico della Commissione europea.

[325] Le 23 lingue ufficiali e di lavoro sono : bulgaro, ceco, danese, estone, finlandese, francese, greco, inglese, irlandese, italiano, lettone, lituano, maltese, olandese, polacco, portoghese, rumeno, slovacco, sloveno, spagnolo, svedese, tedesco e ungherese. Il primo regolamento comunitario che stabilisce quali sono le lingue ufficiali e di lavoro è del 1958 e indica l'olandese, il francese, il tedesco e l'italiano, in quanto lingue degli Stati membri dell'epoca. Da allora, molti altri Paesi sono entrati nell'UE, per cui il numero delle lingue ufficiali e di lavoro è aumentato. Le lingue continuano però a essere meno numerose degli Stati membri, poiché alcune sono usate in più paesi: ad esempio, in Belgio le lingue ufficiali sono l'olandese, il francese e il tedesco, mentre a Cipro la maggioranza della popolazione parla in greco. http://ec.europa.eu/education/languages/languages-of-europe/doc135_it.htm.

[326] Si ricorda che con il Trattato di Maastricht anche la cultura è entrata a far parte delle materie di competenza comunitaria.

[327] Eurobarometro, il servizio di sondaggi e analisi della Commissione europea, ha realizzato due progetti di ricerca sulle competenze linguistiche dei cittadini europei e i loro atteggiamenti nei confronti delle lingue.

I sondaggi si sono svolti nel 2001 e nel 2006, con un intervallo di tempo sufficiente per rilevare eventuali cambiamenti. A causa dell'allargamento dell'UE, però, il secondo sondaggio è stato più ampio rispetto al primo. Il sondaggio del 2006, infatti, comprendeva i dieci Stati membri che hanno aderito nel 2004, nonché Bulgaria, Croazia, Romania e Turchia.

I risultati dei sondaggi sono piuttosto interessanti per molti aspetti. Nel 2001, il 53% degli intervistati ha affermato di saper parlare una lingua straniera accanto alla propria. Nel 2006, tale quota è salita al 56%. I più poliglotti sono i lussemburghesi, dato che il 99% di loro parla almeno un'altra lingua straniera, seguiti dagli slovacchi (97%) e dai lettoni (95%).

Nel 2006, il 28% degli intervistati ha affermato di parlare due lingue straniere, contro il 26 del 2001. Le seconde lingue più diffuse sono l'inglese, il francese e il tedesco, seguite dallo spagnolo e dal russo.

Complessivamente, i sondaggi hanno mostrato che gli Stati membri più piccoli, con più di una lingua ufficiale, vantano i livelli più alti di multilinguismo. Ciò vale anche per i paesi la cui lingua è poco diffusa o che hanno un certo "scambio linguistico" coi paesi vicini. Solo sei Stati membri hanno registrato una maggioranza di monolingui nel 2006: l'Irlanda (66% della popolazione parla solo la

Le difficoltà incontrate nella costruzione di un linguaggio giuridico europeo sono determinate dalla diversità dei sistemi giuridici nazionali, che si manifesta anche in rapporto ai microlinguaggi giuridici.

Le differenze del diritto apportano una grande ricchezza alla costruzione giuridica dell'Europa ma, allo stesso tempo, sono un fattore di distorsione che impedisce l'articolazione unitaria di una comunità costituzionale europea, se non fosse per l'esistenza di elementi di confluenza verso un modello congeniale alle caratteristiche sociali, politiche, geografiche e culturali dell'Unione Europea.

Esistono asimmetrie molto forti tra gli Stati membri dell'Unione Europea che si riflettono, in primo luogo, nei rapporti tra sistemi giuridici di *civil law* e di *common law* ma anche nel rapporto tra i modelli giuridici continentali. Vi sono infatti Stati monarchici e repubblicani, centralizzati e fortemente decentralizzati, con modelli parlamentari e presidenziali o semipresidenziali, con o senza giustizia costituzionale. A queste asimmetrie se ne aggiungono altre che incidono sull'articolazione geografica e sociale dei Paesi dell'Unione: Stati di grande estensione territoriale e Stati minuscoli, Stati continentali e insulari, Stati molto popolosi e Stati poco popolosi. Inoltre occorre considerare il problema dell'integrazione dei Paesi che provengono dall'antico sistema sovietico, poiché essi sono dotati di un patrimonio culturale e giuridico tipico, risultato dell'acquisizione di nuovi modelli costituzionali e legali, integrati da elementi caratterizzanti della propria cultura d'origine. Tali peculiarità sono rappresentative del pluralismo e della ricchezza culturale dell'Europa e possono contribuire sia ad arricchire il linguaggio giuridico europeo sia ad attuare istituzioni e principi che determinino possibili evoluzioni del sistema giuridico comunitario. Al tempo stesso queste differenze sono tante e tali da costituire un ostacolo al processo di armonizzazione della cultura giuridica europea.

Le differenze tra i sistemi sono ancora più evidenti laddove si considerino i microlinguaggi giuridici e, di conseguenza, l'alea di significanza della terminologia tecnica in uso in ogni Stato membro. Il lavoro del diritto comparato come "*quinto metodo di interpretazione giuridica*", coerentemente con il pensiero di Peter Häberle, risulta essenziale per la costruzione di ciò che lo stesso Autore indica come "*diritto costituzionale comune europeo*" e, in definitiva, per l'integrazione dei sistemi giuridici statali europei in un unico sistema

---

propria lingua materna), il Regno Unito (62%), l'Italia (59%), l'Ungheria (58%), il Portogallo (58%) e la Spagna (56%).
Solo una minoranza di europei considera poco importante lo studio delle lingue, per la precisione l'8% nel 2006, con una leggera differenza rispetto al 7% del 2001.
Il sondaggio, aggiornato al 19 agosto 2008, è consultabile sul sito della Commissione europea http://ec.europa.eu/education/languages/languages-of-europe/doc137_it.htm.

giuridico europeo. Le discrasie tra i sistemi giuridici richiedono un'interpretazione dei termini tecnici che si collochi prima nel contesto nazionale e solo successivamente in quello europeo. La costruzione di un linguaggio giuridico europeo unitario e omogeneo non può prescindere dalla valutazione dei linguaggi particolari nazionali. Tuttavia un linguaggio giuridico comune dovrà essere necessariamente multilingue, senza costituire un ostacolo per la traduzione e l'interpretazione delle norme.

Attraverso il linguaggio giuridico europeo si stanno articolando nuove tecniche ed istituzioni che arricchiscono il linguaggio giuridico degli ordinamenti nazionali. Allo stesso tempo, il linguaggio giuridico comune europeo rappresenta una tappa fondamentale verso la realizzazione del cosiddetto "linguaggio anticipatorio", quale giusta via verso la costruzione dell'Europa attraverso la lingua[328].

In un contesto di linguaggio giuridico (e non) plurale non è sufficiente ricercare la traduzione letterale di un termine ma è doveroso interrogarsi preliminarmente sulla possibilità di tradurre concetti giuridici facenti parte di un'esperienza diversa. I concetti giuridici, anche all'interno di ogni singolo ordinamento, sono il risultato di una stratificazione di significati diversi che si sono sviluppati nel tempo, dalla compenetrazione e dallo sviluppo di varie esperienze culturali. Una delle principali difficoltà della traduzione giuridica di termini specifici deriva dal fatto che, spesso, ci si trova di fronte ad una parola che non ha un diretto corrispondente in ogni lingua ma che, per la sua corretta comprensione, necessita di una locuzione definitoria che dia contezza del contenuto concettuale. Per evitare abusi o scorrettezze di linguaggio nella fase di trasposizione nazionale, il Legislatore comunitario utilizza in maniera preponderante dei termini volutamente a-tecnici, al fine di agevolare l'armonizzazione[329]. Lo sviluppo di una cd. linguistica giuridica, si basa proprio sull'approccio interattivo tra ricerca linguistica ed informazione giuridica, funzionale al superamento degli ostacoli alla formazione di un linguaggio giuridico europeo[330].

I problemi terminologici presenti nel diritto comunitario sono stati al centro dell'attenzione della Commissione europea già dal 2003 per quanto attiene il diritto privato ed in particolare il diritto dei contratti[331].

---

[328] Si veda F. BALAGUER CALLEJON *Derecho y Derechos en la Unión Europea* in J. CORCUERA ATIENZA (a cura di), *La protección de los Derechos Fundamentales en la Unión Europea*, Dykinson, 2002.

[329] In questi termini B. POZZO in *Le politiche linguistiche delle istituzioni comunitarie dopo l'allargamento*, Giuffrè, 2006.

[330] *Ibidem*.

[331] Si ricorda, a questo proposito, la Comunicazione della Commissione al Parlamento europeo e al Consiglio del 12 febbraio 2003 – COM(2003)68 definitivo. In tema di maggiore coerenza nel diritto contrattuale Europeo, un piano d'azione e la Comunicazione della Commissione al Parlamento Europeo

L'approccio al tema da parte della pan penalistica è recente ma particolarmente sentito, specie a seguito della caduta dell'organizzazione in pilastri dell'Unione Europea, con l'entrata in vigore del Trattato di Lisbona.

L'incremento della criminalità transnazionale ha reso necessario un approccio giuridico e linguistico comune e condiviso, anche a seguito dello sviluppo delle competenze comunitarie in materia penale e processuale.

Stante la complessità degli obiettivi comunitari e le differenze terminologiche e di significato, il raggiungimento di obiettivi comuni e la certezza del diritto possono e devono essere perseguiti superando le ambiguità concettuale. Si deve partire dall'assunto secondo cui il linguaggio giuridico si differenzia dal linguaggio cd. ordinario, costituendone un sottolinguaggio specializzato, utilizzato precipuamente dai giuristi che, a tal fine, hanno intrapreso studi e acquisito conoscenze specifiche. I concetti prodotti in una determinata realtà giuridica, intrisa del substrato culturale in cui si è sviluppata, non sempre hanno un corrispondente elaborato in un diverso sistema. Ogni linguaggio giuridico contiene propri concetti, strutture, relazioni concettuali e significati caratteristici. Per questi motivi, ogni traduzione in un linguaggio giuridico diverso da quello originario, inevitabilmente crea delle distorsioni[332].

Ma se il fine della stortura concettuale risiede nell'intento comunicativo e armonizzatore tra realtà giuridiche diverse che, per ragioni di giustizia, necessitano di colloquiare tra loro, allora è non solo giustificata ma anche incentivata. Da una valutazione complessiva dell'operazione, infatti, risulta preponderante l'interesse ad una ricerca di relazioni tra sistemi piuttosto che della salvaguardia della purezza di significato di termini e locuzioni. Indipendentemente dal metodo utilizzato, lo scopo di una traduzione giuridica è produrre parole e testi equivalenti, anche laddove non si possa dire di avere raggiunto un'identità. Come ha sostenuto icasticamente Monateri: "*Non si tratta solo di rivolgere la frase: bisogna rivolgere il pensiero*"[333].

Il plurilinguismo è figlio di un sistema ancora in vigore, seppure sempre più sbiadito, in cui sono i singoli Stati e non l'Unione europea a detenere la sovranità. I Paesi però, consci della necessità di un approccio transfrontaliero ad alcune problematiche comuni, socio-politiche, di sicurezza ed economiche, sono disposti a cedere parte dei propri poteri ad organi sovranazionali che vigilano ed agiscono secondo una prospettiva non settoriale ma globale.

---

e al Consiglio dell'11 ottobre 2004 – COM(2004)651 definitivo. In materia di diritto contrattuale europeo e revisione dell'*acquis*: prospettive per il futuro.

[332] Si veda *Ordinary language and legal language*, B. POZZO (a cura di), Giuffrè, 2005, pagg. 46-47.

[333] *Ibidem*, pag. 297

Questo aumenta, tra l'altro, l'esigenza di uno *standard* linguistico comune e comprensibile tra gli Stati, almeno nella materia giuridica e, per quanto qui consta, in ambito penale.

5.3 Le forme di controllo delle richieste di trasmissione di prove digitali e dei soggetti richiedenti: un intervento preventivo contro gli eccessi e gli abusi

Lo sprono all'incremento della cooperazione giudiziaria e di polizia e della circolazione dei dati e delle informazioni nell'ordinamento comunitario non deve costituire una giustificazione per gli abusi e gli eccessi di richieste infondate ed immotivate ovvero di richieste che provengono da soggetti non legittimati. E' necessario, pertanto, prevedere delle regole di controllo di queste procedure per prevenire eventuali distorsioni del sistema e, di conseguenza, predisporre i mezzi di repressione degli effetti negativi generati e la sanzione per i soggetti coinvolti.

Le prove penali, come già ricordato[334], hanno un carattere di dato personale, spesso particolarmente sensibile che, per ciò stesso, deve essere oggetto di trattamento, archiviazione e trasmissione secondo modalità controllate e solo a determinate condizioni.

La ricerca e il trasferimento della prova penale è una forma di cooperazione che si colloca entro la cd. assistenza giudiziaria minore e che, come noto, è transitata da un sistema principalmente rogatoriale[335] ad una forma di cooperazione fra autorità giudiziarie e di polizia degli Stati membri secondo una logica di amministrazione transnazionale della giustizia.

In un processo di bilanciamento tra opposte esigenze, rispettando i diritti e le libertà della persona a fronte delle esigenze di rapida amministrazione della giustizia penale, il rifiuto della cooperazione è legittimo se configgente con la garanzia dei diritti. L'accettazione della richiesta di cooperazione è il risultato della creazione di un equilibrio fra due imperativi: quello collettivo alla sicurezza e quello individuale alla libertà.

Le convenzioni di Bruxelles e di Budapest, per dare esecuzione più rapidamente alle richieste, consentono – in casi particolari – l'uso di fax e tecnologie telematiche, l'inoltro tramite Interpol o qualsiasi organo competente, secondo le disposizioni vigenti[336]. Le ipotesi di rifiuto sono limitate all'assenza di requisiti previsti dalla disciplina vigente o perché é intervenuto un soggetto

[334] Si veda il capitolo Secondo, paragrafo 1.
[335] L'istituto della rogatoria ha mostrato i propri punti deboli, di insufficienza, specie in materia di trasmissione della prova formata per mezzo delle nuove tecnologie, essendo caratterizzata da un oggetto particolarmente volatile. Così N. PARISI, *op. cit.* pag. 446.
[336] Art. 6.4 Convenzione di Bruxelles.

non legittimato o perché non sussiste un giusto motivo fondante. Il rifiuto è inoltre possibile se la richiesta si riferisce a un reato politico o a un reato a questo connesso; in caso di pregiudizio della sovranità, della sicurezza, dell'ordine pubblico o di altri interessi essenziali dello Stato richiedente; nelle ipotesi di rischio di non disponibilità in futuro dei dati conservati, di danno alla loro confidenzialità ovvero di altro pregiudizio [337].

La decisione quadro MERP precisa che le informazioni destinate ad essere usate come prova di un reato possono e devono essere trasferite soltanto a seguito di un'autorizzazione preventiva di un'autorità giudiziaria dello Stato membro che detiene e controlla le informazioni stesse. Analogamente, gli articoli 2.1, 8 e 12.1 del Trattato di Prum.

Tutte le norme europee che disciplinano le procedure di cooperazione[338] mirano al trasferimento rapido del materiale probatorio, conformemente alle disposizioni delle Convenzioni di Bruxelles e Budapest. Un esempio chiaro è costituito dalla decisione quadro MER che, analogamente a quanto previsto nella Decisione quadro 2003/577/GAI, vincola l'autorità di esecuzione ad agire in tempi rapidi e delinea una serie di attività utili a rendere le operazioni più fluide: l'obbligo di inoltrare la richiesta mediante un formulario allegato alla decisione, compilato nella lingua del Paese d'esecuzione; l'indicazione dei termini di scadenza per l'esecuzione della domanda; la previsione di ridotti motivi di rifiuto o di ritardo ad adempiere [339].

Dal punto di vista soggettivo, non ogni persona fisica o giuridica indistinta ha facoltà di avanzare la richiesta, ma soltanto le autorità competenti per ogni Stato.

La Convenzione di Budapest sul *cybercrime* legittima le autorità competenti, in qualità di parti richiedenti, a domandare l'archiviazione di una prova elettronica per i fini delle indagini e del processo penale (art. 25). Le informazioni e i materiali richiesti possono essere fatti circolare solo a determinate condizioni: che venga mantenuto un grado di confidenzialità dei dati e che questi siano utilizzati solo nell'ambito del procedimento per cui sono stati richiesti (art. 28). L'art. 35 della Convenzione prevede che ogni Stato ratificatore si doti di un punto di contatto 24/7, cioè attivo sette giorni su sette e ventiquattr'ore su ventiquattro, per fare fronte alle esigenze di rapida trasmissione delle informazioni utili ai fini penali.

La necessità di istituire dei punti di contatto 24/7 trova espressione, in ambito comunitario, nella Decisione quadro 2005/222/GAI del Consiglio, relativa agli attacchi contro sistemi di informazione. In particolare, l'art. 11 dispone che gli Stati informino il Segretariato Generale del Consiglio e della

[337] Convenzione europea del 1959 art. 29.5-6.
[338] Vedi capitolo Primo.
[339] Si vedano, in particolare, gli artt. 11.1, 15.5 e 15 della Decisione quadro MER.

Commissione in merito al punto di contatto operativo per far fronte alle esigenze dello scambio di informazioni sui reati connessi ad attacchi in danno di sistemi di informazione. Il Segretariato ha poi l'onere di rendere edotti anche tutti gli altri Stati membri.

Nella Comunicazione della Commissione al Parlamento europeo, al Consiglio e al Comitato delle Regioni, verso una politica di lotta alla cibercriminalità[340], è sottolineata l'importanza del rafforzamento della cooperazione operativa transnazionale che non si basi soltanto sulla collaborazione e lo scambio delle informazioni tra le autorità dei singoli Stati membri, ma che coinvolga e responsabilizzi anche Europol, Eurojust ed altre strutture sovranazionali (punto 3.1). Ulteriormente, la Commissione insiste sulle esigenze di formazione continua delle autorità giudiziarie e di contrasto sui vari aspetti della cibercriminalità e sullo sviluppo tecnologico. La Commissione, con la menzionata Comunicazione, si è impegnata direttamente a cooperare strettamente con gli Stati membri, con Europol, con Eurojust, con l'Accademia Europea di Polizia e la Rete Europea di Formazione Giudiziaria per collegare a livello comunitario tutti i programmi di formazione pertinenti (punto 3.1).

Un'altra successiva Comunicazione della Commissione al Consiglio e al Parlamento europeo del 20 luglio 2010 tratta della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia. Lo scopo espresso è quello di fissare i principi cardine della concezione e della valutazione degli strumenti di gestione delle informazioni in ambito UE[341]. La Commissione ritiene – e in ciò si concorda – che da un lato un sistema unico e globale a livello comunitario per la gestione delle informazioni consentirebbe una massima condivisione ma, d'altro lato, costituirebbe una forte limitazione del diritto della persona alla vita privata e alla protezione dei dati, mentre una gestione compartimentata contribuisce al rispetto della *privacy* di ogni singolo cittadino.

L'Unione europea presenta una pluralità di strumenti che disciplinano la raccolta, la conservazione o lo scambio di dati personali nel campo dell'immigrazione, nel contrasto al terrorismo, nel funzionamento dello spazio Schengen e di unione doganale, nella prevenzione e repressione di gravi forme di criminalità transnazionale. Fra questi si può menzionare il Sistema di Informazione Schengen (SIS I) ed il Sistema di Informazione Schengen di seconda generazione (SIS II), un sistema centralizzato ai cui dati possono accedere, nell'ambito delle rispettive competenze legali, le autorità di polizia, le autorità di controllo alla frontiera, le autorità doganali e le autorità giudiziarie nei procedimenti penali ed anche Europol ed Eurojust, limitatamente ad alcune

[340] COM(2007) 267 definitivo del 22 maggio 2007.
[341] Il riferimento è alla Comunicazione COM(2010) 385 definitivo ed in particolare, quanto alle finalità espresse, all'introduzione al testo.

categorie di dati. Le interrogazioni generano un "*hit*" (segnalazione positiva) e solo dopo questa indicazione positiva, le autorità di contrasto possono chiedere informazioni supplementari sulla persona o sull'oggetto cui si riferisce la segnalazione.

Quanto ad EURODAC, sistema centralizzato ed informatizzato di identificazione delle impronte digitali, ogni Stato membro comunica le autorità che hanno diritto di accesso alla banca dati e può inserire dati pertinenti tramite i punti d'accesso nazionali.

Il sistema d'informazione visti (VIS) ha un'organizzazione di tipo centralizzato, costituita da una sezione nazionale presso ciascuno Stato partecipante e da un'unità di supporto tecnico in Francia. Possono accedere alle informazioni ivi contenute solo le autorità per il visto, per l'asilo, per l'immigrazione e le autorità di controllo alla frontiera; la polizia ed Europol possono consultare le informazioni ai fini della prevenzione e della lotta al terrorismo e ad altre forme gravi di criminalità. I dati memorizzati devono essere trattati in conformità alle disposizioni che disciplinano il sistema[342] le quali, a loro volta, si attengono alle regole della Direttiva 95/46/CE e del Regolamento CE 45/2001, della Decisione quadro 2008/977/GAI del Consiglio, della Convenzione del Consiglio d'Europa n. 108 e suo Protocollo addizionale n. 181 del 1981.

Su iniziativa spagnola, nel 2004 il Consiglio europeo ha adottato una direttiva in materia di trasmissione anticipata dei dati relativi alle persone trasportate[343], in base alla quale i vettori aerei sono tenuti a comunicare alle autorità di controllo alla frontiera il nome, la data di nascita, la cittadinanza, il punto di imbarco e il valico di frontiera di ingresso dei passeggeri che si recano in UE da Paesi Terzi. Questi dati possono essere usati solo dalle autorità pubbliche ai fini del controllo alla frontiera e della lotta all'immigrazione illegale. La Convenzione di Napoli II, relativa alla mutua assistenza e alla cooperazione tra amministrazioni doganali, mira a permettere alle amministrazioni doganali degli Stati di prevenire ed accertare le violazioni delle disposizioni doganali comunitarie e nazionali[344]. Ai sensi di questo atto normativo, gli uffici di coordinamento centrali, nell'ambito delle indagini penali concernenti violazioni di disposizioni doganali nazionali e comunitarie, chiedono per iscritto assistenza ai loro omologhi negli altri Stati membri. Le unità possono trasmettere i dati alle autorità nazionali responsabili dell'azione penale, agli organi giurisdizionali nazionali e, previo consenso della Stato membro che li ha forniti, anche ad altre autorità. Ad integrazione della

[342] regolamento CE 767/2008 e decisione 2008/633/GAI del Consiglio.
[343] API – *Advance Passenger Information.*
[344] La Convenzione di Napoli II è stabilita in base all'articolo K3 del Trattato dell'Unione europea relativa alla mutua assistenza e alla cooperazione tra amministrazioni doganali.

Convenzione Napoli II, la Convenzione SID utilizza il sistema d'informazione doganale per facilitare la prevenzione, la ricerca e il perseguimento di gravi infrazioni alle leggi nazionali, mediante la rapida diffusione di informazioni e la cooperazione tra le amministrazioni doganali degli Stati membri. Il SID è un sistema centralizzato gestito dalla Commissione e accessibile tramite terminali situati in ogni Stato e presso la Commissione, Europol e Eurojust. Tali informazioni possono essere utilizzate solo per fini di osservazione e rendiconto e possono essere consultate soltanto dagli analisti designati dagli Stati membri.

Esiste inoltre un archivio d'identificazione dei fascicoli a fini doganali (FIDE) che consente alle autorità nazionali preposte alle indagini doganali, quando istituiscono un fascicolo, di individuare le autorità che possono aver indagato sulle persone fisiche o giuridiche in questione.

Nel 2006 il Consiglio europeo ha adottato l'iniziativa svedese[345] diretta ad ottimizzare la condivisione tra Stati membri di informazioni e *intelligence* criminale che possono essere necessarie ai fini di indagini penali o di operazioni di *intelligence* criminale. L'iniziativa funziona in modo decentrato e consente alla polizia, alle autorità doganali e alle altre autorità investigative di condividere informazioni, specie per i fini della prevenzione e repressione del terrorismo e di tutte le forme più gravi di criminalità transnazionale. L'uso delle informazioni così acquisite è assoggettato alle condizioni d'uso dello Stato che le trasmette. È predisposto un formulario *ad hoc* per richiedere i contenuti.

Con la Decisione quadro 2009/315/GAI del Consiglio, relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario e la decisione 2009/316/GAI che istituisce ECRIS[346] si è mosso un altro importante passo verso la realizzazione piena della cooperazione informativa in ambito UE. In base a queste disposizioni, lo Stato membro di condanna deve trasmettere le informazioni sulle nuove condanne ad ogni Stato in cui il soggetto risulta essere cittadino. ECRIS è un sistema d'informazione decentrato che interconnette le banche dati dei casellari giudiziari, ove i dati sono ordinati e cifrati. Dall'attuazione delle menzionate decisioni quadro ogni Stato dovrà fornire le informazioni estratte dal casellario giudiziario e inviarle alle autorità giudiziarie o amministrative competenti. La Germania, durante la presidenza del Consiglio del 2007, ha posto le base per una discussione sull'eventuale introduzione di un indice europeo dei casellari giudiziari (EPRIS)[347], la cui

[345] Decisione quadro 2006/960/GAI.
[346] Sistema europeo di informazione sui casellari giudiziari che entrerà in vigore nel 2012 ma che già è oggetto di un progetto pilota che coinvolge alcuni Stati membri.
[347] si veda sul punto il documento del Consiglio n. 15526/1/09 del 2 dicembre 2009.

realizzazione fa parte dei progetti del Piano d'Azione per l'attuazione del Programma di Stoccolma (2010-2014).

Su iniziativa finlandese, nel 2000 il Consiglio europeo ha adottato uno strumento che organizza lo scambio di informazioni tra le unità di informazioni finanziarie (UIF) contro il riciclaggio di denaro e il finanziamento del terrorismo. Di norma le UIF sono istituite presso le autorità di contrasto, le autorità giudiziarie o gli organi amministrativi tenuti a riferire alle autorità finanziarie e hanno l'obbligo di scambiare con i loro omologhi nell'UE i dati finanziari o ai fini di contrasto. I dati trasmessi per l'analisi o le indagini su casi di riciclaggio di denaro o finanziamento del terrorismo possono essere usate anche per altre indagini o azioni penali, salvo che lo Stato membro che le ha fornite ne vieti tale uso.

Nel 2002 un gruppo di Stati ha istituito FIU.net, un'applicazione di rete decentrata che permette lo scambio di dati tra le UIF. Anche gli ARO, cioè gli uffici per il recupero dei beni, seppure privi del supporto di una piattaforma *online* funzionano secondo lo stesso sistema.

Quanto precede invita ad alcune osservazioni preliminari sulla gestione delle richieste, la legittimazione dei soggetti e le procedure di controllo preventivo delle interrogazioni. Tutte le misure disciplinano lo scambio decentrato e transfrontaliero, con limitazione delle finalità per cui possono essere accolte le richieste e inoltrate le informazioni. Più strumenti possono raccogliere gli stessi dati personali ma possono usarli solo per scopi limitati nel proprio stretto ambito. I diritti di accesso agli strumenti per la prevenzione e lotta al terrorismo e alle altre forme di criminalità grave riguardano solo il ristretto numero delle autorità di contrasto. L'accesso agli strumenti che rispondono alla logica di Schengen sono di norma accordati alle autorità competenti per l'immigrazione e, a certe condizioni, alla polizia e alle autorità di frontiera e doganali. Si noti che già dal giugno 2004, cioè qualche mese prima che il Consiglio europeo stilasse il Programma dell'Aia[348], il Regno di Svezia intrprendeva un'iniziativa volta a garantire lo scambio rapido delle informazioni e dell'*intelligence*, per le finalità di prevenzione dei reati e per le indagini in materia criminale, privilegiando le autorità di polizia ma senza omettere quelle giudiziarie.

La Commissione, a conclusione della Comunicazione COM(2010) 384 definitivo, ha fornito un catalogo di principi sostanziali e di regole d'intervento che si condividono appieno. Infatti, l'ingerenza di un'autorità pubblica nel diritto di ciascuno al rispetto della vita privata può essere essenziale al soddisfacimento dell'interesse alla sicurezza pubblica e alla prevenzione dei reati. Tra le condizioni legittimanti l'interferenza nella sfera

[348] Il Programma dell'Aia si distingue per il suo carattere di novità, incentivando l'accesso reciproco e l'interoperabilità tra le basi di dati nazionali che, però, non ha trovato realizzazione.

privata, la Commissione (correttamente) inserisce la necessità a che le ragioni avanzate dall'autorità pubblica siano pertinenti, sufficienti e rispondano ad un'esigenza sociale impellente e proporzionata all'obiettivo[349].

5.4 *La formazione del personale coinvolto nelle procedure di cooperazione e di circolazione della prova digitale: una specializzazione necessaria per l'incremento della responsabilizzazione dei singoli*

Il Sostituto Procuratore della Repubblica presso il Tribunale di Trieste, dott. Frezza, in occasione di un intervento ad un incontro di studi, ha sintetizzato con molta chiarezza alcuni tra i principali ostacoli e problemi della cooperazione giudiziaria e di polizia. Segnatamente, in alcuni casi non c'è alcuna possibilità da parte delle autorità investigative di ottenere dall'estero "*qualcosa di diverso di quello che ci viene fornito*", come per il caso in cui sia stato effettuato un accertamento tecnico non ripetibile privo delle garanzie del diritto alla difesa che, certo, non potrà essere utilizzato in un processo italiano (e non solo italiano) ma che, nonostante ciò, potrà servire ad orientare la prosecuzione delle indagini[350].

Sono in particolare le indagini dinamiche, ovvero quelle indagini che consistono nel seguire un fenomeno criminale nel momento in cui si sta compiendo, a necessitare una cooperazione ed una circolazione di informazioni, dati e prove "*di pari dinamicità, vale a dire non impastoiata in formalismi e nel rispetto delle regole che, in quella fase, non hanno alcuna rilevanza. Se poi questa si chiama 'scambio spontaneo di informazioni, o se la riteniamo tipica delle forze di polizia ed estranea all'attività propriamente giurisdizionale, poco importa; quello che importa è che la cooperazione ci sia, ed è impensabile che il PM non sia coinvolto. (…) In sostanza, quello che voglio dire è che l'indagine non è il processo e non deve seguire tutte le regole del processo (…). A mio avviso, compito del PM è quello di assicurare l'effettiva efficacia dell'azione repressiva e, quindi, di puntare ad un risultato non esclusivamente cartaceo*".

Partendo dalle riflessioni proposte dal dott. Frezza, si osserva che, oltre alla volontà di cooperare tra gli Stati e le autorità giudiziarie e di polizia, è necessario il coinvolgimento di personale che sia in grado di gestire

[349] Tali indicazioni provengono dalla decisione della Corte europea dei diritti dell'uomo nella sentenza del noto caso *Marper v. United Kingdom* del 4 dicembre 2008.

[350] Federico FREZZA 6/8 giugno 2005 intervenuto nell'incontro di studio sul tema "*Criminalità organizzata transnazionale: strumenti di contrasto e forme di cooperazione giudiziaria*" riportato in nota 15 pag. 172 di F. CAJANI – G. COSTABILE – G. MAZZARACO *Phishing e furto d'identità digitale*, Giuffrè 2008.

efficacemente le procedure. Infatti, lo sviluppo della cooperazione necessita certamente dello sviluppo tecnologico[351] ma anche di persone formate *ad hoc*.

Come ha avuto modo di sottolineare in più occasioni il dott. Cajani Francesco, Sostituto Procuratore della Repubblica presso il Tribunale di Milano, sezione reati informatici[352], se l'infrastruttura tecnologica può essere un valido supporto alle attività, non bisogna mai dimenticare lo *human factor* cioè il fattore umano, l'intelligenza umana, che è un elemento determinante in ogni circostanza.

Questo concetto trova spazio anche nel testo della Convenzione di Budapest, in particolare nell'art. 35 laddove, nell'intento di sviluppo delle procedure di cooperazione per i reati informatici si richiede la predisposizione di accorgimenti tecnici funzionali allo scopo dell'attività, ma anche il *training* di personale idoneo per la gestione di queste procedure, in grado di comprendere la richiesta avanzata, di fare un controllo preventivo di legittimità e di attivarsi, quando necessario, per il coordinamento delle autorità coinvolte.

Il problema rappresentato dalla limitatezza delle conoscenze è espresso, sebbene in modo marginale e limitato ad una singola vulnerabilità, anche nella Decisione quadro del Consiglio relativa agli attacchi contro i sistemi di informazione. Nel punto 1.3 della citata Decisione, dedicato alla necessità di informazioni accurate e statistiche, si fa riferimento ad una indagine effettuata negli Stati Uniti d'America nel 1999[353] da cui emerge che, a causa della conoscenza ed esperienza limitata degli amministratori e degli utenti di sistema, molte intrusioni non vengono individuate. Ancora in questa Decisione COM(2002) 173 definitivo, al punto 1.4, il Consiglio indica la formazione come uno dei modi più efficaci per affrontare i problemi di criminalità informatica e proteggere i sistemi d'informazione, le telecomunicazioni ed i dati raccolti.

Il Programma comunitario denominato Tecnologie della Società dell'Informazione (TSI)[354] fornisce un quadro per lo sviluppo delle capacità di fronte alle sfide della nuova tecnologia.

La formazione del personale impegnato nelle attività di cooperazione non deve essere limitata alla mera conoscenza del funzionamento delle infrastrutture.

---

[351] Lo sviluppo tecnologico trae la propria linfa anche da una collaborazione più stretta tra pubblico e provato, tra le autorità e le industrie. Sul punto si rinvia al paragrafo 6.1.

[352] Il riferimento, in particolare, è all'intervento compiuto dal dott. Francesco Cajani in occasione di un convegno svoltosi a Barcellona il 26-27 maggio 2011 dal titolo "*The use of new technologies in criminal proceedings*".

[353] Il *Computer Security Institute* ed il *Federal Bureau of Investigation* producono un'indagine annuale sulla criminalità e sulla sicurezza informatica che viene pubblicato agli inizi di ogni anno. Per maggiori informazioni è possibile consultare il sito www.gocsi.com.

[354] Il gruppo TSI è gestito dalla Commissione europea. Per maggiori informazioni si invita alla consultazione del sito internet ww.cordis.lu/ist.

La Commissione europea il 19 marzo 2010 ha presentato al Parlamento europeo e al Consiglio una proposta per l'istituzione di un'agenzia per la gestione operativa dei sistemi di tecnologia dell'informazione su larga scala nel settore della libertà, della sicurezza e della giustizia dello spazio europeo[355], ma anche questo progetto non prescinde dalla necessaria preparazione del personale addetto alla cooperazione. La conoscenza richiesta è molto vasta ed abbraccia non solo l'ambito informatico-telematico, ma anche quello giuridico, delle garanzie da salvaguardare e delle norme in materia di cooperazione e relative procedure attuabili. Le diposizioni volte al migliore funzionamento degli strumenti utilizzati per la cooperazione sono funzionali ad assicurare un flusso di informazioni efficace ed ininterrotto. Risulta altresì necessario che il personale controlli i soggetti richiedenti che vogliano accedere a dati, informazioni e prove e, contemporaneamente, valuti se sussistono i requisiti oggettivi e di contenuto delle interrogazioni promosse. L'indagine sulla sussistenza delle esigenze sociali, sulla proporzionalità degli obiettivi e sulla pertinenza delle giustificazioni addotte non può che essere il prodotto del lavoro di personale scelto e formato a questa attività, conoscitore della materia, dei diritti ed interessi fondanti.

[355] Il riferimento è al testo COM(2010) 93.

CAPITOLO SECONDO

SEZIONE II

La catalogazione dei dati e degli archivi

SOMMARIO: 6. Archivi, banche dati e indicizzazione: problematiche introduttive - 7. Gli archivi e le banche dati dell'Unione europea: le banche dati di Europol, Eurojust e Olaf - 7.1 Le altre principali banche dati UE - 8. Il sistema delle banche dati nazionali: limiti e benefici

6. Archivi, banche dati e indicizzazione: problematiche introduttive

L'attività raccolta di dati e di informazioni in banche dati, siano essi nazionali o comunitari, interessa una pluralità di esigenze contrapposte e configgenti che devono essere bilanciati in modo coerente.

Anzitutto, l'istituzione di archivi, dal punto di vista meramente pratico, richiede l'utilizzo di sofisticate infrastrutture.

Di contro, sono molti i benefici che si possono trarre dal loro uso, sia in fase di investigazione, sia in sede processuale. Ad esempio, l'archivio del DNA permette un'immediata comparazione fra il DNA rilevato e repertato sulla scena del crimine e i risultati già raccolti e conservati nelle banche dati della polizia[356].

L'utilizzo di questi archivi, però, si scontra con le esigenze di garanzia dei diritti fondamentali, con particolare riferimento alla tutela della *privacy*. Come noto, il diritto alla riservatezza non consiste più soltanto nel diritto ad essere lasciati soli[357], ma anche nel diritto al rispetto della vita privata di ciascun individuo.

[356] In questi termini, limitatamente alla banca dati del Dna, si veda C. FANUELE, *op.cit*., pagg. 62-65.

[357] La nozione più risalente e tradizionale di privacy, infatti, faceva coincidere questo diritto con l'unica prerogativa dell'essere lasciati soli. Si considerava, quindi, come una libertà negativa e non anche positiva, avuto riguardo alle categorie del diritto costituzionale.

I moderni strumenti tecnici, quali i *databases*, hanno favorito l'innovazione del concetto di "*sfera personale*", che si deve intendere anche come "*limite negativo interno*" al trattamento informatizzato dei dati personali[358].

In effetti, le informazioni contenute in archivi e banche dati possono astrattamente restare archiviate per un tempo illimitato[359] e possono essere assoggettate, di conseguenza, a molteplici operazioni di trattamento, specie mediante l'interconnessione con altri *databases*. Proprio quest'ultima operazione possibile, in particolare, rischia di compromettere il diritto al riserbo degli interessati[360].

Gli strumenti di raccolta di dati, inoltre, sono spesso oggetto di furti o danneggiamenti dei supporti e dei contenuti, da cui deriva un *vulnus* al diritto alla riservatezza, specie allorché le informazioni sottratte o disperse o corrotte sono dotate di un carattere di particolare sensibilità[361].

La consapevolezza sociale del valore della *privacy* si riverbera anche sulla gestione e sul funzionamento di archivi e banche dati, richiedendo che, apprezzando lo sviluppo delle nuove tecnologie e dovendo perciò bilanciarne l'uso nel rispetto di altri interessi[362], non si generi un meccanismo perverso di limitazione immotivata del diritto alla riservatezza.

Sul piano sociologico si è verificata una generale riduzione delle aspettative di garanzia della *privacy* a seguito dello sviluppo delle scienze tecnologiche e dell'accrescimento delle esigenze di sicurezza e giustizia. Nonostante ciò, gli individui esigono la protezione della facoltà di autodeterminazione informativa dei propri dati personali, cioè un potere di controllo sui dati medesimi[363].

Un primo passo importante verso un equilibrato contemperamento tra interessi contrapposti può validamente consistere nella conoscibilità delle

---

[358] L'espressione si deve a V. TORRE *La gestione del rischio nella disciplina del trattamento dei dati personali* in AA.VV. *Il diritto penale dell'informatica nell'epoca di internet,* a cura di L. PICOTTI, Cedam, 2004, pag. 240.

[359] L'archiviazione di dati per un tempo anche illimitato è resa possibile in ragione delle innovazioni scientifiche e delle sofisticate infrastrutture informatiche a disposizione.

[360] Per un approfondimento sul punto si rinvia a L. D'ANGELO *La conservazione dei dati di traffico telefonico e telematico tra esigenze investigative e tutela della privacy* in AA.VV. Le nuove norme di contrasto al terrorismo, a cura di A.A. DALIA, Giuffré, 2006; G. TADDEI ELMI *Informatica e diritto: un binomio irreversibile* in AA.VV. *Il codice dei dati personali. Temi e problemi*, a cura di G. TADDEI ELMI, Giuffrè, 2006.

[361] Si pensi, in particolare, ai dati genetici il cui furto determina una lesione che non permette soluzioni. Il profilo genetico, infatti, ha una forte capacità di descrivere, in maniera indiretta, la storia biologica di tutti gli appartenenti al medesimo ceppo familiare e di mettere in relazione un soggetto con altre persone legate da vincolo di ascendenza o discendenza.

[362] Per quanto qui rileva, l'interesse contrapposto è quello del buon andamento e della prosecuzione delle indagini e del procedimento cioè il fine della giustizia, da intendere in senso ampio.

[363] Sulla *privacy* come pretesa al controllo dei propri dati personali, nella dottrina italiana si rinvia a F. CAPRIOLI *Colloqui riservati e prova penale*, Giappichelli, 2000.

categorie di informazioni che le pubbliche autorità detengono e del modo in cui sono trattate ed utilizzate.

Lo sviluppo di sistemi informatizzati contenenti dati sensibili e non, rappresenta, per i più garantisti, una minaccia concreta ed attuale per la riservatezza[364] che richiede una regolamentazione puntuale e rigorosa sull'uso di tali archivi.

In precedenza i mezzi tecnologici e i *databases* erano considerati strumenti efficaci di controllo impersonale e mediato di dati, mentre oggi sono valutati con sospetto proprio per il fatto di essere dei contenitori troppo aperti e liberi di informazioni personali.

Sull'opposto versante si pongono i sostenitori della sicurezza sociale, i quali promuovono l'attivazione e il funzionamento efficace di archivi e banche dati, riponendo la fiducia nelle tecniche di sorveglianze, come elementi imprescindibili del vivere moderno e del fenomeno di razionalizzazione e burocratizzazione sociale[365].

La risoluzione coerente del contrasto tra diritto e scienza può scongiurare la creazione di una "*tirannia tecnologica*", contribuendo all'adeguamento della disciplina vigente per il fine di un uso corretto dei nuovi strumenti tecnici.

Ricerca, specializzazione degli operatori, discipline specifiche, regole chiare: tutto può contribuire a che la scienza e la sua applicazione agli archivi e alle banche dati costituisca un valido supporto per la prevenzione e la repressione dei reati, specie di natura transnazionale e non rappresenti, al contrario, una minaccia alla garanzia dei diritti fondamentali.

La sicurezza pubblica, la difesa dell'ordine, e i fini di giustizia sono prerogative irrinunciabile dell'Unione europea, come ribadito nel Trattato di Lisbona ma anche nel Programma di Stoccolma e nel Piano d'Azione 2010-2013, perché lo scopo primario è quello della realizzazione di uno spazio comunitario effettivo di libertà, sicurezza e giustizia.

L'Unione europea è comunque particolarmente attenta alla protezione dei dati, anche e specificamente nell'ambito della cooperazione di polizia e giudiziaria in materia penale. In particolare, la decisione quadro 2008/977/GAI, pur essendo applicabile per i soli scambi transfrontalieri di informazioni e non per il loro trattamento negli Stati membri, persegue un livello minimo di armonizzazione delle norme di protezione dei dati. Questa decisione, tuttavia, non sostituisce le norme settoriali adottate a livello

---

[364] Così la dottrina tedesca maggioritaria e, in particolare, si rinvia a R. PITSCHAS *Informationelle Selbstbestimmung zwischen digitaler Okonomie und Internet*, DuD, 2000, 1998, pag. 139; W. SCHULZ *Verfassungrechtlicher "Datenschutzauftrag" in der Informationsgesellschaft, Die Verwaltung*, 1999, pag. 137.

[365] In proposito si veda R. FOX *Someone to watch over us: back to the panopticon?* in *Criminal Justice*, 2001, pag. 261 e K. BALL – F. WEBSTER *The Intensification of Surveillance*, Pluto Press, 2003, pag. 11.

comunitario, quali quelle che si applicano a particolari sistemi d'informazione, ciascuna delle quali contiene una disciplina specifica sulla garanzia delle informazioni archiviate[366].

Per assicurare il controllo sulla protezione dei dati sono state istituite autorità comuni di protezione che agiscono in base alla disciplina dei singoli strumenti per cui operano. Inoltre, ai sensi del regolamento (CE) n. 45/2001, il Garante europeo della protezione dei dati dispone di poteri di controllo generali sulle istituzioni, organi, organismi e agenzie dell'Unione europea [367].

La Raccomandazione R (87) 15 del Consiglio d'Europa, pur non essendo uno strumento giuridicamente vincolante, definisce i principi in materia di protezione dei dati nelle attività di cooperazione di polizia e giudiziaria tra tutti gli Stati Membri.

Come rilevato dalla Commissione[368], se l'obiettivo dell'Unione europea è quello di istituire un sistema coerente e globale che operi nello spazio comunitario, tra gli Stati membri ed anche nei rapporti con i Paesi Terzi, è doveroso definire delle regole di organizzazione e di gestione degli archivi, secondo uno *standard* comune ed accettabile di protezione dei dati, specie nel settore della cooperazione giudiziaria e di polizia. Pertanto, la Commissione europea sta valutando l'opportunità di allineare le norme settoriali per creare un quadro omogeneo di garanzie.

L'Unione europea, nel progetto della Commissione, deve costituire un punto di riferimento e una forza trainante per lo sviluppo e la promozione degli *standard* di protezione dei dati, da applicare anche ai singoli *databases* comunitari e nazionali, mediante la formulazione di norme giuridiche e la previsione di regole tecniche uniformi.

Le difficoltà di ravvicinamento e omogeneizzazione tra gli strumenti comunitari e quelli degli Stati membri si sono palesate più chiaramente dal 2004, a seguito dell'allargamento dell'Unione europea ai Paesi dell'Est, poiché questi si caratterizzano per tradizioni sociali, politiche, culturali e giuridiche spesso molto diverse da quelle degli altri Paesi.

Nello spazio Schengen, la corretta gestione delle informazioni e il collegamento tra le varie piattaforme costituiscono degli strumenti importanti (spesso decisivi) contro le forme gravi di criminalità [369].

---

[366] Sul punto si pensi alla disciplina sul funzionamento di Europol, di Eurojust, al Sistema Informativo Schengen (SIS) e al Sistema Informativo Doganale (SID).

[367] La ricostruzione dello stato della disciplina in materia di protezione dei dati nell'Unione europea si trova nel testo della Comunicazione della Commissione al Parlamento europeo , al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni del 4 novembre 2010 – COM(2010) 609 definitivo.

[368] Il riferimento è alla Comunicazione COM(2010) 609 definitivo.

[369] Questo concetto è definito nella Comunicazione della Commissione al Parlamento europeo e al Consiglio del 20 luglio 2010 dal titolo "*Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia*" – COM(2010) 385 definitivo.

In questo contesto di riferimento, un sistema di informazione unico e globale a livello UE, caratterizzato dalla molteplicità dei fini, consentirebbe certamente la massima condivisione delle informazioni, ma limiterebbe irrimediabilmente il diritto della persona alla vita privata e alla protezione dei dati, oltre a generare delle obiettive complessità in termini di sviluppo e funzionamento. Al contrario, una buona amministrazione compartimentata contribuisce al rispetto della *privacy*[370].

Gli archivi nazionali e comunitarie si differenziano per gli scopi perseguiti nel sistema di raccolta, conservazione e scambio di dati; presentano una struttura centralizzata o decentrata; interessano categorie differenti di dati personali; sono aperti all'accesso di autorità diverse; sono caratterizzati da *standard* differenti di protezione dei dati; hanno norme proprie di conservazione delle informazioni; sono applicati in modo disomogeneo tra gli Stati; sono previsti meccanismi diversi di revisione delle informazioni raccolte[371].

Alcuni *databases* sono organizzati secondo una funzione di indice. L'indicizzazione dei contenuti permette un vaglio preliminare della richiesta e della ricerca di informazioni avanzate da un'autorità legittimata, limitando così l'accesso alle informazioni complete solo dopo un vaglio preliminare di hit/o hit, cioè di esistenza o assenza dei dati richiesti.

La scelta della tecnica di indicizzazione, però, presenta particolari insidie e difficoltà. Una catalogazione poco chiara e non sistematica a volte può rendere impossibile o ambigua l'individuazione dell'informazione; in altri casi può, invece, svelare troppo del contenuto, violando così la riservatezza del dato.

Da queste considerazioni preliminari ed introduttive si comprende la problematicità del funzionamento e delle geometrie organizzative degli archivi e delle banche dati. Questa complessità cela un'esigenza di sviluppo e di attuazione di nuove iniziative per l'analisi degli strumenti esistenti, nell'ottica di un corretto bilanciamento tra opposte esigenze e al fine di armonizzare a livello UE le disposizioni che regolamentano i sistemi di informazione, tenuto conto delle diverse tradizioni giuridiche degli Stati membri.

La realizzazione piena di uno "*spazio giudiziario europeo*" in materia penale comporta, infatti, il superamento delle politiche nazionali di protezionismo giuridico e giudiziario e richiede l'attenzione verso diversi ambiti di applicazione, compreso quello dei sistemi d'informazione.

[370] *Ibidem*.
[371] *Ibidem*.

7. *Gli archivi e le banche dati dell'Unione europea: le banche dati di Europol, Eurojust e Olaf*

L'Unione europea si caratterizza per la massiccia presenza di sistemi informativi che delineano, quindi, un complesso sistema nel panorama della gestione delle informazioni[372].

Nel *mare magnum* delle banche dati, si distinguono le disposizioni settoriali che regolano il funzionamento di Eurojust, Europol e Olaf e dei rispettivi sistemi di informazione[373].

Europol, nello svolgimento di una delle sue funzioni principali quale la raccolta, la conservazione, il trattamento, l'analisi e lo scambio di informazioni e di *intelligence*, si adopera per il collegamento tra l'unità centrale e le unità nazionali, presso cui si trovano ufficiali di collegamento.

Come si legge nel *considerandum* 10 della decisione che istituisce l'Ufficio europeo di polizia[374], per evitare inutili procedure è opportuno che le unità dislocate negli Stati membri abbiano accesso diretto ai dati del sistema d'informazione Europol.

L'art. 11 della decisione 2009/371/GAI individua Europol stesso come unico responsabile del corretto funzionamento del sistema informativo, sia dal punto di vista tecnico e operativo, sia dal punto di vista dell'attuazione dei successivi articoli 20, 29, 31 e 35, rispettivamente riguardanti i termini per la conservazione e la cancellazione dei dati, la responsabilità in materia di trattamento dei dati, il diritto dell'interessato di rettifica e cancellazione dei dati, la sicurezza dei dati. L'unità nazionale, sempre a norma dell'art. 11, è responsabile della comunicazione con il sistema d'informazione Europol ed in particolare per l'attuazione dell'art. 35 in materia di misure di sicurezza.

L'archivio di Europol può essere usato per trattare unicamente i dati necessari allo svolgimento dei compiti del medesimo Ufficio.

I dati immessi riguardano persone che, in base alla legislazione nazionale dello Stato membro interessato, sono sospettate di aver commesso un reato di competenza di Europol o aver concorso alla sua commissione o soggetti che sono stati condannati per siffatti reati e persone rispetto alle quali esistono

---

[372] Il tema generale della gestione delle informazioni nello spazio europeo di libertà, sicurezza e giustizia è trattato compiutamente ed efficacemente nella Comunicazione della Commissione al Parlamento e al Consiglio del 20 luglio 2010 – COM(2010) 385 definitivo.

[373] Sulle competenze ed il ruolo di Europol, Eurojust e Olaf si rinvia alla lettura del capitolo I, paragrafo 6.

Tra i molteplici sistemi informativi e banche dati comunitarie si ricorda il Sistema informativo Schengen I e II, il sistema VIS, EURODAC, ECRIS per i casellari giudiziari, API – *Advance Passenger Information*, il Sistema Informativo Doganale (SID), l'archivio d'identificazione dei fascicoli a fini doganali (FIDE).

[374] La decisione 2009/371/GAI è stata adottata a norma del titolo VI del Trattato UE.

indicazioni concrete o ragionevoli motivi per ritenere, in base alla legge nazionale dello Stato membro interessato, che possa commettere un reato per cui è competente Europol. Le informazioni possono essere inserite anche quando non si possiedono le generalità precise della persona e se introdotte da Europol direttamente ne deve indicare la fonte di provenienza. Se il procedimento contro l'interessato è definitivamente archiviato o il soggetto viene assolto, i dati relativi devono essere immediatamente cancellati.

Le informazioni inserite nel *database*, in base all'art. 12 della decisione, riguardano le generalità della persona, i codici di previdenza sociale, le patenti di guida, i documenti d'identità, gli elementi utili a identificare caratteristiche particolari (non codificanti il DNA) e, in via facoltativa ed aggiuntiva, i dati relativi ai reati commessi, con indicazioni di tempo e luogo, degli strumenti di reato effettivi o potenziali, dei servizi responsabili e riferimenti delle pratiche, l'eventuale motivo di sospetto di appartenenza ad un'organizzazione criminale, le condanne per reati di competenza di Europol, le generalità della parte che ha introdotto i dati nel sistema informativo.

In base all'art. 13, le unità nazionali, gli ufficiali di collegamento, il direttore, i vicedirettori, il personale di Europol debitamente autorizzato hanno il diritto di introdurre e ricercare i dati direttamente nel sistema. Europol può estrarre i dati nel momento in cui sono utili per lo svolgimento dei propri compiti; le unità nazionali e gli ufficiali di collegamento li estraggono conformemente alle disposizioni legislative, regolamentari, amministrative e procedurali della parte che accede.

Solo la parte che ha immesso i dati può modificarli, rettificarli o cancellarli[375].

Europol prevede una funzione di indice per i dati conservati negli archivi di lavoro per fini di analisi, ovvero quegli archivi realizzati ex art. 14. L'accesso alla funzione indice è concepito in modo che sia possibile determinare se un'informazione è conservata in un archivio di analisi ma non consente di effettuare alcun altro collegamento o deduzione immediati[376].

L'art. 15 legittima il direttore, i vicedirettori e il personale Europol autorizzato, gli ufficiali di collegamento e i membri autorizzati delle unità nazionali ad accedere alla funzione indice. Questa funzione è strutturata in modo da consentire ai soggetti che ne fanno uso di sapere con certezza, in base ai dati consultati, se un archivio di lavoro per fini di analisi contiene dei dati di interesse.

---

[375] Per un approfondimento su tutta la casistica che riguarda l'immissione, la rettifica e la cancellazione dei dati nel sistema d'informazione di Europol, specie quando riguardano soggetti per cui più parti detengono informazioni, si rinvia all'art. 13 della Decisione istitutiva di Europol.

[376] La funzione indice è richiamata all'art. 15 della Decisione 2009/371/GAI. Per conoscere le modalità di costituzione di un archivio di lavoro per i fini di analisi si rinvia all'art. 16 della medesima Decisione.

In base all'art. 18, Europol istituisce, in cooperazione con gli Stati membri, adeguati meccanismi di controllo per verificare la legittimità delle operazioni di recupero e di archiviazione delle informazioni nel sistema e di raccolta di materiali provenienti da un altro archivio automatizzato.

I dati contenuti nei *databases* sono conservati per il tempo necessario allo svolgimento delle funzioni. L'esame e la cancellazione dei dati sono effettuati dalla parte che li ha immessi[377].

Gli strumenti di gestione delle informazioni a disposizione di Europol comprendono il sistema di informazione SIE, gli archivi di lavoro per fini di analisi (AWF) e l'applicazione SIENA. L'applicazione SIENA è utilizzata (non solo da Europol) per potenziare la condivisione di dati sensibili ai fini di contrasto alla criminalità.

In concreto, il sistema informativo di Europol (denominato TECS), che ha affiancato il Sistema Informativo Schengen (SIS), é caratterizzato da una struttura centralizzata.

I dati archiviati sono tanto utili ai fini di giustizia in quanto analizzati scientificamente dal personale qualificato, allo scopo di fornire delle indicazioni utili da applicare operativamente[378].

Il Protocollo aggiuntivo alla Convenzione istitutiva di Europol prevede alcune norme specifiche ed aggiuntive sulla disciplina dei sistemi informativi dell'Ufficio di Polizia.

In particolare, all'art. 1, definisce "*archivi di Europol*", tutti i *record,* la corrispondenza, i documenti, i manoscritti, i dati di *computer* e di *media*, le fotografie, i film, le registrazioni video e di suoni appartenenti o in possesso di Europol o di un membro del suo personale, ed ogni altro materiale analogo che, e parere unanime dei direttore e del consiglio di amministrazione, possa ritenersi parte integrante degli archivi di Europol. L'art. 3 statuisce l'inviolabilità di detti archivi, indipendentemente dalla loro ubicazione.

Il capo V della Decisione 2009/371/GAI disciplina il grado di protezione e di sicurezza dei dati. Il rinvio espresso è alle disposizioni della raccomandazione R(87) 15 del 17 settembre 1987 del Comitato dei Ministri del Consiglio d'Europa laddove indica i principi cardine per il trattamento dei dati automatizzati e non contenuti in archivi.

A norma dell'art. 28 della decisione è prevista la nomina un soggetto responsabile del trattamento che agisce in modo indipendente, garantendo il rispetto delle disposizioni in materia, anche mediante la cooperazione con il personale Europol e con l'autorità di controllo comune.

Ai sensi dell'art. 30, chiunque ha diritto di sapere se i dati personali che lo riguardano sono stati o meno trattati da Europol e di averne comunicazione in

[377] Cfr art. 20 Decisione.
[378] Così E. APRILE *Diritto processuale penale europeo e internazionale*, Cedam, 2007, pagg. 50-51.

forma intellegibile o di farli verificare. L'interessato detiene anche un diritto alla rettifica o cancellazione dei dati a lui riferibili [379].

Europol adotta le misure tecniche e organizzative necessarie per garantire la sicurezza dei dati, attuando misure atte a negare l'accesso alle persone non autorizzate, ad impedire che persone non autorizzate leggano, copino, modifichino o rimuovano supporti di dati, a prevenire l'intrusione ed il trattamento ingiustificato di dati, a controllare gli utilizzatori, gli accessi effettuati e le comunicazioni fatte[380].

Europol e gli Stati membri adottano misure appropriate per garantire la protezione delle informazioni soggette ad obbligo di riservatezza. Tutti i membri del personale si obbligano a rispettare il segreto e la riservatezza dei dati conosciuti nello svolgimento della propria attività [381].

Il consiglio di amministrazione di Europol, in base al contenuto della decisione istitutiva 2009/371/GAI, il 4 giugno 2009, ha emanato una decisione (2009/1010/GAI) aggiuntiva che chiarisce le condizioni di trattamento dei dati del sistema d'informazione Europol. In particolare, all'art. 3 stabilisce che i dati personali contenuti nella banca dati Europol possono essere trattati solo dal personale all'uopo autorizzato e sono utilizzati solo per l'espletamento dei propri compiti[382].

Già con l'Atto del Consiglio europeo del 3 novembre 1998 sono state adottate le norme sul segreto delle informazioni di Europol, applicabili agli archivi di analisi, che poi ha trovato il suo corrispondente, come visto, nella Decisione del 2009.

Il 26 marzo 2009, a Strasburgo, è stato approvato il testo della Raccomandazione del Parlamento europeo, destinata al Consiglio, sul rafforzamento della sicurezza e delle libertà fondamentali su Internet. In questo testo, alla raccomandazione contrassegnata dalla lettera h), il Parlamento invita il Consiglio a garantire che i lavori intrapresi nell'ambito del progetto " *check the web*"e le iniziative per permettere una rapida circolazione delle informazioni sulla cibercriminalità siano sviluppate, anche mediante la creazione e la gestione da parte di Europol di una piattaforma di allarme europea appositamente istituita per questa categoria di reati.

A seguito degli attentati terroristici dell'11 settembre 2001, è stata percepita in Europa l'esigenza di istituire un Unità di cooperazione giudiziaria,

[379] Cfr art. 31 Decisione.
[380] Cfr art. 35 Decisione.
[381] Cfr. artt. 40-41 Decisione.
[382] Per approfondimenti sul tema della tutela dei dati personali e della sicurezza dei dati, nonché sulla loro conservazione, si rinvia alla lettura integrale del testo della menzionata decisione del Consiglio di Amministrazione di Europol.

denominata *Eurojust*[383]. Questo organismo, nello svolgimento delle sue funzioni, si avvale dell'imprescindibile supporto di una banca dati.

I 27 membri che ne compongono il Collegio sono autorizzati ad accedere ai dati personali degli indagati e degli autori dei reati, in particolare ai dati anagrafici, ai recapiti, ai dati di immatricolazione dei veicoli, ai profili di DNA, alle fotografie, alle impronte digitali, ai dati messi a disposizione dai fornitori di servizi di telecomunicazioni e relativi al traffico, all'ubicazione e agli abbonati. Tutte le informazioni che si riferiscono a un caso devono essere inserite nel sistema automatico di gestione dei fascicoli che è applicato sulla rete TESTA della Commissione europea[384].

Un sistema di indice permette la conservazione sistematizzata dei dati personali e non personali, rilevanti per le indagini in corso.

La banca di dati di Eurojust, ormai giunta alla terza generazione (EPOC-III), è caratterizzata da una gestione unica e centralizzata di tutti i dati[385].

Eurojust può scambiare informazioni con autorità nazionali e Paesi Terzi con cui ha concluso accordi.

I dati possono essere conservati per tutto il tempo necessario allo svolgimento dei compiti e al raggiungimento degli obiettivi dell'Unità di cooperazione, ma devono essere cancellati immediatamente, appena chiuso il caso.

La decisione del Consiglio istitutiva di Eurojust del 28 febbraio 2002 (2002/187/GAI), nella parte in premessa, richiama espressamente gli obiettivi perseguiti dal regolamento (CE) n. 1073/1999 del Parlamento europeo e del Consiglio, del 25 maggio 1999, consentendo all'Unità di cooperazione di utilizzare il materiale delle indagini svolte dall'Ufficio per la lotta antifrode (OLAF).

In ragione dell'elevato grado di sensibilità delle attività compiute da Eurojust e dei dati da esso acquisiti, è escluso l'accesso di OLAF a documenti,

---

[383] Quanto al ruolo e alle funzioni di Eurojust si rinvia al capitolo primo, paragrafo 6.

[384] L'interconnessione mediante il sistema TESTA (*Trans-European Services for Telematics between Administrations*) permette la trasmissione delle informazioni in via telematica, garantendo l'immediata notificazione e la risposta in tempo reale alle richieste di informazioni. Di più, il sistema TESTA procede automaticamente alla memorizzazione delle informazioni inviate nella sua banca dati, in modo tale da ottenere un ulteriore risparmio di tempo nel caso di una successiva richiesta concernente gli stessi dati da parte di un altro Paese.
La rete TESTA è da lungo tempo utilizzata anche dalla Commissione europea ed è da essa finanziata, anche per lo studio di evoluzioni di sistema.
Cfr AA.VV. *Cooperazione informativa e giustizia penale nell'Unione europea* (a cura di F. PERONI – M. GIALUZ), Edizioni CRTrieste, 2009, pagg. 202-205.

[385] La modalità di gestione centralizzata, propria della banca dati di Eurojust ma anche di TECS, rispecchia un'idea secondo cui le informazioni sono principalmente di "proprietà" delle autorità nazionali di provenienza e, per questo motivo, si deve procedere ad un controllo serrato sulle modalità di visualizzazione e trasmissione tra i Paesi.
Cfr *Ibidem*, pag. 125.

relazioni, note o informazioni, qualunque ne sia il supporto, detenuti o creati nel quadro della trattazione delle cause dell'Ufficio di cooperazione, siano esse in corso o concluse.

Conformemente alla decisione istitutiva, Eurojust stabilisce un indice dei dati relativi alle indagini e può costituire degli archivi di lavoro temporanei, contenenti anche dati personali (art. 14)[386].

In base al disposto dell'art. 16 della Decisione, l'Ufficio di cooperazione giudiziaria dell'UE gestisce un *database* automatizzato che è caratterizzato da un indice molto dettagliato, volto a fornire un sostegno alla gestione e al coordinamento delle indagini e delle azioni penali al cui coordinamento contribuisce l'Eurojust, segnatamente tramite il controllo incrociato delle informazioni; agevolare l'accesso alle informazioni sulle indagini e le azioni penali in corso; agevolare il controllo della legittimità del trattamento dei dati personali e del rispetto della decisione istitutiva dell'Ufficio.

L'indice contiene rinvii agli archivi di lavoro temporanei istituiti da Eurojust.

In base al disposto dell'art. 18, solo i membri nazionali e i loro assistenti, nonché il personale autorizzato di Eurojust possono avere accesso ai dati personali trattati dall'Ufficio di cooperazione giudiziaria .

Chiunque ha il diritto di chiedere a Eurojust che si rettifichino, blocchino o cancellino le informazioni che lo riguardano, qualora risultino errate o incomplete o nei casi in cui l'inserimento o la conservazione di queste siano contrari alle disposizioni di garanzia della decisione istitutiva dell'Ufficio (art. 20).

Sia Eurojust sia gli Stati membri, nella misura in cui siano interessati dai dati trasmessi, assicurano la protezione delle informazioni contro la distruzione accidentale o illecita, la perdita accidentale o la diffusione,

---

[386] L'art. 14 della Decisione 2002/187/GAI prevede che Eurojust può, nell'ambito delle sue competenze e per svolgere le sue funzioni, trattare dati personali avvalendosi di procedimenti automatizzati o di casellari manuali strutturati. L'Ufficio di cooperazione giudiziaria adotta le misure necessarie per garantire un livello di protezione dei dati personali almeno equivalente a quello risultante dall'applicazione dei principi sanciti dalla convenzione del Consiglio d'Europa del 28 gennaio 1981 e successive modifiche. I dati personali raccolti da Eurojust e forniti dalle autorità competenti degli Stati membri o da altri *partner*, sono adeguati, pertinenti e non eccedenti rispetto alle finalità del trattamento.
L'art. 15 prevede che Eurojust possa trattare, nell'ambito delle sue specifiche competenze come previste dalla Decisione istitutiva dell'Ufficio, solo dati afferenti il nome, il cognome, l'*alias* o gli pseudonimi delle persone interessate; la data e il luogo di nascita; la cittadinanza, la razza e la nazionalità; il sesso, il luogo di residenza, di svolgimento della professione e di soggiorno; i codici di previdenza sociale, le patenti di guida, i documenti d'identità e i dati del passaporto; le informazioni riguardanti le persone giuridiche, se comprendono informazioni relative a persone fisiche identificate o identificabili ed oggetto di un'indagine o di un'azione penale; i conti bancari e conti presso altri istituti finanziari; la descrizione e la natura dei fatti contestati, la data in cui sono stati commessi, la loro qualifica penale e il livello di sviluppo delle indagini; i fatti che fanno presumere l'estensione internazionale del caso; le informazioni relative alla presunta appartenenza ad un'organizzazione criminale.

l'alterazione e l'accesso non autorizzati o contro qualsiasi altra forma di trattamento non autorizzato (art. 22).

L'Ufficio di cooperazione giudiziaria, conformemente al diritto nazionale dello Stato membro in cui ha sede, è responsabile di qualsiasi danno causato ad una persona derivante da un trattamento di dati non autorizzato o scorretto effettuato (art. 24).

L'obbligo della riservatezza si applica a qualsiasi persona e a qualsiasi organismo che collabori con Eurojust (art. 25).

L'Ufficio di cooperazione può inoltre stipulare accordi o accordi di lavoro con Europol, Olaf, l'Agenzia per la gestione della cooperazione operativa alle frontiere esterne degli Stati membri dell'Unione europea (Frontex), con il Consiglio europeo ed in particolare il suo centro di situazione congiunto e con la rete europea di formazione giudiziaria, al fine di concordare lo scambio di informazioni (art. 26, paragrafo 2) [387].

Eurojust ha sviluppato una stretta collaborazione con OLAF. Per le esigenze di ricezione e trasmissione delle informazioni tra Eurojust e OLAF, gli Stati vigilano affinché i membri nazionali di Eurojust siano considerati autorità competenti esclusivamente per le esigenze dei regolamenti (CE) n. 1073/1999 e Euratom n. 1074/1999 del Consiglio del 25 maggio 1999, relativo alle indagini svolte dall'Ufficio per la lotta antifrode (art. 26).

OLAF, nello svolgimento dei suoi compiti[388], raccoglie e tratta una quantità considerevole di dati. A tutte le informazioni comunicate all'Ufficio è riservata un'adeguata protezione, in osservanza del Regolamento CE 45/2001 a cui ha aderito.

Nel corso dell'indagine coordinate da OLAF, i dati possono essere trasmessi anche alle autorità competenti degli Stati membri e alle istituzioni, organi e organismi interessati (l'Ufficio è l'interlocutore diretto delle autorità giudiziarie e delle autorità preposte all'applicazione della legge nazionali) [389].

La Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (CE) n. 1073/1999, relativo alle indagini svolte dall'Ufficio per la lotta antifrode (OLAF) (COM(2006) 244 definitivo, mai

---

[387] Eurojust e Olaf hanno sottoscritto, in data 14 aprile 2003, un memorandum d'intesa basato su alcune direttive principale espresse, tra cui la selezione delle informazioni relative a singoli casi specifici, da trasmettere reciprocamente.
L'art. 10 della decisione 2008/976/GAI prevede che la Rete giudiziaria europea e Eurojust intrattengano rapporti privilegiati anche attraverso la messa a disposizione reciproca delle informazioni raccolte dalle unità centrali.
Cfr C.M. PAOLUCCI *Cooperazione giudiziaria e di polizia in materia penale,* Utet, 2011, pagg. 456-457.

[388] Per un approfondimento sul ruolo di OLAF e le sue competenze si rinvia al capitolo primo, paragrafo 6.

[389] Si veda la decisione istitutiva di Olaf : Decisione 1999/352/CE, CECA, Euratom della Commissione europea, del 28 aprile 1999.

pubblicato in Gazzetta Ufficiale CE), auspicava un accrescimento della cooperazione informativa tra questo organo e le istituzioni e gli organi europei, tra OLAF e Stati membri, tra OLAF e informatori, riconoscendo l'importanza dei dati da questo raccolti nello svolgimento della propria attività [390].

Come meglio descritto nella relazione dell'attività relativa all'anno 2007[391], OLAF, dal punto di vista delle strutture di archiviazione dei dati, è dotato del cd. *Case Management System*. Questa infrastruttura computerizzata è la prima risorsa d'informazioni organizzative dell'Ufficio. Esa contiene il *database* di OLAF e tutte le informazioni delle attività nuove, in corso e concluse. Mediante la consultazione di questo sistema informativo, il personal e autorizzato può tenere sotto osservazione lo stato di avanzamento dei singoli casi in tutte le fasi, dalla genesi all'epilogo, garantendo l'integrità dei documenti originari. Tutti gli avvenimenti significati ed i dati utili, riguardanti un caso, sono registrati nel sistema.

I dati raccolti nel corso di attività investigative di *computer forensics* promosse da OLAF sono inseriti in archivio e, a ciascuno, è correlato un segno, un simbolo, una parola chiave o qualsiasi altro mezzo che possa identificarne il contenuto e permetta di riferirlo direttamente ad un caso specifico trattato. In questo modo viene agevolata anche la ricerca e l'analisi successiva dei dati [392].

7.1 Le altre principali banche dati UE

L'Unione europea ha fatto grossi passi in avanti da quando, nel 1985 nella località di Schengen, i *leader* di cinque Paesi europei hanno deciso di abolire i controlli alle frontiere comuni. Da lì si è sviluppata, nel 1990, la convenzione Schengen, madre di tutte le politiche informative che oggi contano uno sviluppo considerevole nello spazio giudiziario europeo.

Nell'alveo dei molteplici archivi dell'Unione europea è possibile distinguere tra banche dati tendenzialmente giudiziarie (come EPOC –III di Eurojust), di *intelligence* (come TECS di Europol), di polizia (come la banche dati interforza) e archivi misti (come il VIS).

---

[390] Per leggere il testo della proposta di regolamento si consulti l'indirizzo internet: http://europa.eu/legislation_summaries/fight_against_fraud/antifraud_offices/l34008_it.htm (consultato in data 30 ottobre 2010).

[391] La relazione dell'attività di OLAF del 2007 è la più recente consultabile sulla pagina internet http://ec.europa.eu/ anti_fraud/reports/olaf/2007/en.pdf (consultato in data 13 novembre 2010).

[392] I dati sono archiviati per un tempo massimo di vent'anni dopo la conclusione delle indagine e poi sono immediatamente distrutti.

Per un approfondimento sulla normativa di protezione dei dati applicata da Olaf si rinvia alla pagina web: www.ec.europa.eu/dgs/olaf (consultato in data 23 febbraio 2011)

L'analisi della disciplina specifica di ciascuna banca dati e l'identificazione della *res* acquisibile, permette di potere inserire un archivio nell'una o nell'altra categoria.

L'Unione europea non si è occupata soltanto di sviluppare dei *databases* interni al proprio ambito territoriale, ma anche di incrementare le dinamiche di scambio di informazioni nei rapporti transfrontalieri.

Il *Sistema d'Informazione Schengen* (SIS) è operativo dal 1995 nello scopo di preservare la sicurezza pubblica, interna allo Stato e interna allo spazio Schengen, e facilitare la circolazione delle persone mediante l'uso di informazioni comunicate attraverso questo sistema.

Il SIS, attualmente giunto ad una versione evoluta di seconda generazione (SIS II), si caratterizza per essere un archivio centralizzato, costituito da una sezione nazionale presso ciascuno Stato partecipante (N-SIS) e da un'unità centrale di supporto tecnico in Francia, a Strasburgo (C-SIS).

Gli Stati membri possono segnalare persone ricercate per l'arresto ai fini dell'estradizione; cittadini di Paesi Terzi ai fini della non ammissione; persone scomparse; testimoni e persone citate a comparire dinanzi all'autorità giudiziaria; persone e veicoli soggetti a monitoraggio straordinario, in quanto costituiscono una minaccia per la sicurezza pubblica o la sicurezza dello Stato; veicoli, documenti e armi da fuoco persi o rubati; banconote registrate.

I dati inseriti nel SIS indicano i nomi e gli *alias* o gli pseudonimi, i segni fisici caratteristici, la data e il luogo di nascita, la cittadinanza e l'indicazione se la persona è armata o violenta.

Lo scambio di dati avviene solo tramite C-SIS che, ricevuta la segnalazione da parte di N-SIS, la trasmette a tutti gli altri N-SIS.

Ai dati possono accedere, nell'ambito delle rispettive competenze legali, le autorità di polizia, le autorità di controllo alla frontiera, le autorità doganali e le autorità giudiziarie nei procedimenti penali. Le autorità competenti per le immigrazioni e gli organismi consolari possono consultare soltanto i dati relativi ai cittadini di Paesi Terzi iscritti nell'elenco delle persone soggette a divieto d'ingresso e le informazioni sui documenti persi o rubati. Anche Europol ed Eurojust hanno accesso ad alcune categorie di dati inseriti nel SIS[393].

I dati personali inseriti nel Sistema Informativo Schengen ai fini della ricerca di un soggetto, possono essere conservati solo per il tempo necessario al raggiungimento dello scopo per cui sono stati raccolti, mentre i dati sul monitoraggio straordinario di persone ritenute pericolose per la sicurezza

[393] In particolare, Europol ha accesso ai dati relativi alle persone soggette a monitoraggio straordinario e ai dati relativi alle persone ricercate per l'arresto ai fini dell'estradizione; Eurojust può accedere alle segnalazioni relative alle persone ricercate per l'arresto ai fini dell'estradizione e alle segnalazioni relative ai testimoni e alle persone citate a comparire dinanzi all'autorità giudiziaria.

dell'Unione europea, devono essere tassativamente cancellati dopo un anno dall'archiviazione[394].

Le interrogazioni al sistema generano un *"hit"* (risposta positiva) quando l'informazione richiesta corrisponde ad una segnalazione esistente. Una volta ottenuta la segnalazione positiva, le autorità di contrasto possono chiedere notizie supplementari sulla persona o sull'oggetto a cui si riferiscono tramite la rete di uffici SIRENE[395].

Con l'ingresso nello spazio Schengen dei nuovi Sta, Le segnalazioni al SIS sono aumentate in maniera considerevole da quando hanno fatto ingresso nell'area Schengen gli Stati dell'Europa dell'Est. Tra gennaio 2008 e gennaio 2010 il numero totale di segnalazioni è passato da 22,9 milioni a 31,6 milioni [396].

Questo dato allarmante ha reso necessario lo sviluppo del sistema di seconda generazione con funzioni tecniche potenziate, in grado di gestire un maggiore numero di dati e di interconnettere orizzontalmente tutte le informazioni riferite ad uno stesso soggetto[397].

Il SIS applica il principio della limitazione dei fini nel trattamento dei dati, per cui le informazioni canalizzate nel Sistema possono circolare ed essere utilizzate solo per i fini per cui sono state richieste[398].

Il rispetto del canone di finalità limitata è garantito anche dalle regole di funzionamento della banca dati *Eurodac*.

---

[394] Attualmente il SIS è applicabile nella sua interezza di potenzialità in 22 Stati membri, oltre che in Svizzera, Norvegia e Islanda; il Regno Unito e l'Irlanda partecipano con l'esclusione delle segnalazioni relative ai cittadini di Paesi Terzi iscritti nell'elenco delle persone soggette a divieti d'ingresso; Cipro, Romania e Bulgaria hanno firmato la convenzione ma non l'hanno ancora attuata.

[395] SIRENE è l'acronimo di *Supplementary Information Request at National Entry* (Informazioni supplementari richieste all'atto dell'ingresso nel territorio nazionale).
Il manuale SIRENE consta di in un insieme di istruzioni indirizzate agli operatori degli uffici SIRENE dei singoli Stati membri.
Si tratta, in particolare, di regole e procedure attinenti allo scambio, bilaterale o multilaterale, delle informazioni supplementari, nell'ambito del sistema Schengen.
La Commissione, attese le profonde modifiche ed evoluzioni che hanno interessato il diritto dell'Unione europea negli ultimi anni, è intervenuta modificando alcuni aspetti della disciplina, per garantire l'uniformità delle procedure e l'adeguamento agli sviluppi intervenuti, mediante una decisione del 1 luglio 2011, pubblicata in Gazzetta Ufficiale CE il 15 luglio 2011.
Il manuale precedente del 2007 é, dunque, sostituito per intero dalla nuova versione che cerca di meglio adeguare l'attività crescente degli uffici SIRENE alle esigenze di protezione dei dati personali.

[396] I dati provengono dai Documenti del Consiglio europeo n. 5441/08 del 30 gennaio 2008 e n. 6162/10 del 5 febbraio 2010.

[397]Il progetto di sviluppo del Sistema Informativo Schengen è stato affidato alla Commissione europea, avvalendosi dell'applicazione della rete di trasmissione sicura, già nota ed utilizzata da questo organismo comunitario, denominata s-TESTA (acronimo di *Secure Trans-European Services for Telematics between Administrations* – Rete di servizi trans europei sicuri per la comunicazione telematica tra amministrazioni).

[398] I riferimenti sull'organizzazione del SIS e del SIS II si trovano in C.M. PAOLUCCI *op.cit*., pagg. 468-469; AA.VV. *Cooperazione informativa*, *op.cit*.; Comunicazione della Commissione al Parlamento europeo e al Consiglio COM (2010)385 definitivo.

Questo archivio contiene informazioni relative agli stranieri che hanno attraversato irregolarmente le frontiere dell'Unione europea.

Eurodac è un sistema centralizzato e informatizzato di identificazione delle impronte digitali di determinati cittadini di Paesi Terzi. È entrato in funzione a partire dal gennaio 2003 in tutti gli Stati membri (esclusa la Danimarca), in Norvegia e in Islanda. Nel 2004 i dieci nuovi Stati membri dell'Europa dell'Est si sono aggiunti, seguiti dalla Danimarca e poi dalla Romania e dalla Bulgaria. In seguito sono stati siglati degli accordi con la Svizzera e con il Liechtenstein al fine di consentire anche a questi Paesi di utilizzare il sistema.

Lo scopo principale di Eurodac è quello di coadiuvare l'esame di una domanda di asilo da parte di uno Stato membro.

Alle persone di età inferiore ai 14 anni che chiedono asilo in uno Stato membro e a coloro che sono fermati in relazione all'attraversamento irregolare di una frontiera esterna, sono rilevate automaticamente le impronte. Confrontando tali impronte con quelle registrate in Eurodac è possibile identificare le persone che sono state trovate illegittimamente presenti sul territorio nazionale di uno Stato UE.

Ogni Stato ha il compito di comunicare l'elenco delle autorità che sono legittimate all'accesso dei dati di Eurodac[399].

I Paesi membri inseriscono i dati pertinenti nella banca dati centrale tramite i punti di accesso nazionali.

Le impronte digitali dei richiedenti asilo sono conservate per dieci anni, mentre quelle dei migranti in situazione di irregolarità sono cancellate appena l'interessato ha ottenuto un permesso di soggiorno o la cittadinanza di uno Stato membro oppure dopo che ha lasciato il territorio degli Stati membri.

Anche Eurodac funziona tramite la rete s-TESTA della Commissione europea.

Per quel che concerne il profilo relativo alla protezione dei dati, è applicabile la direttiva 95/46/CE e il regolamento CE n. 2275/2000 che pone una serie di regole particolari.

In sintesi, il regolamento riafferma i canoni di legalità e finalità limitata (art. 1) e prevede dei limiti all'accesso. L'art. 15 legittima l'accesso di ciascuno Stato membro ai soli dati da esso inseriti (ad eccezione di quelli relativi alla presenza di precedenti richieste di asilo). Sul piano soggettivo, il regolamento riconosce alle persone interessate il diritto ad essere informate sul responsabile del trattamento e sulle finalità dello stesso, nonché i diritti di chiedere la rettifica e la cancellazione dei dati (art. 18).

[399] Solitamente sono indicate le autorità competenti per le materie dell'asilo e dell'immigrazione, le guardie di frontiera e le autorità di polizia.

La Commissione europea è tenuta a trasmettere annualmente al Parlamento europeo e al Consiglio europeo una relazione sull'attività dell'unità centrale di Eurodac.

Sul piano operativo, si è notato che il sistema ha funzionato in maniera ambivalente. Nel periodo 2003-2005 sono stati trasmessi con successo i dati relativi a 657.753 richiedenti asilo e sono stati registrati nella banca da ti centrale i dati relativi a 48.657 cittadini di Paesi Terzi, fermati mentre attraversavano clandestinamente una frontiera esterna. Nello stesso arco temporale, sono stati registrati i dati relativi a 101.884 cittadini di Paesi Terzi in posizione irregola re nel territorio di uno Stato membro. Nei due anni successivi, sono aumentate significativamente le registrazioni dei dati dei richiedenti asilo e dei soggetti fermati all'atto dell'attraversamento dei confini esterni [400].

I maggiori profili di problematicità nella gestione di questo sistema d'informazione si sono riscontrati con riferimento alla tutela dei dati personali, specie per quanto attiene la cancellazione dei dati riferiti ad un soggetto che ottiene il permesso di soggiorno o la cittadinanza, poiché spesso lo Stato membro che ha inserito i dati non è informato della nuova posizione dell'interessato [401].

Se Eurodac é ormai una realtà testata, il *Sistema di informazione Visti (Visa Information System* – VIS) rappresenta un tassello fondamentale della politica comune dell'Unione europea in materia di visti e costituisce una delle iniziative chiave per garantire la libera circolazione delle persone in uno spazio di libertà, sicurezza e giustizia.

L'idea ha preso le mosse già a partire da un'autorevole esplicitazione del Consiglio europeo di Laeken. Nelle conclusioni, infatti, i Capi di Stato e di Governo hanno invitato il Consiglio e gli Stati membri ad adottare le disposizioni necessarie per l'attuazione di un sistema comune di identificazione dei visti [402].

La Commissione europea, a meno di un anno di distanza dalla presentazione dello studio di fattibilità sul VIS, ha avanzato una proposta di decisione del Consiglio che istituisce il Sistema di Informazione Visti (COM(2004)99 definitivo).

VIS mira ad affrontare due aspetti fondamentali: migliorare l'attuazione della politica comune in materia di visti, agevolando l'esame delle domande di

[400] I dati si rinvengono nella Relazione della Commissione al Parlamento europeo e al Consiglio sulla valutazione del sistema di Dublino (COM(2007)299 definitivo) in http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0299:FIN:IT:PDF (consultato in data 30 aprile 2011).

[401] Per un approfondimento sul sistema Eurodac si veda AA.VV. *Cooperazione informativa*, *op.cit*.; Comunicazione della Commissione al Parlamento europeo e al Consiglio COM(2010)385 definitivo.

[402] Si vedano le conclusioni della Presidenza in http://ww.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/it/ec/68836.pdf (consultato in data 22 maggio 2011).

visto e i controlli ai valichi di frontiera esterni, contribuendo a prevenire le minacce alla sicurezza interna degli Stati membri.

Questo sistema informativo è di tipo centralizzato, gestito da un'unità centrale sita in Francia e da una sezione nazionale presso ciascuno Stato partecipante.

Il regolamento VIS, Regolamento CE n. 767/2008, disciplina quella che è destinata a divenire la più grande banca dati biometrica del mondo. Essa si avvale di un confronto biometrico per garantire l'attendibilità delle impronte digitali e verificare l'identità dei titolari del visto alle frontiere esterne.

Il VIS contiene dati relativi alle domande di visto, le fotografie, le impronte digitali, le decisioni correlate alla richiesta di visto e il collegamento con le relative domande.

In considerazione della delicatezza dei dati trattati, sono stati effettuati diversi studi volti ad approfondire il rapporto tra benefici e controindicazioni rispetto alla loro raccolta[403]. L'efficacia immediata di questo sistema è sicuramente l'agevolazione delle attività di prevenzione e lotta alle frodi sul visto e al cd. *visa shopping*.

Le autorità per il visto, l'asilo e l'immigrazione e le autorità di controllo alla frontiera hanno accesso alla banca dati del VIS per verificare l'identità del titolare del visto e l'autenticità del visto; Europol e le forze di polizia possono consultarla ai fini della prevenzione e della lotta al terrorismo e alle altre forme gravi di criminalità[404].

Il Regolamento VIS contempla quattro diverse forme di accesso a secondo dello scopo: a fini di verifica ai valichi di frontiera esterni (art. 18); ai fini di verifica all'interno del territorio degli Stati membri dell'identità del titolare del visto, dell'autenticità del visto o della sussistenza delle condizioni di ingresso, di soggiorno o di residenza (art. 19); ai fini di identificazione delle persone che non soddisfano le condizioni per l'ingresso, il soggiorno o la residenza nel territorio dello Stato membro (art. 20); per la determinazione della competenza per le domande di asilo (art. 21); per l'esame della domanda di asilo, da parte delle autorità competenti (art. 22).

L'ingresso alla banca dati non avviene in maniera diretta ma indiretta, attraverso uno o più punti d'accesso[405].

---

[403] In particolare, si veda il documento prodotto dal *Working Party on the protection of individuals with regard to the processing of personal data* (Gruppo Articolo 29) in http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_en.pdf (consultato in data 2 luglio 2011).

[404] Così nella Decisione quadro 2008/633/GAI del Consiglio, pubblicata in Gazzetta Ufficiale CE, L 218 del 13 agosto 2008.

[405] Il carattere indiretto dell'accesso è stato difeso dal Parlamento europeo, già nel corso dei lavori preparatori.

I fascicoli relativi alla domanda possono essere conservati per cinque anni. È prevista, inoltre, la cancellazione anticipata qualora il richiedente abbia acquisito la cittadinanza di uno tato membro (art. 25).

La gestione operativa del VIS centrale e delle interfacce nazionali viene affidata a un organo di gestione, lo stesso di SIS II e Eurodac.

Sul piano soggettivo, il Regolamento VIS riconosce agli interessati il diritto a essere informati sull'autorità nazionale competente per il controllo, sulle modalità di trattamento e sulle categorie di destinatari dei dati. è garantito un ampio diritto di accesso, rettifica e cancellazione da parte dell'interessato.

Il VIS è applicato in tutti gli Stati membri, esclusi il Regno Unito e l'Irlanda, e in Svizzera, Norvegia e Islanda.

Questo Sistema Informativo funziona sulla rete s-TESTA della Commissione europea[406].

Ad integrazione della Convenzione di Napoli II[407], relativa alla mutua assistenza e alla cooperazione tra amministrazioni doganali, la convenzione SID ha introdotto il *Sistema Informativo Doganale* (SID, appunto) per facilitare la prevenzione, la ricerca e il perseguimento di gravi infrazioni alla legge nazionale, rendendo più efficace, mediante la rapida diffusione di informazioni, la cooperazione tra amministrazioni doganali degli Stati membri[408].

Il SID è un sistema informatico centralizzato, gestito dalla Commissione europea e reso accessibile tramite terminali situati in ogni Stato membro (N-SID) e presso la Commissione europea, Europol e Eurojust.

I dati ivi archiviati sono raggruppati nelle seguenti categorie: merci, mezzi di trasporto, imprese, persone e merci, denaro contante bloccato, sequestrato o confiscato.

Le informazioni raccolte si sostanziano nel nome e nell'*alias* o negli pseudonimi, nella data e nel luogo di nascita, nella cittadinanza, nel sesso, nei segni particolari, nei documenti d'identità, nell'indirizzo, nelle eventuali segnalazioni se la persona ha già fatto uso di violenza, nei motivi dell'inclusione dei dati nel SID, nell'azione proposta e nel numero di immatricolazione del mezzo di trasporto.

Ai dati SID possono accedere le autorità nazionali doganali, tributarie, agricole, sanitarie e di polizia, Europol ed Eurojust.

---

[406] Per un approfondimento, vedi nota 46.

[407] Convenzione stabilita in base all'articolo K.3 del Trattato sul funzionamento dell'Unione europea, pubblicata in Gazzetta Ufficiale CE, C 24 del 23 gennaio 1998.

[408] La Convenzione SID è stata elaborata in base all'art. K.3 del Trattato sul funzionamento dell'Unione europea sull'uso dell'informatica nel settore doganale, pubblicata in Gazzetta Ufficiale CE, C 316, del 27 novembre 1995, modificata dalla decisione 2009/917/GAI del Consiglio europeo, pubblicata in Gazzetta Ufficiale CE, L 323 del 10 dicembre 2009.

I dati immessi in questo Sistema Informativo possono essere copiati in altri sistemi di trattamento dei dati soltanto ai fini di gestione dei rischi o di analisi operativa e possono essere consultati soltanto dagli analisti designa ti dagli Stati membri.

I dati personali copiati dal SID sono memorizzati per il tempo necessario al raggiungimento dello scopo e, comunque, per un tempo non superiore a dieci anni.

Il SID ha, inoltre, istituito un archivio di identificazione dei fascicoli ai fini doganali (*FIDE*) per aiutare, prevenire, ricercare e perseguire gravi infrazioni alle leggi nazionali[409]. Il FIDE consente alle autorità nazionali preposte alle indagini doganali, quando istruiscono un fascicolo, d'individuare le altre autorità che possono avere indagato sulle persone o sulle imprese in questione. Tali autorità possono immettere nel FIDE dati provenienti dal fascicolo, quali i dati anagrafici delle persone indagate e la ragione sociale, la denominazione commerciale, il numero di partita IVA e l'indirizzo delle imprese indagate.

I dati provenienti dai fascicoli in cui non sono state rilevate frodi doganali possono essere conservati per un periodo massimo di tre anni; se invece sono state rilevate frodi doganali possono essere conservati fino a sei anni. Qualora l'indagine abbia dato luogo a una condanna o all'applicazione di sanzioni, le informazioni possono essere conservati per dieci anni.

La convenzione SID è in vigore in tutti gli Stati membri.

Un cenno merita l'Organizzazione Internazionale di Polizia Criminale, meglio nota come *Interpol,* la quale opera attraverso una propria rete telematica, costituita da una banca dati mondiale collocata presso il Segretariato generale di Lione ed interrogabile in tempo reale attraverso il sistema di accesso diretto (*Automatic Search Facility*).

Nel 2010 l'Unione europea ha approvato la conclusione dell'accordo con gli Stati Uniti d'America sul trattamento ed il trasferimento di dati di messaggistica finanziaria UE, ai fini del programma di controllo delle transazioni finanziarie dei terroristi[410].

---

[409] Il FIDE, acronimo di *Fichier d'Identification des Dossiers d'Enquetes douanières,* si basa sul regolamento CE n. 766/2008 del Consiglio europeo.

[410] L'accordo TFTP UE-USA è stato concluso all'esito della Risoluzione del Parlamento europeo P7_TA-PROV(2010)0279 dell'8 luglio 2010. La proposta di accordo TPTF è stata sviluppata dal dipartimento del Tesoro degli Stati Uniti, in seguito agli attentati terroristici dell'11 settembre 2001, per identificare, controllare e perseguire i terroristi e i loro finanziatori.
Nel novembre del 2009, la presidenza del Consiglio dell'Unione europea e il governo degli Stati Uniti hanno firmato un accordo interinale sul trattamento ed il trasferimento dei dati di messaggistica finanziaria che il Parlamento europeo non ha approvato. Sulla base di un nuovo mandato, la Commissione europea ha negoziato un ulteriore progetto di accordo con gli Stati Uniti, presentando al Consiglio, in data 18 giugno 2010, una proposta che ha riscontrato l'assenso anche del Parlamento europeo in data 8 luglio 2010.

L'accordo obbliga i fornitori designati di servizi di messaggistica finanziaria a trasferire al dipartimento del Tesoro degli Stati Uniti, una serie di dati contenenti, tra l'altro, il nome, il numero di conto, l'indirizzo e il numero di identificazione dell'ordinante e/o del o dei beneficiari della transazione finanziaria. Gli Stati Uniti assisteranno l'Unione a istituire un sistema equivalente al *TFTP*. L'accordo è stato siglato per una durata di cinque anni e ciascuna parte può sospenderlo in ogni momento.

8. Il sistema delle banche dati nazionali: limiti e benefici

Non esistono delle fonti istituzionali e dei dati ufficiali per ricostruire il sistema delle banche dati nazionali degli Stati membri dell'Unione europea in materia penale, per i fini della cooperazione di polizia e giudiziaria.

Pertanto, non è possibile fornire un quadro esaustivo del grado di sviluppo dei sistemi di archiviazione di dati, delle normative ed del livello di garanzia dei diritti fondamentali[411].

Nel panorama giuridico europeo e mondiale, quasi quotidianamente si assiste ad istanze di sensibilizzazione allo sviluppo di archivi che raccolgano le informazioni più varie, al fine di potenziare l'apparato di prevenzione e lotta alla criminalità, specie transfrontaliera.

Da uno sguardo attento alla realtà circostante, ciascuno può acquisire la consapevolezza della quantità di dati prodotti, a volte inconsapevolmente, che spesso, a insaputa, sono raccolti, archiviati o collegati ad altre informazioni già note, per creare un *dossier* individuale.

Le informazioni conosciute possono essere un utile mezzo per descrivere le persone. Si pensi, per esempio, alle immagini tratte da *google street view*, oppure ai sistemi di geolocalizzazione dell'apparecchio comunicativo *i-phone* o ai dati bancari contenuti negli archivi degli Istituti di credito, ai dati delle comunicazioni telefoniche o telematiche intercorse e trattenuti dalle società che erogano questi servizi, alle informazioni, anche sensibili, trattenute da chi eroga i servizi più vari o dagli Internet Service Provider (ISP).

Tutti questi dati (e molti altri ancora), specie se incrociati, sono in grado di agevolare la ricostruzione di fatti, di vicende e della vita delle persone.

Dalla descrizione di questo panorama, si comprende l'esistenza di un numero elevato di banche dati presenti in ciascun territorio nazionale (oltre che

[411] In questo panorama di riferimento così magmatico ed evanescente, è degno di nota l'elenco delle banche dati europee divise per argomento oppure in ordine alfabetico, consultabile sulla pagina internet http://europa.eu/documentation/order-publications/databases-subject/index_it.htm#100 (consultato in data 3 agosto 2011).

in ambito comunitario), ciascuna delle quali è legittimamente competente a contenere e trattare alcune informazioni[412].

Non tutti questi archivi sono accessibili e creati appositamente per i fini della cooperazione di polizia e giudiziaria.

L'Unione europea ha prodotto una serie di atti normativi relativamente ai dati, alla loro protezione, alle modalità di trattamento e di circolazione, in alcune ipotesi onerando gli Stati partecipanti di istituire delle banche dati a livello nazionale, con l'obiettivo ultimo di creare uno spazio europeo di libertà, sicurezza e giustizia.

Alcune leggi fondamentali sul funzionamento e l'organizzazione dell'Unione europea prevedono l'istituzione di archivi caratterizzati da una limitazione di finalità, per il tramite dei quali possono essere trattate soltanto alcune categorie specifiche di informazioni che sono oggetto di raccolta (a volta generando anche delle ambigue sovrapposizioni tra strumenti informativi differenti, ma che contengono le medesime tipologie di dati).

In alcuni casi, le stesse materie interessate richiedono necessariamente lo sviluppo di banche dati nazionali, in collegamento tra loro per lo scambio di informazioni.

Si pensi, per esempio, alle politiche di protezione degli interessi finanziari dell'Unione europea, quale fattore trainante per lo sviluppo di sistemi informativi e di scambio di dati tra le autorità impegnate a garantire il rispetto delle norme in materia[413].

Un'ulteriore spinta di matrice europeistica, ma diretta agli Stati membri, invita allo sviluppo della cooperazione informativa e, quindi, anche delle

[412] Si consideri che le banche dati non contengono informazioni l'una necessariamente diverse dall'altra ma spesso vi sono delle sovrapposizioni di contenuti.

[413] Limitatamente al panorama italiano, si pensi, per esempio alla Centrale rischio finanziario, istituita e gestita dalla Banca d'Italia, che contiene dati sulle abitudine di pagamento di ciascuno o ancora il più noto CRIF, gestito da un Istituto di Credito di Bologna che ha il compito di immettere nei propri *database*, tutti gli elementi che le società finanziarie e creditizie gli segnalano sul conto dei propri debitori. Il problema nasce, perché mentre in tale banca dati circa l'85% dei dati inseriti si riferiscono a persone che pagano regolarmente ed onorano il loro debito, il restante 15% si riferisce a quelli che vengono indicati come "cattivi pagatori".
Ancora, sempre restando in Italia, le autorità fiscali hanno a disposizione un buon numero di banche dati per lo svolgimento delle indagini finanziarie. Oltre alle banche dati europee, quali VIES per il controllo dei dati sulle partite IVA, a livello nazionale dal 30 aprile 2007 è divenuta operativa l'anagrafe dei conti. Gli operatori finanziari (come banche e intermediari) devono comunicare all'archivio presso l'anagrafe tributaria l'esistenza di rapporti intrattenuti, i rapporti costituiti o cessati nel periodo a partire dal 2005, mediante comunicazione mensile.

banche dati per la prevenzione e la repressione dei cd. *serious crimes*[414] e della cibercriminalità[415].

È del 30 giugno 2011 l'approvazione della Commissione Finanza italiana della Camera dei Deputati della proposta di legge contro le frodi assicurative, che prevede la creazione di un archivio informatico nazionale[416].

Sarà istituita una struttura *ad hoc* presso l'Isvap la quale, avendo a disposizione questa banca dati, dovrebbe potere facilitare l'attivazione del sistema di allerta preventivo.

L'archivio sarà gestito dalla Consap.

Nel corso del tortuoso *iter* di definizione del testo della proposta di legge, uno dei principali ostacoli incontrati riguardava la definizione degli organismi legittimati all'accesso al sistema informativo[417].

La firma del Trattato di Prum, avvenuta il 27 maggio 2005, da parte di sette Paesi membri dell'Unione europea, segnatamente Belgio, Lussemburgo, Paesi Bassi, Germania, Francia, Spagna e Austria, rappresenta un tassello fondamentale nel lungo processo di sviluppo della cooperazione di polizia e giudiziaria tra gli Stati e della cooperazione informativa i n particolare.

La finalità principale di questo Trattato riguarda il potenziamento della cooperazione nella lotta al terrorismo, alla criminalità transfrontaliera e alla migrazione illegale.

Poiché è emerso l'interesse di vari Stati membri di aderire all' Accordo di Prum, durante la Presidenza tedesca del Consiglio europeo del 2007, la Germania ha proposto di trasformare il testo in uno strumento dell'UE.

La decisione di Prum fissa le norme per lo scambio transfrontaliero di profili DNA, impronte digitali, dati di immatricolazione dei veicoli e informazioni su persone sospettate di preparare attentati terroristici[418].

Questo strumento è da leggersi in chiave di complementarietà e di reciproca interazione, nel quadro della progressiva armonizzazione degli ordinamenti statali interni in materia penale e del rafforzamento della cooperazione tra le forze di polizia e le autorità giudiziarie deg li Stati membri.

---

[414] Per *serious crimes* si devono intendere i reati di maggiore allarme sociale, quali il terrorismo, la criminalità organizzata, il traffico di esseri umani e di sostanze stupefacenti.
È noto che, in materia di terrorismo, la spinta verso l'istituzione di organi e sistemi, anche informativi, per la prevenzione e repressione affonda le proprie radici già con il gruppo TREVI 1, creato nel 1976.

[415] Già nella proposta di decisione quadro del Consiglio europeo, COM(2002)173 definitivo, relativa agli attacchi contro i sistemi di informazione, la Commissione europea ha spinto gli Stati membri dell'Unione europea alla realizzazione di piattaforme informatiche in cui raccogliere i dati relativi al numero di attacchi e di reati informatici registrati e la tipologia di questi.

[416] Il fine principale è quello di calmierare i prezzi troppo elevati dei contratti assicurativi italiani, mediante la lotta alle frodi Rc auto.

[417] La notizia è stata pubblicata su Il Sole 24 Ore, n. 177 del 1 luglio 2011, pag. 33.

[418] Decisione 2008/615/GAI del Consiglio europeo; decisione 2008/616/GAI del Consiglio.

I primi due elementi caratterizzanti della decisione di Prum si sostanziano nella semplificazione dello scambio di informazioni tra le autorità e nella predisposizione di adeguate garanzie in materia di tutela dei dati, specie nella fase di circolazione.

Il sistema Prum è organizzato secondo una gestione decentrata, in grado di mettere in collegamento i punti di contatto nazionali e le banche dati istituite in ciascuno Stato membro, contenenti i profili di DNA, le impronte digitali e i dati di immatricolazione dei veicoli, avvalendosi della rete s-TESTA.

I punti di contatto nazionali hanno potere in ordine alla trasmissione di tali dati agli utenti finali, in osservanza alla disciplina nazionale e possono trattare le richieste ricevute e inviate per procedere al confronto transnazionale dei profili di DNA.

Il confronto dei profili DNA e delle impronte digitali può essere effettuato in base ad un sistema *hit/no hit* (anonimo) attraverso cui le autorità sono legittimate a chiedere informazioni personali su un soggetto interessato solo se la consultazione iniziale ha dato una risposta positiva [419].

L'atto europeo non considera la predisposizione di uno schedario unico europeo ma, rappresentando un esempio di attuazione del principio di disponibilità (seppure con zone d'ombra), incentiva la realizzazione della condivisione delle informazioni tra gli Stati.

A differenza di quest'ultima banca dati, che permettere di accedere direttamente ai dati relativi al proprietario a partire dal numero di immatricolazione, gli altri due archivi non consentono di identificare immediatamente la persona a cui si riferiscono, ma sono soggetti ad un procedimento comune di consultazione che si articola in due fasi. La prima fase disciplina l'accesso automatizzato *on line* all'interno delle banche di dati, rendendo disponibile solo gli indici di consultazione; in una seconda fase, all'esito del sistema *hit/no hit*, l'autorità richiedente può attingere all'informazione.

La procedura di accesso è anch'essa biforcata: ove l'autorità compulsante disponga di un profilo di DNA riferibile ad una persona identificata, questa può attivare la procedura di consultazione automatizzata (*automated searching*) al fine di verificare la concordanza con i dati già registrati in archivio; ove, per contro, la parte richiedente disponga di un profilo di DNA non attribuibile ad una persona determinata o determinabile, viene dato avvio ad un sistema di comparazione (*automated comparison*).

L'inoltro si compie in forma non automatizzata, a cura dell'autorità richiesta e solo nei casi in cui il sistema abbia permesso di registrare una concordanza.

[419] La Commissione europea presenterà una relazione di valutazione sull'applicazione della decisione di Prum al Consiglio nel corso del 2012.

Dalla lettura degli articoli 3 e 4 della decisione 2008/615/GAI, l'accesso alla banca dati del DNA sembra riservato alle attività di investigazione, mentre gli archivi riferiti alle impronte digitali e ai dati di immatricolazione dei veicoli sono compulsabili sia in fase investigativa, sia con finalità preventiva, sia con finalità repressiva.

Da uno sguardo d'insieme e da un'analisi comparatistica delle diverse banche dati del DNA istituite a livello nazionale, si riscontrano sistemi differenti di organizzazione e di gestione che possono rendere difficile lo scambio diretto dei dati tra gli Stati, in assenza di una mutua fiducia [420].

Bisogna premettere che in Europa, l'Inghilterra è l'unico Stato, al pari degli Stati Uniti e del Canada, a poter vantare una legislazione evoluta in materia di banca dati del DNA[421].

In Germania sono stati presentati diversi progetti di legge volti ad istituire una banca dati del DNA ma la definizione si è a lungo procrastinata, fino a che, nel 1998, un omicidio in Bassa Sassonia portò gli inquirente a richiedere un campione di saliva a circa diciottomila persone di sesso maschile, tra i diciotto e i trent'anni, residenti in quella regione. Così è stato chiaro che non era più possibile rinunciare ad avere un *database* del DNA.

Nell'aprile del 1998 è stato ufficialmente istituito un archivio nazionale del DNA, contenente le tracce rilevate sul luogo del delitto e i profili delle persone sospettate di un reato. Non è stata prevista la conservazione di campioni biologici. Inoltre, ai sensi del paragrafo 81a StPO, i campioni ematici possono essere prelevati da soggetti sospettati senza il loro consenso, da parte di un medico o su autorizzazione del giudice.

---

[420] Ecco perché si discute sulla fattibilità e l'opportunità di istituire un archivio di dati del DNA unico a livello europeo. Così C. FANUELE *Un archivio centrale per i profili del DNA nella prospettiva di un diritto comune europeo* in *Diritto Penale e Processo*, 2007, pagg. 387-401.

[421] La legislazione inglese in materia di banca dati del DNA, di cui si offrono solo brevi spunti, ha origine dal *Criminal Justice and Public Order Act* del 1994, prevedendo un *database* contenente i profili DNA delle persone condannate per alcuni reati dettagliati nella norma. Successivamente la CJPA 2001 ha ampliato l'applicazione della disciplina, incentivando il cd. *mass screening*, per permettere allo Stato di disporre di una piattaforma genetica completa della popolazione.

Il *Criminal Justice Act* del 2003 ha poi aggiunto alle preesistenti ulteriori categorie di soggetti i cui dati genetici possono essere archiviati, quali i sospettati di un reato.

L'entrata in vigore del CJA 2003 ha notevolmente indebolito le garanzie individuali e così, anche in considerazione del grande numero di profili di DNA contenuti nel *database* del Regno Unito, il *Forensic Science Service* ha perfezionato un software, chiamato *familiar searching*, in grado di elaborare una lista di possibili individui correlati da legami di parentela, sulla base di un singolo profilo di DNA.

Sono seguite ulteriori riforme legislative che hanno portato, nel 2006, alla possibilità di campionare i profili di DNA di tutte le persone arrestate.

Per un approfondimento sul sistema di banche dati del DNA e le norme regolatrici nel Regno Unito, si rinvia a C. FANUELE *Dati genetici e procedimento penale*, Giuffré, 2009, pagg. 168-194.

È vietato usare i profili di DNA per finalità diverse da quelle dell'accertamento penale e, in particolare, è proibito l'uso ai fini delle indagini sulla personalità o sul patrimonio genetico dell'imputato o del condannato.

I profili dei campioni genetici sono conservati in una banca dati istituita presso il *Bundeskriminalamt*; i dati ivi contenuti possono essere trattati e elaborati per finalità preventiva, repressiva o di cooperazione giudiziaria internazionale.

Successivamente, una legge del 12 agosto 2005, ha ampliato la categoria di soggetti i cui profili genetici sono suscettibili di conservazione, includendo anche i campioni prelevati da persone indagate nel corso di un procedimento per reati particolarmente efferati.

Di regola, dopo cinque o dieci anni dal passaggio in giudicato della sentenza, i dati vengono distrutti.

La normativa introdotta in materia di banca dati del DNA, poiché limitativa di libertà fondamentali, è stata sottoposta al vaglio della Corte Costituzionale Federale in ben tre diversi casi.

In tutti e tre le ipotesi la Corte ha ritenuto che la limitazione del diritto alla *privacy,* a seguito dell'applicazione di tale norma sui campioni del DNA, è legittimata da un interesse pubblico effettivo all'istituzione di un *database*, al fine di agevolare le attività d'indagine.

Lo stesso organo giurisdizionale ha tenuto, però, a precisare che è necessario valutare di caso in caso se sussistono i presupposti per l'inserimento dei campioni di DNA nell'archivio.

In Francia, al contrario, è stata adottata una disciplina in materia di archivi di DNA particolarmente garantista.

L'attenzione rivolta dal Governo francese è visibile già dall'intervento effettuato nel 1994, da parte del Parlamento nazionale, emanando una legge specifica sul rispetto dell'integrità nel prelievo del DNA. Questa normativa ha portato alla conseguenza che in Francia, prima di procedere al prelievo di un campione genetico, si rende necessario acquisire il consenso dell'interessato, poiché il corpo umano è considerato inviolabile in modo assoluto. Tuttavia, il rifiuto di sottoporsi al prelievo può essere utilizzato contro la persona sospettata.

In conseguenza di questa disciplina, la banca dati del DNA francese ha una dimensione molto limitata e contiene un numero esiguo di profili, cioè solo quelli riferiti alle persone condannate.

Questa banca dati è stata istituita con la legge 98-468 del 17 giugno 1998, con la quale è stato introdotto nel codice di procedura penale francese l'art. 706-54.

L'archivio genetico francese è comunque effettivamente operativo non da molto, a causa degli ostacoli incontrati sulla strada della sua realizzazione [422].

In Italia, l'istituzione di una banca dati del DNA è molto recente, nonostante il Comitato nazionale per le biotecnologie e la biosicurezza avesse già approvato un progetto il 14 aprile 2005, elaborando anche una serie di regole sulla categoria dei campioni, i soggetti su cui compiere prelievi, le modalità di raccolta, conservazione, archiviazione e cancellazione.

Da questa esperienza era scaturito anche uno schema di disegno di legge che non è mai stato approvato dal Consiglio dei ministri.

Un ulteriore progetto di legge è stato presentato un anno più tardi, il 18 maggio 2008, apportando delle modifiche a quello precedente, anche in base alle direttive impartite dal Garante della Privacy, ma nemmeno questo testo si è mai tradotto in norma per la fine anticipata della XV legislatura [423].

Solo con la legge 30 giugno 2009, n. 85, è stata finalmente istituita la banca dati nazionale del DNA. In adempimento agli obblighi internazionali, questa norma munisce le forze di polizia di uno strumento investigativo ormai divenuto necessario.

La banca dati del DNA è istituita presso il Ministero dell'Interno, per facilitare l'identificazione degli autori del delitto.

L'accesso ai dati è consentito alla polizia giudiziaria e all'autorità giudiziaria solo per i fini di identificazione personale e per la collaborazione internazionale di polizia.

Questo *database* provvede a raccogliere i profili di DNA dei soggetti sottoposti a misure restrittive della libertà, di quelli relativi a reperti biologici acquisiti nel corso di un procedimento penale, per le persone scomparse o loro consanguinei, di cadaveri e resti cadaverici non identificati. È inoltre possibile procedere al confronto dei vari profili di DNA per i fini di identificazione.

I dati devono essere cancellati e i campioni genetici devono essere distrutti a seguito di sentenza di assoluzione o quando siano state violate le norme sulle procedure di raccolta e archiviazione [424].

Un'iniziativa belga del 2004 ha previsto l'istituzione del sistema europeo di informazione sui casellari giudiziari (ECRIS), inteso a impedire ai condannati per reati a sfondo sessuale di svolgere lavori a contatto con minori in altri Stati membri [425].

---

[422] Si veda, sul punto, la discussione generata a livello governativo in www.assemblee-nationale.fr (sito consultato in data 20 aprile 2009).

[423] Sul punto si veda la relazione dell'On. Manlio Contento, Commissione Riunite II e III – Resoconto di martedì 10 febbraio 2009, sul sito internet www.camera.it (consultato in data 23 gennaio 2010).

[424] Per un approfondimento sulle banche dati nazionali del DNA si rinvia a C. FANUELE, *op.cit.*, pagg. 200 e ss.

[425] Il sistema ECRIS ha sostituito l'ormai inefficace modello di assistenza giudiziaria in materia penale, basato sulla Convenzione del Consiglio d'Europa per scambiarsi informazioni sulle condanne

Nel 2006 e 2007 la Commissione europea ha presentato un pacchetto di riforma, composto da tre strumenti fondamentali: la decisione quadro 2008/675/GAI del Consiglio europeo che impone agli Stati membri di prendere in considerazione le precedenti decisioni di condanna in occasione di un nuovo procedimento penale (cd. principio di *ne bis in idem* europeo); la decisione quadro 2009/315/GAI del Consiglio europeo relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario; la decisione 2009/316/GAI del Consiglio europeo che istituisce ECRIS quale strumento tecnico per lo scambio di informazioni estratte dal casellario giudiziario.

La piena attuazione del sistema d'informazione è prevista per il 2012 ma già attualmente è in corso un progetto pilota cui partecipano quindici Stati membri, nove dei quali hanno iniziato lo scambio elettronico di informazioni estratte dai casellari giudiziari.

Secondo il *considerandum* 1 della decisione quadro 2009/315/GAI, l'Unione europea si è prefissa l'obiettivo di fornire ai cittadini un livello elevato di sicurezza in uno spazio di libertà, sicurezza e giustizia. Tale obiettivo presuppone lo scambio di informazioni estratte dal casellario giudiziario tra le competenti autorità degli Stati membri.

La decisione prevede un *minimum* di informazioni che devono essere fornite: le informazioni relative alle persone condannate (nome completo, data di nascita, luogo di nascita completo di città e Stato, sesso, cittadinanza ed eventuali nomi precedenti); informazioni relative alla natura della condanna (data della condanna, nome dell'organo giurisdizionale, data in cui la decisione è diventata definitiva); informazioni relative al reato che ha determinato la condanna e informazioni relative al contenuto della condanna. Inoltre, se iscritte nel casellario giudiziario, devono essere trasmesse anche le informazioni sul nome dei genitori del condannato, sul numero di riferimento della condanna, luogo del reato e interdizioni derivanti dalla condanna. Se l'autorità ne ha la disponibilità, devono essere trasmesse anche le impronte digitali, eventuali pseudonimi e i numeri dei documenti identificativi.

La decisione 2009/316/GAI è diretta a definire le modalità di trasmissione tra Stati membri delle informazioni riguardanti le nuove condanne allo o agli Stati membri di cittadinanza del condannato, a definire gli obblighi di conservazione e a fissare un quadro sistematico per lo scambio delle informazioni.

---

pronunciate a livello nazionale (Convenzione del 20 aprile 1959). Il Consiglio europeo ha mosso un primo passo per una riforma adottando la decisione 2005/876/GAI che imponeva agli Stati membri di designare un'autorità centrale incaricata di trasmettere periodicamente agli altri Stati membri le condanne pronunciate nei confronti dei loro cittadini (la menzionata decisione è stata pubblicata in Gazzetta Ufficiale CE, L 322 del 9 dicembre 2005).

ECRIS è un sistema d'informazione decentrato che interconnette le banche dati dei casellari giudiziari degli Stati membri tramite la rete s-TESTA della Commissione europea.

I dati sono cifrati e strutturati in base a un formato predeterminato e comprendono i dati anagrafici, le condanna, la pena, il reato e le ulteriori informazioni, tra cui le impronte digitali, se disponibili.

I dati personali trasmessi ai fini di un procedimento penale potranno essere usati solo per questa finalità e per ogni diverso uso sarà necessario il consenso dello Stato che li ha trasmessi.

Non è prevista alcuna disposizione sulla conservazione dei dati, in quanto in materia è lasciata piena sovranità legislativa agli Stati [426].

Il sistema informativo ECRIS è dotato di una banca dati di indice delle informazioni contenuti, denominata EPRIS.

Obiettivo della decisione ECRIS è dare attuazione alla decisione quadro 2009/315/GAI, per costruire e sviluppare un sistema informatizzato di scambio di dati tra Stati membri sulle condanne, in un modo facilmente comprensibile.

La decisione non si prefigge di armonizzare i sistemi nazionali di casellario giudiziario e, pertanto, non obbliga lo Stato membro di condanna a modificare il suo sistema interno di casellario giudiziario per quanto at-tiene all'uso delle informazioni per scopi interni.

La predisposizione di tavole di riferimento delle categorie di reato e delle categorie di pene e misure di cui alla presente decisione dovrebbero facilitare, mediante un sistema di codici, la traduzione automatica e la reciproca comprensione delle informazioni trasmesse.

Per garantire il funzionamento efficiente di ECRIS, la Commissione offre un supporto generale e un'assistenza tecnica, comprese la raccolta e l'elaborazione delle statistiche.

Il sistema informativo è composto da un *software* di interconnessione conforme a un pacchetto comune di protocolli per lo scambio di informazioni fra le banche dati di casellari giudiziari degli Stati membri e un'infrastruttura di comunicazione comune che forma una rete cifrata.

Si è già avuto modo di sottolineare[427] che alcune tra le principali banche dati dell'Unione europea sono caratterizzate da una gestione centralizzata che si sostanzia in un archivio centrale europeo ed una diramazione a raggiera di tanti punti di contatto e archivi nazionali, quanti sono gli Stati aderenti.

[426] A partire dal 2016 la Commissione europea è obbligata a pubblicare delle relazioni periodiche sul funzionamento di ECRIS.

[427] Il riferimento è ai paragrafi 8 e 8.1 di questo capitolo.

Questo rilievo vale, in particolare, con riferimento alle banche dati di Eurojust, di Europol, il Sistema Informativo Schengen (SIS e SIS II) e il Sistema Informativo Doganale (SID)[428].

[428] Quanto a queste ultime due banche di dati menzionate, sono denominati N-SIS e N-SID i corrispettivi nazionali del SIS e del SID comunitari.

CAPITOLO SECONDO

SEZIONE III

La prova digitale, i diritti della persona e le esigenze di giustizia e di sicurezza interna ed esterna

SOMMARIO : 9. Prova digitale e diritto ad un equo processo: il profilo dell'acquisizione della prova, del diritto al contraddittorio e della valutazione - 10. Prova digitale e diritto alla difesa dell'indagato - 11. Prova digitale ed diritto alla privacy del terzo e dell'imputato

9. Prova digitale e diritto ad un equo processo: il profilo dell'acquisizione della prova, del diritto al contraddittorio e della valutazione

L'adesione dell'Unione europea alla Convenzione europea dei diritti dell'Uomo[429], obbliga l'ordinamento comunitario e gli ordinamenti nazionali ad uno sforzo riformistico, laddove necessario, per adeguare la legislazione agli impegni assunti. Il nuovo sistema di tutela richiede di analizzare ed attuare anche il diritto derivato dalla funzione di *lawmaker* della Corte di Strasburgo[430].

In questo contesto di riferimento, l'art. 6 CEDU detiene un ruolo di particolare importanza per la materia processuale penale, poiché concentra in un'unica disposizione una pluralità di contenuti che si riverberano trasversalmente sull'intero procedimento, anche in materia di prova penale (e, per quanto qui d'interesse, sulla prova penale digitale) [431].

La nozione di giusto processo evoca, fra le altre, anche il discusso problema relativo alle prove ottenute illecitamente e alle prove raccolte in maniera illegale[432].

---

[429] Per un approfondimento sull'argomento si rinvia al capitolo I paragrafo 2.

[430] Così B. PIATTOLI *Mandato di arresto europeo: istanze di armonizzazione processuale, distonie applicative e tutela multilivello dei diritti fondamentali* in *Diritto penale e processo*, 2007, 8, pag. 1108.

[431] Vedi nota 1.

[432] Si è già ampiamente trattato del problema della buona pratica nell'acquisizione della prova digitale e del tema della genuinità della prova. Si rinvia, sul tema, al capitolo secondo.

A sostegno di questo rilievo, ma con un ragionamento a contrario, nella sentenza *Schenk contro Svizzera* della Corte Europea dei Diritti dell'Uomo[433], i giudici di Strasburgo negano, da un lato, che in via di principio ed in astratto si debba sempre escludere dal processo una prova raccolta in maniera illegale, ma, dall'altro lato, ritengono l'accertamento dei fatti globalmente corretto a livello procedurale, in una simile condizione, purché corroborato da altro e diverso materiale probatorio "genuino" e solo nell'ipotesi in cui si ha motivo legittimo e valido di ritenere che non si sarebbe verificata comunque una contestazione immediata, da parte dell'accusato, sulle risultanze e sull'utilizzabilità della prova[434].

Per ovviare a questo problema è stata introdotta la decisione quadro sul mandato europeo di ricerca della prova, la cui applicazione, pur essendo stato raggiunto ormai da tempo l'accordo politico per la sua adozione, stenta a prendere corpo[435].

Anche l'art. 82, paragrafo 2, TFUE fornisce un valido sprono verso la previsione di regole comuni sulla prova penale nello spazio giudiziario UE, in particolare laddove é contemplata la possibilità di adottare direttive che contengano norme minime in tema di ammissibilità reciproca della prova tra gli Stati membri e su altri temi affini alla procedura penale, da individuarsi a cura del Consiglio, in via preliminare, mediante una decisione.

In un auspicabile sistema di mutuo riconoscimento tra gli Stati membri della prova penale e della prova digitale in particolare, è prioritario agevolarne la circolazione, ma è anche necessario che l'elemento probatorio raccolto,

---

Sulla simmetria tra la nozione di giusto processo e la nozione di prove illecite, si rinvia a M. CHIAVARIO voce *giusto processo* in *Enciclopedia giuridica Treccani*, Edizione Tipografica Treccani, 2001, pag. 8.

[433] La sentenza è stata emessa dalla Corte in data 12 luglio 1988.

[434] Una problematica affine è stata trattata recentemente dal Giudice presso il Tribunale di Vigevano, nel noto caso dell'omicidio di Garlasco, balzato a lungo agli onori della cronaca giudiziaria italiana e straniera. Nella sentenza conclusiva del processo di I grado, il Giudice ha molto laconicamente motivato in ordine alla sua valutazione positiva del contenuto dei dati informatici acquisiti, ritenendoli pienamente utilizzabili ai fini del giudizio. L'organo giudicante, ci si permette di osservare, ha erroneamente misconosciuto le conseguenze negative che si possono essere riversate anche sui dati rimasti (forse!) integri e genuini all'esito di un intervento di *computer forensics*, contestabile dal punto di vista scientifico e operativo.
Per un approfondimento si rinvia, volendo, a E. COLOMBO *La sentenza del caso di Garlasco e la computer forensics: analisi di un complesso rapporto tra diritto ed informatica* in *Ciberspazio e diritto*, 3, 2010.

[435] Sul tema si veda S. ALLEGREZZA *L'armonizzazione della prova penale alla luce del Trattato di Lisbona* in *Cassazione penale*, 10, 2008, pagg. 2000 ss; J.A.E. VERVAELE *European Evidence Warrant*, Intersentia, 2005, in particolare nella parte in cui l'Autore riporta i lavori preparatori della proposta di decisione quadro sul mandato europeo di ricerca della prova; R. BELFIORE *Il mandato europeo di ricerca della prova e l'assistenza giudiziaria nell'Unione europea*, in *Cassazione penale*, 2008, 10, pagg. 2804 ss.

acquisito e valutato rispetti e garantisca il principio del giusto processo, nella sua interezza di contenuti.

L'aspetto della qualità della prova raccolta è funzionale al raggiungimento di questo obiettivo e permette, anche nella prosecuzione del processo, di contare su di un altissimo profilo scientifico e di affidabilità del materiale probatorio.

Lo studio e la formazione specialistica, il coinvolgimento di soggetti esperti e di chiara fama nella comunità scientifica, sono tutti elementi che permettono di depurare il processo da errori, suggestioni e prove pseudo-scientifiche che ne possono inquinare lo svolgimento e l'esito [436].

Solo in questo modo la prova scientifica può rappresentare un vero ausilio nella ricerca del fatto e nel giudizio di valore, raggiungendo il risultato di un processo giusto che faccia emergere una verità quanto più vicina a quella fattuale.

Per quanto attiene, in particolare, alla prova digitale, spesso l'esigenza di contesti garantiti di formazione dell'elemento probatorio si scontrano con le circostanze contingenti oggettive e soggettive. Non sempre le autorità intervenute sulla scena del crimine sono dotate di un potenziale tecnico e conoscitivo adeguato, in grado di raccogliere una prova digitale secondo gli standard scientifici più elevati che ne garantiscono la genuinità; non sempre si ha tempo necessario e la possibilità di acquisire le autorizzazioni degli organi giurisdizionali, quando rischio.

Il rischio insito nel trascorrere del tempo è quello che i dati informatici, caratterizzati dalla volatilità, possano essere persi, distrutti o modificati in assenza di un intervento immediato delle autorità investigative.

Le esigenze della giustizia, dunque, spesso si scontrano con le esigenze di tutela dei diritti fondamentali dell'accusato o dell'indagato ad un equo processo, basato su elementi probatori genuini e attendibili [437].

La realtà giuridica contemporanea dimostra però che. molto spesso, la prova informatica rappresenta un valido supporto per il fine di giustizia, seppure è altrettanto vero che difficilmente è da sola determinante per la decisione finale del processo, nel senso di una condanna o di un'assoluzione dell'accusato.

La prova digitale, con l'insieme degli apparati di supporto infrastrutturali, persegue un altro fine insito nell'ampia nozione di giusto

[436] In questi termini si veda M. PINO, M. D'ALOIA La prova scientifica nel processo penale: il requisito della formazione, in La prova scientifica nel processo penale, a cura di L. DE CATALDO NEUBURGER, Cedam, 2007, pagg. 104 ss.

[437] Il problema del bilanciamento delle opposte esigenze nella raccolta ed acquisizione della e-evidence è stato più volte evidenziato dai relatori presenti in occasione del convegno organizzato dall'ERA a Barcellona il 26-27 maggio 2011 – convegno già citato in precedenza.

processo, cioè permette una significativa riduzione del tempo necessario per le indagini.

La ragionevole durata del processo, infatti, è uno degli obiettivi primari a cui deve mira ogni autorità giurisdizionale, anche spronato dalle esortazioni della Corte di Strasburgo, per attuare un vero *fair trial*[438].

La speditezza procedurale è un obiettivo comune anche ai procedimenti per crimini transnazionale, per la cui prevenzione e repressione è necessaria una stretta collaborazione tra le autorità investigative di diversi Stati membri, in ragione della complessità delle indagini. La prova digitale può rispondere a questa logica di compressione delle tempistiche procedurali, in particolare se ne viene agevolata la rapida circolazione e nei casi in cui sono raccolti i dati in tempo reale[439], così declinando tutte le esigenze di giustizia.

La tutela del giusto processo non può prescindere dall'autenticità degli elementi probatori assunti e, prima ancora, dal riconoscimento di ciò che può essere prova digitale e ciò che non lo è.

La raccolta della *e-evidence* deve seguire dei passaggi obbligati che ne assicurino la genuinità, i quali si possono riconoscere nell'identificazione degli elementi probatori, nella loro preservazione e validazione, nella procedura di garanzia della catena di custodia, nella tutela della sicurezza e nella protezione dei contenuti acquisiti.

Come si è già avuto modo di accennare, la tendenza degli organi giudicanti è spesso quella di ammettere una prova elettronica, anche quando non vi è certezza sull'*iter* procedurale seguito per la raccolta e sulle *best practices* utilizzate[440], motivando sul fatto che, in sede valutativa, non ha costituito prova fondamentale ai fini della decisione[441].

Ciononostante, questa forzatura del sistema che si verifica nel diritto applicato, non può essere incoraggiata perché è contraria alle regole procedurali di sistema e perché mina alla garanzia del diritto al *fair trial*.

L'utilizzo di *best practices,* che rappresentano il meglio dello stato dell'arte informatica, permette di testare i risultati ottenuti anche in un momento

[438] Così M. GERCKE nell'intervento fatto al seminario di studi menzionato nella precedente nota.

[439] Su questa particolare opportunità d'indagine che permette la raccolta simultanea di dati, in particolare delle intercettazioni telematiche, si rinvia alla lettura del testo della Convenzione di Budapest sul *cybercrime* ove si trova traccia espressa di questa previsione ancora poco attuata. Le difficoltà di realizzazione nascono principalmente per l'assenza di personale ed infrastrutture idonee ed anche a causa degli ostacoli frapposti dai più garantisti, i quali vedono in questa attività investigativa una minaccia alle libertà fondamentali dell'individuo.

[440] Si ricorda che, allo stato, non esistono delle regole di computer forensics vincolanti e comuni per tutti gli organi procedenti e per tutti gli Stati dell'Unione Europea.

[441] Per un approfondimento, si veda S. MASON *Electronic Evidence,* Butterworths, 2010.

successivo alla loro raccolta e, di conseguenza, di scongiurare i possibili dubbi di manipolazione dell'elemento probatorio[442].

Il diritto al contraddittorio sulla e per la prova è un ulteriore campo di applicazione della nozione ampia di giusto processo.

Va segnalato che il diritto al contraddittorio, come aspetto della più ampia nozione del diritto ad un equo processo previsto dall'art. 6 CEDU, richiede alle autorità giudiziarie di ciascuno Stato membro, in conformità alla Convenzione e all'interpretazione della Corte di Strasburgo, richiede che ogni documento e parere sia reso conoscibile alla parte affinché, anche su di essi, possa essere esercitato il diritto di difesa in condizione di parità tra le parti [443].

La prova digitale è, per lo più, una prova pre-costituita al processo, raccolta in fase di indagini, che transita nel procedimento in base ad un mero controllo di legittimità (che, come visto, troppo spesso trascende da un vaglio di autenticità), senza una garanzia piena del diritto delle parti al contraddittorio per e sulla prova, cioè privando dell'intervento interlocutorio di tutte le parti coinvolte nella fase iniziale di raccolta, aspetto questo funzionale al giusto processo.

Il confronto ed il controllo sul materiale che accede al processo e forma oggetto di valutazione per l'organo giudicante, coadiuva il raggiungimento del fine di verità processuale che trascende da elementi corrotti e non autentici e, contestualmente, integra il principio di parità delle armi previsto dall'art. 6 CEDU.

Nel caso in cui la prova digitale è raccolta in violazione di altri diritti dell'individuo - quale il diritto alla *privacy* -, deve essere garantita la possibilità al soggetto interessato di sollevare (eventualmente) una contestazione in

---

[442] *Ibidem*. L'Autore del menzionato testo, in occasione di un intervento al seminario di studi organizzato da ERA a Barcellona il 26-27 maggio 2011, sul tema della *e-evidence* ha tenuto precisare che l'applicazione di *best practices* è essenziale per garantire l'autenticità della prova digitale. D'altro lato è necessario considerare che la tecnologia, specie in campo informatico, è in continuo sviluppo e, di conseguenza, sono richieste delle continue revisioni alle linee guide, per fare fronte alle mutate esigenze dello sviluppo della scienza. Nel processo, in sede di ammissione e poi di valutazione della prova, si deve, dunque, considerare la migliore pratica applicabile al momento della raccolta dell'elemento probatorio.

[443] L'interpretazione dell'art. 6 CEDU in relazione alla garanzia del diritto al contraddittorio, è riportata, per conformità, nella sentenza della Corte di Cassazione italiana del caso Cucinotta (Sez. V, 14 giugno 2007, n. 31132, Cucinotta, rv. 237600).

La Corte di Legittimità ha cassato la decisione con cui il giudice di appello aveva dichiarato l'inammissibilità della richiesta di revisione omettendo di comunicare all'interessato il parere del P.G., in quanto – ancorché nella fase preliminare di ammissibilità della richiesta sia legittima l'adozione di una procedura non partecipata e nonostante l'art. 634 c.p.p. non preveda che in tale fase sia sentito il P.G. – ove sussistano le conclusioni del rappresentante dell'Ufficio del P.M., esse devono essere comunicate e, pertanto, conoscibili dalla controparte.

merito, per agevolare il dialogo tra le parti, al fine di un vaglio coerente di ammissibilità e utilizzabilità[444].

Si dissente dalle pratiche di aggiramento del diritto al contraddittorio per e sulla prova digitale, in quanto prova pre-costituita, e dalla tendenza ad ammettere al processo questo elemento probatorio, per vie traverse, mediante l'escussione del personale intervenuto in fase di indagini. In questo modo, infatti anche qualora si decida per la non ammissibilità della prova elettronica per difetto di genuinità, il contenuto di essa filtra ugualmente nel fascicolo processuale e viene, così, a costituire oggetto di valutazione in sede decisionale[445].

Il contraddittorio per la prova, invece, permette almeno un confronto aperto tra le parti sui criteri di affidabilità, una verifica sul metodo e sul grado di falsificabilità e un confronto con le regole proprie della comunità scientifica, per conoscere il tasso di errore e di comune accettazione di esso[446].

Per realizzare un vero contraddittorio di tipo tecnico è necessario che l'interessato (indagato o imputato) possa valersi, qualora lo ritenga opportuno, di un esperto di sua fiducia, in grado di confrontarsi con la prova in maniera scientifica[447]. La previsione formale di questa facoltà non è sintomatica della sua effettività poiché l'intervento di un tecnico obbliga ad un impegno economico rilevante che non tutti possono permettersi[448]

---

[444] Sul rapporto tra prova digitale e diritto alla privacy si dirà più approfonditamente nel prosieguo del capitolo.

[445] È vero che, durante l'escussione del teste o del perito o del consulente tecnico, ogni parte ha diritto di interagire in condizione di parità ma, ad ogni buon conto, il contraddittorio è limitato al solo contenuto di quanto espresso, ovviando alle regole di esclusione della prova.

[446] In questi termini P. TONINI *Progresso tecnologico, prova scientifica e contraddittorio* in L. DE CATALDO NEUBURGER *op.cit.,* pag. 49 ss.

[447] Il *curriculum* formativo e specialistico del tecnico è uno degli elementi che anche l'organo giudicante tiene in debita considerazione, allorquando si trova a dover valutare – e giudicare – le diverse posizioni espresse da più esperti su una stessa *res probans*.
Appare doveroso puntualizzare che non esistono molti percorsi formativi in materia di *computer forensics*, specie in Italia. dove si stanno evolvendo solo negli ultimi anni alcuni *curriculum* specialistici. Diversamente, negli Stati Uniti d'America la cultura in materia è molto più radicata e specializzata.
Nel corso del convegno di studi svolto a Cagliari il 17-18 giugno 2011 dal titolo "*Crime Scene Investigation: investigazioni sulla scena del crimine*", molti intervenuti hanno segnalato, sulla base di esperienza personale, che spesso il nome del tecnico e la fama acquisita nella comunità scientifica di appartenenza, costituiscono proprio il punto centrale per la formazione del convincimento del giudice conformemente a questo esperto. Ci si limita semplicemente a riportare questa segnalazione emersa, senza sviluppare alcun approfondimento e senza esprimere alcun giudizio di valutare, lasciando l'interrogativo aperto se questa é una realtà davvero estesa e radicata nel territorio italiano e presente anche all'estero.

[448] Questa considerazione che, a prima vista, può apparire molto banale, richiama tutto il dibattito ancora acceso in Italia in relazione all'effettività della parità delle armi tra accusa e difesa e della reale applicazione delle regole sulle indagini difensive. Ci si limita a ricordare che uno dei problemi sollevati riguarda proprio lo scarso utilizzo delle facoltà investigative del difensore per impossibilità dell'indagato/imputato di sopportarne il peso economico.

L'articolato intreccio delle trame che compongono il diritto al contraddittorio si sostanzia anche nel diritto alla traduzione e interpretazione nel processo penale, in particolare con riferimento agli articoli 5.2 e 6.3 della CEDU e all'interpretazione che di essi è fornita dalla Corte. L'importanza di questa attività e la necessità della sua garanzia è ribadita nella direttiva 64/2010, segnatamente agli articoli 2 e 3, laddove è tutelato il diritto dell'interessato alla traduzione scritta almeno dei documenti fondamentali, in un tempo ragionevole. L'individuazione del catalogo dei "documenti fondamentali" è lasciato alla libera discrezionalità degli Stati membri, nei limiti della tutela di un processo equo. Esiste una regola di chiusura che permette di richiedere la traduzione anche di atti che non sono considerati fondamentali, quando è fornita una motivazione ragionevole[449].

Il contraddittorio di cui trattasi non si deve esaurire in un confronto tra esperti informatici ma deve svilupparsi anche mediante un dialogo tra le parti (accusa e difesa) e pertanto, come garantito dall'art. 6, paragrafo 3, CEDU, ciascun individuo ha diritto all'assistenza legale.

In questo scenario irrompe la contrapposizione tra sovranità ed esigenze di giustizia, da una parte, e prerogative individuali, dall'altra [450].

Nel più ampio contesto della creazione di uno spazio di libertà, sicurezza e giustizia, la tensione verso un giusto processo europeo, specie quando si procede per crimini transnazionali, dipende anche dall'effettività del mutuo riconoscimento delle prove digitali (e della prova penale in generale) tra gli Stati membri. La realizzazione di questo principio non può prescindere dalla reciproca fiducia nella legalità dei singoli ordinamenti giuridici e dalla previsione di norme minime comuni in materia di prova penale. L'affermazione del principio dell'ammissibilità vicendevole della prova nello spazio giudiziario UE se legalmente raccolta in uno Stato membro, è espressa in nuce già nella dichiarazione conclusiva del Consiglio di Tampere del 1999, nel Libro verde sulla tutela penale degli interessi finanziari comunitari e sulla

---

Per un approfondimento sul tema si rinvia, *ex multis,* a A. DI MAIO *Le indagini difensive: dal diritto di difesa al diritto di difendersi provando*, Cedam, 2001; P. VENTURA *Le indagini difensive*, Giuffré, 2005.

[449] Sul punto si rinvia a T. SPRONKEN – G. VERMEULEN – D. DE VOCHT – L. VAN PUYENBROECK *EU Procedural Rights in Criminal Proceedings*, Maklu, 2009, pagg. 34-37.
Un problema correlato attiene al grado qualitativo della traduzione che, specie se riguarda delle lingue poco comuni, richiede delle conoscenze che trascendono le normali attitudini richieste ad un traduttore. Per questo, l'auspicio è che a breve in europea si sviluppi un percorso formativo *ad hoc.* che permetta di raggiungere l'accreditamento per le traduzioni giuridiche di diritto comunitario soltanto a professionisti scelti e accuratamente selezionati, i quali possano dimostrare di aver sviluppato delle conoscenze e delle attitudini specializzanti.

[450] L'esistenza di questa tensione che trova la sua massima espressione nella ricerca di sviluppo delle procedure di cooperazione è bene sottolineata da N. PARISI op.cit., pag. 448.

creazione di una procura europea del 2001[451] e indirettamente accolta anche nella decisione quadro sul mandato europeo di ricerca della prova[452].

La valorizzazione della prova digitale, per come raccolta e poi acquisita al processo, dipende dalla valutazione che ne fa il giudice.

L'organo giudicante, in un giusto processo, è terzo ed imparziale e soggetto soltanto alla legge. Pertanto, anche rispetto alla prova digitale, da ammettere o già ammessa, è il giudice l'unico soggetto atto alla razionalizzazione degli avvenimenti e dei contenuti, verso l'obiettivo della giustizia.

La giurisdizione si deve attuare per mezzo di un organo giusto, che motivi le sue decisioni e che dia atto di un processo svoltosi secondo equità, contemperando gli interessi dell'accusato con quelli dell'amministrazione della giustizia[453].

Si è, infatti, superato da tempo l'orientamento che ammetteva l'esistenza di una scienza esatta, le cui risultanze oggettive non potevano essere confutate e nemmeno essere liberamente valutate dal giudice, poiché portatrici di una verità assoluta[454].

L'organo giudicante, contrariamente, è oggi chiamato a rapportarsi in maniera critica anche rispetto alla prova scientifica in generale e, quindi, alla prova digitale, esaminando i risultati acquisiti secondo un ragionamento abduttivo[455] di filtro e di interpretazione del contenuto probatorio.

L'esame valutativo comprende l'accertamento della validità della prova e della tecnica scientifica utilizzata nella sua raccolta, quali elementi che fondano un processo di validazione del contenuto. In particolare, ciò che preliminarmente interessa il giudice, per il fine di un giusto processo, è il controllo sull'adozione del metodo scientifico più adatto e più evoluto e il rispetto delle leggi scientifiche che lo regolano, nonché il controllo sulla metodologia procedurale seguita.

In caso di dubbia l'affidabilità della prova digitale, ovvie ragioni di giustizia consiglierebbero un apprezzamento prudente dei contenuti in fase di valutazione e di decisione, attraverso un ragionamento coerente e logico[456].

---

[451] Libro verde presentato dalla Commissione in data 11 dicembre 2001, COM(2001) 715 definitivo.

[452] *Ibidem*.

Il Consiglio di Tampere si è tenuto il 15-16 ottobre 1999: per approfondimenti sui contenuti si veda Cass.pen., 2000, pag. 302 ss; il Libro verde sulla Procura europea è COM(2010) 715 del 11 dicembre 2001. La decisione quadro MER è 2008/978/GAI.

[453] Cfr M. CHIAVARIO op.cit.

[454] Il testo di riferimento per un primo ragionamento illuminante sul rapporto tra scienza e diritto, è rappresentato da F. STELLA *Giustizia e modernità,* Giuffré, 2003.

[455] Sulla nozione di abduzione, si veda P. TONINI *Manuale di procedura penale*, Giuffrè, 2005.

[456]Sulla valutazione della prova scientifica, si veda P. TONINI *op.cit*.; G. DAQUI *La prova scientifica e lo spazio del libero convincimento* in L. DE CATALDO NEUBURGER *op.cit*., pag. 70 ss.

Nella prassi del diritto vivente, molto spesso si assiste a procedimenti penali che si concludono con sentenze dettate più dall'intimo convincimento dell'organo giudicante che dalla certezza della prova. Questo certamente stride con la garanzia di un *fair trial*, come invece auspicato in ambito comunitario ed internazionale.

Indipendentemente dalle categorie di prove a disposizione del giudice, non sarà mai possibile raggiungere in un processo l'utopica conoscenza della verità assoluta, ma è necessario fare i conti con il concetto di verità giudiziale, distinto da quello di verità materiale.

Se, dunque, la giustizia penale è una giustizia imperfetta, almeno il momento valutativo delle prove deve essere circondato dalle maggiori garanzie di accuratezza e di attendibilità, affinché il giudizio di diritto non si allontani oltremodo da un giudizio "giusto", il più possibile prossimo alla verità fattuale[457].

10 Prova digitale e diritto alla difesa dell'indagato

Nell'ampia nozione del diritto ad un equo processo, come enucleato nell'art. 6 della Convenzione Europea dei Diritti dell'Uomo e come interpretato nella giurisprudenza della Corte, vi rientra anche il multiforme concetto del diritto alla difesa dell'indagato.

Il soggetto accusato di un reato, messo di fronte ad una prova digitale, deve potersi difendere personalmente o a mezzo di un proprio difensore.

In primo luogo, come in ogni altra circostanza, anche rispetto a questo tema è necessario considerare le differenze di garanzia del diritto alla difesa previste in ogni Stato membro. In alcuni casi, infatti, si rileva un livello di tutela non sufficiente se parametrato a quanto previsto dalla legislazione comunitaria a cui ciascuno Stato membro è obbligato ad adeguarsi[458].

La comprensione effettiva delle accuse mosse a carico dell'indagato è una condizione essenziale alla piena realizzazione del diritto di difesa ed alla scelta consapevole e meditata della linea difensiva da seguire da parte del predetto e del suo difensore.

La CEDU è molto chiara nell'indicazione degli elementi che devono essere resi noti e dettagliati alla parte interessata: natura e motivi dell'accusa. Questi avvisi devono essere dati nel più breve tempo possibile.

La locuzione "nel più breve tempo possibile" è molto vaga e non pone un termine finale definito la cui determinazione, dunque, è lasciata alla libera discrezionalità del Legislatore nazionale. L'assenza dell'indicazione temporale

[457] Sul punto si invita alla lettura di AA.VV. *Prova scientifica e metodo scientifico*, Utet, 2009.
[458] Così B. PIATTOLI *op.cit.*, pag. 1110

precisa contiene in nuce l'eterna tensione tra l'interesse alla segretezza delle indagini (almeno per un certo tempo, in certe condizioni d'intervento e quando si procede per certe categorie di reati o nei confronti di certi soggetti) per i fini di giustizia e l'interesse della difesa ad un intervento tempestivo.

Il fattore temporale, infatti, tanto può essere un elemento a favore quanto un elemento contrario alla piena esplicazione del diritto alla difesa, specie nei casi in cui l'indagato si determini per estrinsecare il proprio diritto di difendersi provando[459]. Certe attività difensive, soprattutto gli accertamenti tecnici complessi, come quello informatico, che si eseguono su infrastrutture e dati in continuo mutamento, soggetti a sottrazione, furto, distruzione e modificazione con un semplice "click" richiedono una particolare attenzione ed un notevole dispendio di tempo.

Prima ancora di garantire la comprensione "tecnico-giuridica" delle accuse mosse, l'indagato deve essere messo nelle condizioni di capire la lingua usata nelle comunicazioni ufficiali, nei documenti e anche nei contenuti delle prove addotte.

Un'altra componente del diritto di difesa è rappresentata dal diritto ad una difesa tecnica o all'autodifesa.

Quando l'accusato si trova di fronte a una o plurime prove digitali poste a suo carico, la predisposizione di una valida difesa da questi elementi probatori dipende dalla possibilità di analizzarli e di addurre considerazioni *a contrario*, mostrando e dimostrando difetti, illegittimità e non autenticità dei contenuti. Tale operazione richiede l'intervento di un consulente esperto che sia messo nelle condizioni di confrontarsi con quei dati e di poterli esaminare con tutti i mezzi legittimi a sua disposizione, formulando osservazioni utili ai fini della difesa dell'accusato. Lo sfruttamento di queste facoltà difensive richiede anche la fruibilità di un tempo necessario per lo svolgimento dell'attività difensiva [460].

Il *vulnus* al diritto di difesa consiste non solo e non tanto nella previsione di attività di indagini difensive limitate, ma, quanto alla prova digitale, all'assenza di una disciplina legislativa che individui cos'è la *e-evidence*, quali sono i metodi da applicare per una genuina raccolta dei materiali probatori – almeno dal punto di vista dei principi generali -, come deve essere acquisita al processo, quali devono essere le regole base per la valutazione della prova e della sua autenticità.

Solo facendo chiarezza sulla disciplina e permettendo all'accusato e al suo difensore di avere contezza degli elementi di prova, sarà possibile per costoro difendersi in modo pieno e, possibilmente, in condizione di parità con l'accusa.

---

[459] Sul diritto di difendersi provando si rinvia a AA.VV. *Prova penale, op.cit.*, sez. I.

[460] Sulle garanzie del diritto alla difesa nel senso del diritto di disporre di tempi e strumenti difensivi adeguati, si rinvia a D.J. HARRIS – M. O'BOYLE – C. WARBRICK *Law of the European Conventionon Human Rights,* Preston Press, 1995.

Questo perché una buona difesa non si attua solo attraverso la produzione di contenuti e di altre prove *a contrario*, ma anche mediante la dimostrazione dell'illegittimità, della non autenticità e della non utilizzabilità della prova digitale raccolta dall'accusa[461].

Si consideri anche che la difesa ha già una posizione di svantaggio per il solo fatto che gli è riconosciuto un diritto limitato di accesso al dato originale (da intendersi come il primo dato raccolto) e, di conseguenza, il controllo sull'autenticità delle copie risulta essere un'operazione di particolare complessità[462].

Secondo Januus Tehver la tutela del diritto di difesa e, parallelamente, del rispetto della vita privata e familiare, richiederebbe una rivalutazione del binomio "accesso e copia" dei dati digitali, diverso dal binomio "ricerca e apprensione". Nei casi in cui i dati vengono recuperati *on-site* o *in remote* il legittimo proprietario non ne viene privato, ma semplicemente si procede ad effettuarne una copia, piuttosto che asportare il dato originale.

Inoltre, sarebbe necessario diversificare i poteri e le modalità do acquisizioni della prova digitale nelle ipotesi in cui i dati si trovano nella disponibilità del sospettato, rispetto ai casi in cui, invece, si trovano presso soggetti terzi, con cui non sussiste alcuna relazione rispetto al reato (quali gli Internet Service Provider o ISP, erogatori del servizio) [463].

Per garantire l'effettività del diritto di difesa, l'art. 6, paragrafo 3, CEDU prevede la possibilità di accesso all'istituto dell'assistenza legale gratuita, almeno parziale, in favore dei soggetti non abbienti[464].

Questa previsione di gratuità esiste in tutti gli Stati membri ma con considerevoli differenze. In alcune legislazioni nazionali non è previsto l'obbligo di informare la persona interessata del diritto all'assistenza gratuita; laddove l'obbligo sussiste, ciascuna norma interna prevede, però, degli scopi correlati differenti. Molti Paesi, inoltre, non sono in grado di fornire un *budget* finanziario congruo per permettere che questo diritto alla difesa gratuita sia effettivo.

---

[461] In questi termini si è espresso, tra le righe, G. BRAGHO' *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa* in *Diritto dell'Informazione e dell'Informatica*, 2005, pag. 517 ss.

[462] Queste considerazioni critiche, tra le altre, si condividono con l'intervento fatto al seminario di studi ERA del 26-27 maggio 2011, più volte citato, da J. TEHVER, chiamato proprio ad analizzare le esigenze ed i limiti della difesa di fronte alla prova digitale nel processo penale.

[463] *Ibidem.*

[464] Le considerazioni, che si riportano, sul diritto all'assistenza legale gratuita sono il frutto dei risultati di una ricerca voluta dalla Commissione europea nel 2005, al fine di monitorare il livello di salvaguardia dei diritti fondamentali procedurali nell'Unione europea. Il *report* finale dello studio è stato pubblicato in T. SPRONKEN – G. VERMEULEN – D. DE VOCHT – L. VAN PUYENBROECK *EU Procedural Rights in the Criminal Proceedings*, Maklu, 2009.

Nella maggior parte degli Stati non esiste un meccanismo di controllo sulla qualità dell'assistenza legale prestata in ipotesi di gratuità, mentre laddove questo accertamento esiste è anche particolarmente severo [465].

In base all'art. 6 CEDU ed all'interpretazione che ne è dato dalla Corte di Strasburgo, emerge chiaramente come il diritto di difesa meriti una valutazione "europeistica", alla luce degli istituti e degli organismi di diritto sovranazionale, perché dalla firma del Trattato di Maastricht del 1992 non si è accolto soltanto un cambiamento economico ma anche culturale, sociale e, perché no, giuridico.

In un futuro – ed auspicato – scenario europeo di reciproco riconoscimento delle prove acquisite in ciascuno Stato membro, parte della dottrina riconosce un *vulnus* al diritto di difesa ed al ruolo del difensore, in particolare per l'assenza – almeno allo stato - di criteri comuni e condivisi di raccolta e di acquisizione della prova penale in generale, e della prova digitale in particolare[466].

Il rapporto con la nuova Procura europea che si dovrebbe realizzare a breve, in osservanza all'art. 86 TFUE, necessiterà di riempire il diritto di difesa di un nuovo contenuto, specie per dettare parametri di principio sui rapporti con questo organo di indagine comunitario. Gli aumentati poteri di un organo investigativo europeo, infatti, si devono necessariamente riflettere in aumentate facoltà della difesa affinché, in un panorama di accresciuta criminalità transnazionale che richiede uno sforzo europeistico congiunto, il diritto di difesa non resti un "illustre sconosciuto". Il contrappunto al potere del PME si trova enunciato nel Libro Verde in materia, nella parte in cui si precisa che questo organo agisce nel rispetto dei diritti fondamentali, e in osservanza ai principi generali che regolano la fase preparatoria del processo, durante la quale la procura europea deve condurre tutte le indagine necessarie all'acclaramento della verità, raccogliendo qualsiasi elemento utile per istruire il caso, sia esso a carico o a favore dell'indagato [467].

---

[465] Il diritto all'assistenza legale, secondo la Commissione europea, è un tassello fondamentale tra i diritti procedurali di un soggetto anche solo indagato. Il contenuto di questo diritto è coperto da Trattati europei e internazionali e da Carte di diritti: l'ICCPR, la Dichiarazione Universale dei Diritti dell'Uomo, la Carta dei Diritti Fondamentali nell'Unione Europea (meglio nota come Carta di Nizza), la Carta Africana dei Diritti Umani e dei Diritti degli Individui e la Risoluzione delle Nazioni Unite sui principi cardine del ruolo degli avvocati del 1990.

[466] La questione in merito è stata sollevata da G. FRIGO in occasione dell'intervento effettuato al convegno UAE svoltosi a Como nel 2002 dal titolo *"Il libro verde: gli avvocati nello spazio di libertà e sicurezza dell'Unione europea"*.

[467] Nonostante si cerchi, da un punto di vista oggettivo, di valutare questo elemento come un valido contrappeso ai poteri dell'organo inquirente, nella pratica non sempre il PM agisce come organo di giustizia, ricercando veramente elementi a carico e discarico, pur essendone obbligato.
La prassi giuridica italiana (ci si limita a questa prospettiva per ragioni di opportunità e perché si possiede un'esperienza diretta) dimostra che, nonostante la previsione dell'art. 358 c.p.p., il pubblico ministero è incontrovertibilmente legato alla logica della ricerca di elementi utili per sostenere

La difesa, inoltre, sempre secondo il menzionato Libro Verde, mantiene il diritto di poter accedere al fascicolo della Procura Europea, restando salvi i principi del contraddittorio e la presunzione di non colpevolezza.

Il diritto di difesa deve essere analizzato, anche in relazione alla prova, nei suoi molteplici aspetti caratterizzanti. L'art. 47 della Carta europea dei diritti fondamentali del 2000, definisce il diritto di difesa come un diritto (o una facoltà) individuale di *farsi consigliare,* oltre che farsi difendere e rappresentare. Il riferimento è a quella che viene definita come *"informazione tecnica"*, in grado di rendere edotto l'interessato dei suoi diritti[468] e di poterlo indirizzare nella scelta più propizia, sia nella fase precedente al processo sia nella fase processuale[469].

Il soggetto interessato deve essere informato compiutamente riguardo tutte le informazioni che ha diritto ad avere, anche per potersi difendere in un contraddittorio pieno[470].

11 Prova digitale ed diritto alla privacy del terzo e dell'imputato

La protezione del diritto alla *privacy* di ogni cittadino, come descritta dall'art. 8 della Convenzione europea dei Diritti dell'Uomo[471], si scontra con le esigenze di giustizia, di prevenzione ed accertamento del reato e di applicazione di tutti i mezzi e le procedure utili a tale scopo, comprensivi della prova digitale.

Nella società contemporanea, dove la tecnologia è ormai di tutti e per tutto[472], dove i supporti e le infrastrutture informatico-telematiche proliferano in ogni ambiente, dove le *devices* sono molteplici e si generano milioni di dati digitali ogni giorno, si comprende che il grado di invasività della prova digitale

---

principalmente la sua posizione (e quindi la posizione di organo tipicamente d'accusa), curandosi poco di raccogliere elementi a favore del soggetto indagato.

[468] In questi termine e per un approfondimento, si veda L. P. COMOGLIO, *L'informazione difensiva nella cooperazione giudiziaria europea* in *Rivista di Diritto Processuale*, 3, 2006, pagg. 861-863.

[469] Per completezza, si ricorda che la nozione e l'effettiva garanzia del diritto alla difesa hanno interessato la Corte EDU (con consistenti riflessi sul processo italiano), anche in relazione al tema del processo *in absentia*. Dalla vicenda del caso Cat Berro, del caso Somogyi e del caso Ay sono derivate le condanne all'Italia per violazione dell'art. 6 CEDU, in considerazione del carattere di non equità di un processo svoltosi *in absentia* se "*non sia accertato in maniera in equivoca che egli ha rinunziato al suo diritto a comparire e a difendersi*". Per un approfondimento si rinvia a AA.VV. La *Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Giuffré, 2011, pagg. 508-520.

[470] Il riferimento è ancora al caso Cucinotta, pertanto si rinvia alla nota 15.

[471] Per un approfondimento sul diritto al rispetto della vita privata e familiare di cui all'art. 8 CEDU si rinvia al capitolo primo, paragrafo 6.

[472] Si parla spesso, in ambito comunitario, di democrazia della rete.

è molto forte perché, potenzialmente, permette di controllare molti aspetti del vivere quotidiano.

La *e-evidence* costituisce un supporto valido ed ormai imprescindibile per il procedimento penale[473], ma questo non deve portare ad un abuso della raccolta e dell'acquisizione al processo, perché esistono altre esigenze e altri diritti contrapposti che devono essere bilanciati caso per caso. La necessità di un attento contemperamento tra interessi differenti è ancora più forte quando i dati digitali che si vogliono apprendere si trovano archiviati non presso l'accusato ma presso soggetti terzi, siano essi persone giuridiche (*pensiamo agli Internet Service Provider*) o persone fisiche a cui si deve la massima protezione della riservatezza.

Come sottolineato da Joackim Eckert[474], la raccolta della prova digitale da parte degli investigatori può avvenire all'interno del territorio del proprio Stato oppure all'estero; può essere effettuata in un luogo di privata dimora, in un'industria, in una Banca, in un pubblico ufficio, in uno studio privato. Gli spazi di ricerca non si limitano a quelli fisici ma guardano anche luoghi "virtuali", quali la rete *internet* e i *social networks*[475].

In ragione della vastità dell'area d'intervento e della necessità di acquisire la prova informatica, è necessario garantire uno *standard* di protezione dei dati appresi che, ad oggi, presenta livelli differenti da Stato a Stato.

È necessario procedere con cautela e con i più ampi controlli in relazione alle attività di incrocio di dati informatici che possono generare un grave *vulnus* alla vita privata dell'individuo.

Il diritto alla *privacy* deve essere garantito anche allorquando, nelle operazioni investigative di apprensione di dati elettronici, si viene a contatto

---

[473] In un mondo digitalizzato dove la prova digitale impera, sembra anacronistico sentire, in occasione del convegno tenutosi a Cagliari – menzionato già in nota 17 di questo paragrafo - che non è necessario allarmarsi e preoccuparsi oltremodo di razionalizzare e disciplinare le modalità di raccolta e l'utilizzabilità di questo tipo di prova poiché vi sono realtà in cui è tanto poco diffusa e raramente acquisita al fascicolo dibattimentale

[474] Joackim Eckert è Giudice presso il Tribunale di Monaco, in Germania. Il riferimento è all'intervento tenuto da costui in occasione del seminario di studi di Barcellona del 2011, già citato

[475] *Facebook, Twitter, Badoo, LinkedIN , Google+* e molti altri social networks esistenti, rappresentano ormai un punto di incontro e di comunicazione tra soggetti lontani e vicini e anche tra professionisti.
Questi *ambient* rappresentano anche una fonte di informazioni e di prove per le autorità investigative, per orientare lo sviluppo delle indagini o per raccogliere prove spesso decisive ai fini del processo.
La cronaca giudiziaria ci riporta spesso dei casi in cui le immagini o le comunicazioni presenti sul profilo di un social network hanno aiutato alla risoluzione anche di omicidi.
Si veda, per esempio, il caso dell'omicidio avvenuto il 23 ottobre 2010 in Galles, quando un giovane ha ucciso la ex fidanzatina di soli quindici anni a sassate per una scommessa fatta con un amico di una colazione gratis. Il giovane assassino aveva riempito la bacheca del suo profilo nel *social network facebook* di strategie e piani per far uccidere la ragazzina, come buttarla giù da un dirupo o farle assumere una *overdose* di digitale purpurea (che aveva in effetti acquistato) per provocarle un blocco cardiaco.

con una moltitudine indiscriminata di dati che non riguardano i fatti per cui si procede e sui quali, dunque, deve essere mantenuto il massimo riserbo.

Le modalità utilizzate per la raccolta ed archiviazione delle prove digitali devono anch'esse essere idonee e funzionali alla protezione dei dati rispetto ad accessi indiscriminati, estrazione illegittima di copie e furti di informazioni[476].

Questa esigenza è attuata mediante la previsione di autodisciplina degli organismi di gestioni degli archivi e delle banche dati e la predisposizione di regole serrate sulle modalità d'accesso e di estrazione dei contenuti, affiancate da un Organismo di Controllo[477], il quale ha lo scopo precipuo di verificare le operazioni compiute, il numero di accessi, le eventuali illegittimità verificatesi.

I molteplici profili entro cui può realizzarsi una violazione del diritto alla riservatezza necessita di un intervento verticale a livello comunitario che possa arginare i possibili abusi da parte degli organi nazionali e possa soddisfare le esigenze di razionalità.

Appare significativo, a riguardo, la funzione di garanzia assunta dall'ordinamento comunitario, per esempio, nella disciplina delle cc.dd. intercettazioni per instradamento, contenuta nella Convenzione dell'Unione europea sull'assistenza giudiziaria in materia penale, che tende a moderare le spinte anarchiche e spesso poco garantiste da parte dei singoli Stati.

Questo obiettivo, che abbraccia la tutela del diritto alla riservatezza espresso nell'art. 8 CEDU, è postulato, in un altro contesto settoriale, anche nella decisione quadro sul mandato di arresto europeo, laddove si impone un adeguamento ai precetti della Convenzione europea[478].

L'art. 8 CEDU garantisce ad ogni persona il diritto al rispetto della vita privata e familiare, del domicili e della corrispondenza e precisa che "non può esservi ingerenza di un'autorità pubblica nell'esercizio di tale diritto" se non previsto da una legge e per motivi di necessità[479].

Questa disposizione deve fungere da punto di riferimento anche quando, per raccogliere una prova digitale, si accede al "*domicilio informatico*" di un soggetto e, contestualmente, si viene a contatto con dati ed informazioni che non riguardano la persona direttamente interessata ma un soggetto terzo, totalmente estraneo, rispetto al quale si deve garantire rigorosamente la *privacy* dei dati a lui riferibili.

---

[476] *Ibidem*

[477] Questo, per esempio, nel caso della banca dati di Europol.
Per un approfondimento sulle politiche di gestione e di garanzia della *privacy* da parte degli organismi comunitari e in relazione alle banche dati, si rinvia al Capitolo Secondo, sezione II.

[478] In questi termini, E.M. CATALANO *Molte incertezze e piccoli passi nel percorso di europeizzazione del diritto processuale penale* in *Diritto Penale e Processo*, 4, 2007, pagg. 522-530.

[479] A questa previsione si affianca quella, più generica, dell'art. 8 della Carta Fondamentali dei Diritti dell'Unione europea che protegge i dati di carattere personale.

Le nuove tecnologie hanno ormai generato un fenomeno perverso di limitazione, a volte esagerata e incontrollata, del diritto alla riservatezza di ogni individuo, risolvendosi, sul piano sociologico, in una riduzione delle aspettative di rispetto della *privacy*[480].

[480] In questi termini, C. FANUELE *Dati genetici e procedimento penale*, Cedam, 2009, pag. 78 e relativa citazione in nota 128.

CAPITOLO TERZO

La circolazione della prova digitale nell'ambito della cooperazione nello spazio giudiziario europeo

SOMMARIO: 1. Il linguaggio e la traduzione nelle procedure di cooperazione e di circolazione del contenuto della prova: l'individuazione di termini e isti tuti condivisi tra gli Stati membri dell'Unione europea - 1.1 Le scelte linguistiche di alcuni organi e nelle principali procedure di cooperazione - 2. Le modalità per una genuina acquisizione della prova digitale ai sensi della disciplina comunitaria ed alcune emblematiche normative nazionali - 3. La circolazione di prova digitale : organi e soggetti legittimati – 4. La circolazione dei dati e la struttura delle banche di raccolta. Dal sistema centralizzato al principio di domanda diretta nel iure condito comunitario: una svolta nella cooperazione informativa

1. *Il linguaggio e la traduzione nelle procedure di cooperazione e di circolazione della prova: l'individuazione di termini e istituti condivisi tra gli Stati membri dell'Unione europea*

La collaborazione tra Stati e la circolazione della prova in ambito UE richiedono un approccio tecnico-giuridico alle procedure e ai mezzi d'iniziativa e realizzazione, siano essi rappresentativi del principio di mutua assistenza o di mutuo riconoscimento, indipendentemente dallo strumento di cooperazione utilizzato e dagli organi comunitari e nazionali coinvolti.

A tal fine, è indispensabile che le autorità degli Stati membri, per poter fruire dei risultati della cooperazione, siano messe nelle condizioni di comprenderne appieno i contenuti sotto il profilo concettuale.

In una Babele di lingue d'Europa l'obiettivo della reciproca comprensione deve realizzarsi nel più breve tempo possibile, per non pregiudicare il raggiungimento degli interessi sottesi ai fini di giustizi a penale.

Come si è già avuto modo di sottolineare, il problema della traduzione giuridica, che si riflette anche nelle procedure di cooperazione e di circolazione

della prova, si sostanzia nella complessità legata alla circolazione dei concetti[481].

Le differenze tra gli ordinamenti statuali, infatti, si riflettono sui sistemi nazionali generando un ostacolo alla piena realizzazione di uno spazio libero di cooperazione di polizia e giudiziaria tra gli Stati membri, sia nelle ipotesi di assistenza giudiziaria, sia di reciproco riconoscimento[482].

L'Unione europea è particolarmente attenta alla salvaguardia del multilinguismo anche per la portata etico-culturale e di democraticità che supporta questa scelta. Questo lodevole obiettivo implica uno sforzo maggiore nella pratica di cooperazione da parte del giurista-linguista, il quale non deve fermarsi alla trasposizione letterale dell'idioma nazionale, ma deve indagare e studiare il sistema giuridico di riferimento[483].

Il parallelismo tra traduzione ed interpretazione che connota l'ambito del multilinguismo giuridico anche in materia penale, caratterizza non solo il regime linguistico della normativa comunitaria ma è sensibile alle procedure di cooperazione e di circolazione della prova.

Il pluralismo linguistico rappresenta una ricchezza ma, bilanciato con l'esigenza di sicurezza e giustizia, non deve risultare un ostacolo al dialogo tra le autorità nazionali, giudiziarie e di *law enforcement*, indebolendo o ritardando gli effetti positivi della cooperazione e della cooperazione immediata[484].

La globalizzazione del crimine e la rapidità con cui esso si sviluppa, richiedono risposte unitarie e solerti, per evitare gli aggravi delle conseguenze dannose e l'espansione incontrollata del fenomeno.

---

[481] Per un approfondimento sul problema della traduzione giuridica e dell'interpretazione, come strumenti utili per la circolazione dei concetti, si rinvia al capitolo Primo.

[482] In occasione del convegno tenutosi a Como il 14 luglio 2011 nel più ampio progetto biennale di ricerca dal titolo "*Giuristi, lingua ed Unione europea: la circolazione dei concetti in un mondo multilingua*", il dott. Filippo Spiezia, Assistente del Membro Nazionale presso Eurojust, intervenuto con una relazione dal titolo "*Regimi linguistici e cooperazione giudiziaria nella prospettiva di Eurojust*" (atti del Convegno in corso di pubblicazione), ha portato all'attenzione dell'uditorio un caso concreto che rappresenta l'emblema del problema linguistico e di interpretazione concettuale. L'esempio riguardava un intervento di Eurojust, nel suo ruolo di ufficio di coordinamento, su richiesta di un Tribunale italiano a seguito di una domanda di rogatoria all'estero. Quando l'autorità giudiziaria italiana ha fatto riferimento all'istituto dell'"incidente probatorio", il traduttore inglese si è bloccato e, trovatosi in difficoltà, ha scelto di procedere ad una traduzione meramente letterale ("*evidence accident*"), nulla sapendo di stare commettendo un errore o meglio ancora una traduzione non di qualità, poiché non ha così trasmesso alcun significato collegato al concetto originario e non noto all'interlocutore di lingua diversa dall'italiano.

[483] *Ibidem*.

[484] *Ibidem*. Il dott. Filippo Spiezia, in particolare, sottolinea gli effetti negativi di un allungamento dei tempi ed un aggravamento delle procedure di cooperazione specie nella lotta al crimine organizzato. Il multilinguismo, dunque, se diviene una barriera al dialogo aperto tra le autorità giudiziarie e di contrasto, può al contrario diventare un'opportunità per il crimine ed un fattore facilitante la criminalità transnazionale in generale, di criminalità organizzata in modo particolare.

Preliminarmente all'analisi della dimensione strettamente pratico-operativa, occorre affrontare le problematiche connesse alla traduzione e all'interpretazione degli atti normativi che regolano i rapporti di cooperazione giudiziaria.

La necessità di un approccio ermeneutico multilivello[485], richiede l'analisi in parallelo della fonte nazionale di trasposizione e della fonte sovranazionale di riferimento, coadiuvata dalla ricostruzione dei documenti di accompagnamento al testo convenzionale o degli atti preparatori alla norma, nell'intento di chiarire il significato delle espressioni più dubbie.

Il secondo passaggio obbligato consiste nella lettura critica della giurisprudenza comunitaria ad opera degli organi deputati all'interpretazione conforme, come ineliminabile punto di riferimento, in particolare la Corte Europea dei Diritti dell'Uomo e la Corte di Giustizia delle Comunità Europee.

Più in generale, lo sforzo richiesto non è quello di ricercare un istituto noto e già categorizzato nell'ordinamento nazionale, poiché spesso non trova un corrispondente perfettamente omologo in un sistema giuridico di diversa tradizione. È necessario, invece, indagare la *voluntas* del legislatore extranazionale per comprendere il significato intrinseco e profondo dei concetti espressi e le modalità di attuazione degli stessi.

L'obiettivo dell'Unione europea volto ad agevolare le procedure di cooperazione, si sostanzia, dal punto di vista operativo, nel passaggio da una forma di cooperazione interstatuale ovvero governativa, basata principalmente sullo strumento della rogatoria internazionale, a una forma intermedia di rapporto diretto tra le autorità degli Stati membri, fino alla concretizzazione del principio del mutuo riconoscimento.

Il fine del rafforzamento della cooperazione si trova espresso a chiare lettere nel Trattato di Lisbona, nel Programma di Stoccolma e anche nel testo dell'*Action Plan* 2010-2014.

Per il raggiungimento di esso è necessario intensificare gli sforzi verso forme rapide di confronto e scambio a livello di traduzione ed interpretazione nelle procedure di cooperazione (e non solo).

Ormai allargate irreversibilmente le maglie delle resistenze statuali, stante anche un più omogeneo quadro politico-giuridico dell'UE, l'elemento linguistico non può e non deve costituire un ostacolo alla piena evoluzione dei rapporti di cooperazione.

È di intuitiva evidenza, in questo contesto, l'esigenza di una traduzione delle rogatorie e delle richieste di cooperazione nella lingua prevista dai singoli atti convenzionali che regolano i rapporti interstatuali.

[485] La giurisprudenza della Corte di Cassazione italiana riconosce e attua questa pratica ermeneutica che considera un quadro normativo e giuridico multilivello e multilingue. In questi termini, si veda la sentenza della Corte di Cassazione, Sezioni Unite, Ramoci, 30 gennaio 2007, n. 4614.

L'attività di traduzione-interpretazione deve quindi essere svolta bi-direzionalmente, cioè sia quando viene avanzata una richiesta sia quando si ottengono le informazioni richieste.

Non sono da sottovalutare i costi che devono essere sostenuti per svolgere questo tipo di attività[486], poiché richiedono una particolare professionalità.

Solitamente è lo Stato richiesto di assistenza ad accollarsi le spese dell'esecuzione della traduzione.

Nei rapporti annuali di Eurojust, osservatorio privilegiato sotto questo profilo per le sue competenze, è segnalata la scarsa qualità delle traduzioni nelle procedure di cooperazione, con particolare riferimento alle rogatorie [487].

La scarsa attenzione linguistica nella richiesta di assistenza giudiziaria o di polizia può determinare lunghi tempi d'attesa, talvolta solo per ricevere un *feedback* positivo o negativo dall'autorità richiesta.

Qualora sia necessaria una nuova traduzione, l'ulteriore allungamento dei tempi può compromettere l'esito delle operazioni investigative o il corretto svolgimento dell'attività giudiziaria.

Il problema linguistico persiste ed anzi incrementa nel passaggio da una dimensione di cooperazione di tipo intergovernativo ad un rapporto diretto tra le autorità, laddove la cooperazione è il prodotto di una combinazione di forme e moduli tradizionali con metodi innovativi e a volte "atipici". In questo contesto, la conoscenza della lingua straniera da parte dei soggetti coinvolti nello scambio informativo consentirebbe un flusso proficuo e continuo, ottimizzando così l'operatività delle procedure di cooperazione.

In situazioni del genere, la conoscenza di una "lingua franca", comune a tutti, può costituire un *quid pluris* determinante a livello operativo, specie se

---

[486] Si pensi solo che nella DGT (Direzione Generale di Traduzione), l'agenzia incaricata di tutte le traduzioni scritte della CE, lavorano circa 1.750 traduttori a tempo pieno e 600 professionisti che si occupano di varie attività di gestione, amministrazione, comunicazione, pianificazione, ricerca e sviluppo.
Gli ultimi dati parlano di una produzione annuale di circa un milione e mezzo di pagine, l'80% delle quali tradotte dalle risorse interne alla DGT stessa, mentre il restante 20% da traduttori esterni**.** La DGI (DG Interpretazione, l'ex SCIC) invece si avvale di uno *staff* permanente di circa 500 interpreti di ruolo (funzionari) e 150 amministrativi, ai quali si affiancano più di 2700 interpreti freelance riconosciuti. Per quanto riguarda le cifre dell'interpretariato, la DG Interpretazione fornisce 700-800 interpreti per circa 50/60 riunioni che si tengono quotidianamente a Bruxelles e in altri luoghi. Le ultime cifre rivelano che nel 2009, la DGI ha prodotto 135.000 giornate di interpretariato in circa 10.500 riunioni. La cifra più recente delle spese di traduzione nell'Unione Europea è di 1.123 milioni di euro, corrispondente all'1% del suo *budget* annuale.
Dividendo tale cifra per la popolazione dell'Unione risultano 2,28 euro per abitante all'anno. Ogni volta che vengono aperte le porte ad un nuovo paese e ad una nuova lingua, a questo budget vanno aggiunti 25 milioni di euro. Questi dati sono presenti all'indirizzo internet: http://www.traduzione-testi.com/traduzioni/operatori-nel-settore-traduzioni/spese-di-traduzione-nellunione-europea.html (consultato in data 30 giugno 2010).

[487] I rapporti annuali di Eurojust sono consultabili sul sito dell'organismo (www.eurojust.europa.eu).

visto nell'ambito di squadre investigative comuni che strutturalmente operano in un gruppo etnicamente disomogeneo e composito.

Questa lingua può essere individuata nell'idioma inglese, almeno per quanto concerne il linguaggio tecnico-giuridico e gli istituti tipici.

Non si esclude che tra i membri delle autorità coinvolte vi siano persone con una conoscenza almeno sufficiente o buona di una o più lingue diverse da quella nativa e che, pertanto, decidano di sfruttare questo patrimonio cognitivo per tessere relazioni più fitte con autorità giudiziarie e di polizia estere, spesso ritenendo di non necessitare dell'intervento di un traduttore o di potere prescindere dal coinvolgimento di organismi UE di collegamento come Europol e Eurojust.

Un tale atteggiamento, se da un lato è costruttivo e agevola la rapida cooperazione, in alcune circostanze può rivelarsi negativo, perché porta a trascurare il contributo, spesso determinante, di questi organismi nell'analisi di dati investigativi e nell'individuazione delle migliori forme di cooperazione, grazie alla prospettiva preferenziale data dalla struttura centralizzata, dalla specializzazione e dalla presenza di rappresentanti degli Stati membri [488].

Da qui l'annosa diatriba tra la garanzia del multilinguismo, per i suoi aspetti di democraticità, e lo sviluppo di una cultura e una formazione linguistica comune che fornisca uno strumento unitario di comunicazione tra operatori, mediante la scelta di una sola lingua, quale potrebbe essere l'inglese, con tutti i problemi connessi di interpretazione e traduzione dei concetti giuridici.

Il problema linguistico nelle procedure di cooperazione di polizia e giudiziaria in ambito UE potrebbe essere validamente superato dalla piena attuazione del principio del mutuo riconoscimento, come voluto dall'art. 82 del Trattato di Lisbona, la cui operatività piena riposa su solide basi di reciproca fiducia tra gli Stati e di condivisione di valori. I dubbi di traduzione-interpretazione verrebbero sciolti da un'armonizzazione delle legislazioni statuali, oltre che da un auspicabile incremento della legislazione penale comunitaria, individuando gli omologhi di ogni istituto giuridico.

In un contesto di comunanza di valori, il multilinguismo giuridico degli organi e delle autorità competenti per le procedure di cooperazione può rappresentare una precondizione per lo sviluppo del mutuo riconoscimento e per una rapida circolazione delle informazioni tra gli organi comunitari, le autorità di polizia e giudiziaria degli Stati membri [489].

---

[488] L'aspetto deteriore di questo atteggiamento di tipo auto-referenziale è stato sottolineato con forza dal dott. Filippo Spiezia in occasione del convegno di Como più volte citato, anche in base alla sua propria esperienza professionale in Eurojust.

[489] Purtroppo, ad oggi, questo scenario di multilinguismo degli operatori della cooperazione costituisce soltanto una proposta o un'aspettativa di sviluppo futuro e non una realtà contemporanea.

Ad oggi si deve scontare un ritardo linguistico-formativo che non permette un'immediata comprensione delle richieste di cooperazione e delle informazioni inviate in risposta, se eseguite nella lingua madre, ma nemmeno permette, in ogni circostanza e qualsiasi siano le autorità coinvolte, di dialogare per mezzo della lingua-franca, l'inglese, che comunque continua ad essere la lingua più diffusa e conosciuta.

Il problema linguistico nelle procedure di cooperazione e per la circolazione della prova, con le sue peculiarità, resta aperto e soggetto a diverse soluzioni, ciascuna delle quali presenta dei vantaggi e dei limiti.

La garanzia del pluralismo linguistico rende impossibile l'immediata comprensione delle richieste e dei suoi risultati, se non accompagnati da una traduzione ed interpretazione corrette. La traduzione e l'interpretazione spesso sono poco proficue perché sono il frutto di una difficile (se non impossibile) operazione di equivalenza di valori ed istituti giuridici di ordinamenti di diversa cultura e tradizione. L'uso di una lingua-franca non è percorribile a causa della limitatezza delle conoscenze linguistiche degli organi richiedenti e richiesti e del permanere del problema di esprimere concetti avulsi ad altri ordinamenti giuridici[490]. Una sola lingua comune può velocizzare il flusso dei dati e delle informazioni, soprattutto se supportato da un multilinguismo degli

---

Non si è a disposizione di dati ufficiali che indichino lo stato delle competenze linguistiche e più in particolare delle conoscenze almeno della lingua giuridica da parte dei soggetti coinvolti nelle procedure di cooperazione. Il dato di comune conoscenza che si tramanda come massima d'esperienza riporta una scarsa attitudine e capacità linguistiche, più in generale, della popolazione dell'Unione europea. Questo sentore è confortato da riscontri indiretti quali il numero elevato di traduttori e interpreti dell'Unione europea, la preoccupazione di Eurojust per la scarsità delle traduzioni giuridiche, l'attenzione comunitaria allo sviluppo di un programma formativo per l'istruzione e la formazione linguistica.

In relazione a quest'ultima indicazione, si richiama la Comunicazione della Commissione al Consiglio, del 13 aprile 2007, dal titolo «Quadro per l'indagine europea sulle competenze linguistiche» [COM(2007) 184 definitivo - Non pubblicata nella Gazzetta ufficiale]. L'indagine europea sulle competenze linguistiche si prefigge di gettare le basi di un futuro indicatore europeo delle competenze linguistiche. Questo indicatore consentirà di misurare e di migliorare l'apprendimento delle lingue straniere nell'Unione europea (UE). L'indicatore europeo delle competenze linguistiche () permetterà d'identificare le migliori pratiche d'insegnamento e di apprendimento. Offrirà anche la possibilità di valutare i progressi realizzati rispetto agli obiettivi del quadro strategico per il multilinguismo concernente l'accesso dei cittadini dell'Unione europea (UE) al multilinguismo e all'apprendimento sin dall'infanzia di almeno due lingue straniere.

Più in particolare, l'Unione europea è molto attenta alla formazione dei giudici nazionale a che sia anche una formazione anche linguistica, finanziando progetti volti a tale scopo.

La consapevolezza del dott. Filippo Spiezia, nel suo intervento al seminario di studi più volte citato, della necessità di creare un vero magistrato europeo che sappia dialogare con gli altri colleghi di altri Stati, comprendendosi reciprocamente non solo dal punto di vista linguistico ma anche delle ragioni di sistema, richiama il tema dei modi della formazione. Si noti che la Commissione europea, sostituendo il vecchio programma Agis, il primo gennaio 2007 ha promosso un progetto da realizzare nel periodo 2007-2013 sulla formazione dei magistrati collegata ad una dimensione europea, con un forte impulso anche finanziario.

[490] Uno fra tutti, si torna a ricordare l'esempio della difficile, se non impossibile, traduzione in inglese dell'istituto di diritto processuale italiano dell'"*incidente probatorio*".

operatori che può prescindere dalle forme di traduzione-interpretazione. L'impiego dell'interprete-traduttore può risultare soddisfacente, anche in un contesto multilingua, se sussistono delle basi condivise di istituti e valori tra i sistemi giuridici degli Stati membri.

Nell'analisi del problema linguistico nelle procedure di cooperazione e di circolazione della prova è necessario considerare l'interesse dell'indagato-imputato a conoscere e comprendere il contenuto degli procedimentali, nella prospettiva della garanzia dei diritti.

In base ai dettami della Direttiva 2010/64/UE su traduzione e interpretazione nel procedimento penale e nelle procedure di attuazione del mandato di arresto europeo, in particolare al punto 30 dei *consideranda*, si esige che i documenti fondamentali, o almeno le parti rilevanti di essi, siano tradotti a beneficio di indagati o imputati per garantire l'equità del procedimento. In base all'art. 3 della menzionata Direttiva, tra i documenti fondamentali rientrano le decisioni che privano una persona della propria libertà, gli atti contenenti i capi d'imputazione e le sentenze. In qualsiasi altro caso sono le autorità competenti a qualificare un atto o documento come fondamentale. Gli indagati, gli imputati o il loro difensore possono presentare una richiesta motivata a tale scopo.

Non è invece necessario tradurre i passaggi di documenti fondamentali che non siano rilevanti allo scopo di consentire agli indagati o agli imputati di conoscere le accuse a loro carico. È possibile fornire una traduzione orale o un riassunto orale di documenti fondamentali, anziché una traduzione scritta, a condizione che non pregiudichi l'equità del procedimento.

Da questi pochi richiami al testo della Direttiva si evince la sua applicabilità anche a tutti quegli atti, documenti e provvedimenti che sono il risultato di una procedura di cooperazione di polizia e giudiziaria, rendendone comunque necessaria e dovuta la traduzione (con tutte le difficoltà già più volte sottolineate).

Ciò a dire che, anche qualora si scegliesse un regime di monolinguismo condiviso tra gli Stati membri, da applicare nelle procedure di cooperazione, il problema linguistico di traduzione-interpretazione permarrebbe, manifestandosi in momenti e circostanze differenti. In altre parole, il tempo (ed il denaro) eventualmente risparmiato nelle procedure di cooperazione sarebbe speso successivamente, restando, così, irrisolto il rischio di dispersione delle prove e di un allungamento dei tempi del processo e del procedimento.

Indipendentemente dall'approccio scelto per il miglioramento e la diffusione rapida delle procedure di cooperazione e di scambio di dati nello spazio giuridico comunitario, il tema della formazione resta una componente essenziale e ineliminabile. Esso richiede lo sviluppo delle conoscenze del

sistema giuridico comunitario e degli Stati membri e delle capacità linguistiche da parte di tutti gli organi e soggetti coinvolti [491].

1.1 Le scelte linguistiche di alcuni organi comunitari e nelle principali procedure di cooperazione

La scelta linguistica effettuata da ciascun organo comunitario e per le procedure di cooperazione incide sull'intero sistema di collaborazione, sui tempi necessari e sui costi da sostenere.

Ogni opzione in tal senso è (o almeno dovrebbe essere) il frutto di un ragionamento ponderato in base agli scopi da raggiungere, alla struttura organica, ai soggetti coinvolti e all'attività tecnicamente svolta.

La Decisione Quadro sul MAE da' preminenza all'identità del dato linguistico di categorie criminali omogenee (*nomen iuris*), a prescindere dalla corrispondenza completa della fattispecie delittuosa. Nonostante ciò alcuni Stati hanno scelto una trasposizione nazionale che facesse corrispondere ad una fattispecie indicata nella Decisione anche più fattispecie interne, per ricalcare il modello proprio e per maggiore aderenza al principio di legalità e tassatività delle fattispecie criminose [492].

All'art. 8, comma secondo, del citato atto normativo è previsto che il mandato europeo sia tradotto nella lingua ufficiale o in una delle lingue ufficiali dello Stato di esecuzione (qualora siano riconosciute più lingue ufficiali).

Tuttavia ogni Stato, all'atto dell'esecuzione, può accettare un mandato di arresto europeo anche in un'altra lingua ufficiale dell'Unione europea per volontà propria o perché previsto dalla norma nazionale di implementazione.

Nell'allegato 4 del *European Handbook on EAW*, si trova una descrizione precisa del regime linguistico accettato dagli Stati membri in materia. Dalla lettura di questi prospetti emerge un quadro molto variegato che è indice di una carenza di una posizione comune. Vi sono Stati che accettano il mandato

[491] Un forte impulso è giunto con il Trattato di Lisbona che, all'art. 82, prevede, in materia di cooperazione giudiziaria, che il Parlamento ed il Consiglio, secondo la procedura legislativa ordinaria, adotteranno misure per sostenere la formazione dei magistrati per diffondere una cultura giuridica europea.
Nella Comunicazione della Commissione sul Programma di Stoccolma è stata di nuovo ribadita l'importanza della formazione giudiziaria, ai fini della piena attuazione del Programma di Stoccolma, e anche della formazione di tutte le professioni legali, anche mediante il progetto pilota di lancio di possibili esperienze di Erasmus tra tutte le autorità giudiziarie ed i professionisti del diritto.

[492] Così, per esempio è successo in Italia laddove al magistrato nazionale è richiesto, per ogni singolo caso di applicazione del Mandato di Arresto Europeo, di controllare se la fattispecie indicata da un'autorità straniera corrisponde ad una delle tipologie delittuose trasposte nella legislazione nazionale.

solo nella propria lingua ufficiale[493]; Stati che accettano anche in altra lingua diversa da quella nazionale ma solo a condizione di reciprocità[494]; Stati che accolgono il mandato in più lingue diverse dalla propria[495]; Stati che accettano il MAE in una lingua diversa da quella nazionale soltanto nei confronti di Stati con cui esistono accordi bilaterali[496]; uno Stato che accetta il MAE nella lingua nazionale ma anche in francese, inglese e tedesco, a condizione che si tratti di uno Stato che a sua volta accetta la richiesta di mandato in altre lingue diverse da quella nazionale[497]; Stati che accettano il MAE solo nella loro lingua nazionale ma che si impegnano a tradurlo e farlo precedere anche da un *alert* nel sistema SIS.

Questo regime tanto differenziato mostra una tendenza generale alla conservazione del multilinguismo e particolare di tutela della propria lingua nazionale da parte di ogni Stato. La scelta di accogliere il MAE nella lingua nazionale di quei Paesi con cui vi sono accordi bilaterali è sintomatico della volontà di agevolare i rapporti fiduciari, i quali tuttavia sono subordinati non tanto a dati di fatto e collaborazioni pratiche, quanto più ad una pattuizione scritta e ad impegni formalmente assunti. A parere di chi scrive, dunque, questa scelta rappresenta una forma di rapporto fiduciario un po' artificiale ed artificiosa, perché non può prescindere da una burocratizzazione e da un'assunzione reciproca di impegni. La fiducia, invece, dovrebbe nascere con maggiore spontaneità e senza troppe forzature, limiti e formalità.

La scelta di chi accoglie le richieste di mandato in altra lingua solo se provenienti da Stati che a loro volta hanno espresso la propria volontà reciproca di apertura verso altre lingue nazionali, sembrerebbe sintomatica di una politica premiale e di sprono per altri Stati ad accogliere la stessa soluzione. In questa possibile prospettiva interpretativa, l'intenzione può considerarsi lodevole.

Purtuttavia ancora molte nazioni accettano il MAE nella sola lingua nazionale e questa scelta può essere letta almeno secondo due punti di vista

[493] Questi Stati sono: la Bulgaria, la Francia, la Grecia, l'Italia, la Polonia, il Portogallo, l'Irlanda e il Regno Unito.
[494] Questa condizione è accettata soltanto dalla Germania e dall'Austria.
[495] Il riferimento è al Belgio che accoglie il francese, l'inglese e l'olandese; Cipro che accetta il greco, il turco e l'inglese; Danimarca che accetta lo svedese e l'inglese; l'Estonia che accoglie anche il mandato in inglese; la Lettonia che accetta l'inglese come anche la Lituania, la Slovenia e Malta; l'Olanda che accoglie il mandato in inglese o in altra lingua ufficiale dell'Unione europea se accompagnata da una traduzione inglese; la Romania che accetta i mandati anche in inglese e in francese e la Svezia con il danese, il norvegese e l'inglese. A ciascuno Stato, ovviamente, va aggiunta l'accettazione della richiesta di mandato di arresto europeo nella propria lingua nazionale
[496] È questo il caso della Repubblica ceca e slovacca che hanno un trattato bilaterale, oltre ad un trattato stipulato da entrambe con l'Austria e che, dunque, accettano il MAE nelle lingue degli Stati parte dell'accordo.
[497] La menzionata ipotesi riguarda la sola Ungheria.

differenti: *in primis* come segno di ancoraggio al proprio nazionalismo e alla propria sovranità nazionale anche sotto l'aspetto linguistico, nell'intento di evitare ogni possibile forma di contaminazione straniera; d'altro lato può rappresentare un più banale (ma anche preoccupante) *gap* linguistico e anche di traduzione e di traduttori, che porta inevitabilmente a rigettare le richieste formulate in altre lingue.

La differenziazione del regime linguistico provoca ritardi e spesso compromette il buon esito del mandato di arresto. Il problema poi è accentuato nei casi in cui, a seguito della richiesta di mandato, vengono fornite delle informazioni supplementari da parte dell'autorità ricevente, sul cui punto la decisione quadro non dice nulla.

In base all'art. 3, comma sei, della Direttiva 64/2010/CE, nel procedimento di esecuzione di un mandato di arresto europeo lo Stato membro di esecuzione deve assicurare la traduzione scritta del documento trasmesso dalle proprie autorità competenti ai soggetti destinatari che non comprendono la lingua in cui il mandato d'arresto europeo è redatto o è stato tradotto dallo Stato membro emittente[498].

Dai vari rapporti finali stilati sul controllo dell'operatività del mandato di arresto europeo, sono emerse delle pratiche rassicuranti, consistenti nell'accettazione delle richieste in una lingua diversa da quella nazionale, specie nei casi di urgenza ovvero in caso di trasmissione di informazioni supplementari.

Questa prassi applicativa di elasticità linguistica è sostenuta ed incoraggiata nel testo della Raccomandazione n. 5, collegata al rapporto annuale sul MAE[499].

La Decisione quadro 2008/978/GAI del Consiglio del 18 dicembre 2008, relativa al mandato europeo di ricerca delle prove diretto all'acquisizione di oggetti, documenti e dati da utilizzare nei procedimenti penali, all'art. 6, prevede che il MER sia trasmesso per il tramite di un formulario standardizzato compilato a cura degli Stati, il cui modello si trova in allegato all'atto normativo. Il *format* è compilato o tradotto dallo Stato di emissione nella lingua ufficiale o in una delle lingue ufficiali dello Stato di esecuzione. Ciascuno Stato membro può, al momento dell'adozione della menzionata Decisione quadro o successivamente, attestare in una dichiarazione depositata presso il Segretariato Generale del Consiglio che accetterà i mandati o la

[498] Non si ritiene, in questa sede che sia necessario ricostruire di nuovo tutte le disposizioni della menzionata Direttiva ma semplicemente si torna a ribadire che, oltre alla necessità di una traduzione e interpretazione è richiesto che queste siano di una qualità tale da garantire un equo processo.

[499] Questi dati sono stati presentati dal dott. Filippo Spiezia in occasione della relazione al seminario di studi comasco del 14 luglio 2011.

traduzione di un mandato in una o più lingue ufficiali delle istituzioni dell'Unione.

L'utilizzo di un documento unico per tutti i Paesi è un valido supporto per ovviare ai problemi di interpretazione e traduzione, essendo il risultato di un sentire comune dell'Unione europea e di ciascuno Stato membro.

Non esistendo un'armonizzazione dei sistemi giuridici e non essendosi realizzato ancora quell'auspicato avvicinamento delle legislazioni nazionali, almeno sotto il punto di vista delle norme minime, il formulario presente un inevitabile limite di genericità.

Si chiede, infatti, che l'autorità emittente certifichi che gli oggetti, i dati e i documenti richiesti *« se si trovassero nel territorio dello Stato di emissione, potrebbero essere acquisiti in base al diritto dello Stato di emissione in un caso nazionale analogo, anche se in applicazione di misure processuali eventualmente diverse »*. L'indicazione dell'autorità di emissione nazionale è rimessa alla discrezionalità degli Stati, stante la non omogeneità dei sistemi. Nella Direttiva sono elencati il magistrato inquirente, il pubblico ministero, il giudice o l'organo giurisdizionale[500] e, in conclusione, è inserita una formula di chiusura riferita a *« qualsiasi altra autorità giudiziaria come definita dallo Stato di emissione che, nel caso specifico, agisca nella sua qualità di autorità inquirente nel procedimento penale e sia competente a ordinare l'acquisizione dei mezzi di prova nei casi transfrontalieri in base alla normativa nazionale »*.

Tra i dati richiesti nel formulario, l'autorità dello Stato di emissione deve indicare le lingue con cui è possibile comunicare.

Il formulario, in applicazione di quanto previsto dalla Direttiva, oltre a contenere una sezione dettagliata con l'indicazione dei soggetti da contattare anche ed eventualmente per informazioni suppletive, presenta un elenco di reati rispetto ai quali è possibile avanzare la richiesta del MER, indipendentemente poi dalle specificità di tali fattispecie criminose nei singoli ordinamenti nazionali e anche indipendentemente dal fatto che queste siano o meno penalmente rilevanti[501].

Il mandato europeo di ricerca della prova riguarda dati, oggetti e documenti. La nozione di "documento" inserita in un ambito giuridico non crea particolari difficoltà di mera traduzione meccanica ma, se pensiamo al

[500] Il riferimento chiaro è alla macro differenza di sistema processuali tra quegli ordinamenti che presentano ancora la figura del giudice istruttore, come è il caso per esempio della Francia, e chi, come l'Italia, conosce solo il pubblico ministero.

[501] L'unica specifica è stata richiesta dalla Germania in relazione al reato di sabotaggio, di terrorismo, di criminalità informatica, di razzismo e xenofobia, di racket e estorsione, di truffa per cui, a norma dell'art. 23, paragrafo 4, della Decisione Quadro lo Stato di emissione deve compilare anche la parte del formulario sui motivi e le circostanze di fatto per cui si avanza il MERP, sono nei casi in cui si voglia confermare ce il reato o i reati soddisfano i criteri indicati da tale Paese per la tipologia criminosa in questione.

documento come prova, allora è necessario indagare la definizione propria di ciascun sistema[502].

L'iniziativa del Regno del Belgio, della Repubblica di Bulgaria, della Repubblica di Estonia, del Regno di Spagna, della Repubblica d'Austria, della Repubblica di Slovenia e del Regno di Svezia per una direttiva del Parlamento europeo e del Consiglio, relativa all'ordine europeo di indagine penale (2010/C 165/02) è nata dall'evidenza di un sistema insufficiente ed inefficiente di ricerca della prova, troppo frammentato e complesso per garantire lo sviluppo della cooperazione giudiziaria.

L'OEI offre un regime unico per l'acquisizione di prove. Per alcuni tipi di atti d'indagine, come il trasferimento temporaneo di persone detenute, l'audizione mediante videoconferenza o teleconferenza, l'acquisizione di informazioni su conti bancari o operazioni bancarie o le consegne controllate, sono tuttavia necessarie disposizioni supplementari che dovrebbero essere incluse nell'OEI. Gli atti d'indagine che implicano l'acquisizione di prove in tempo reale, in modo continuo e per un tempo determinato sono coperti dall'OEI, ma è opportuno che all'autorità di esecuzione sia concessa flessibilità con riguardo a tali atti, in considerazione delle differenze esistenti tra le legislazioni nazionali degli Stati membri.

La direttiva sostituisce le decisioni quadro 2003/577/GAI e 2008/978/GAI, nonché i vari strumenti relativi all'assistenza giudiziaria in materia penale per quanto riguarda l'acquisizione di prove da utilizzare nei procedimenti penali.

Anche l'OEI, come il mandato europeo di ricerca della prova, è modulato sulla base di un formulario *standard*, come previsto dall'art. 5.

Ciascuno Stato membro indica la lingua o le lingue ufficiali delle istituzioni dell'Unione che possono essere usate, in aggiunta alla lingua o alle lingue ufficiali dello Stato membro interessato, per completare o tradurre l'OEI quando lo Stato in questione è quello di esecuzione.

Permane tuttavia il rischio che, anche con questo strumento non ancora attuato (in quanto non pubblicato in Gazzetta Ufficiale), si generi una forte ed incontrollata disomogeneità linguistica che contrasta con l'obiettivo di efficacia ed efficienza della misura.

---

[502] A titolo esemplificativo e per meglio chiarire il problema sollevato, si consideri che per il diritto processuale italiano le prove documentali vanno annoverate nell'ambito delle prove c.d. precostituite, cioè quelle che preesistono al processo e non sono caratterizzate dalla formazione nell'ambito dello stesso e soprattutto della preordinazione al processo medesimo. Le prove documentali, invero, non nascono per essere utilizzate nel processo ma hanno piuttosto una valenza sostanziale, che le rende per lo più idonee ad una utilizzazione stragiudiziale.
Proprio alla luce dell'evoluzione, si suole distinguere, comunemente, tra prove documentali tipiche e prove documentali atipiche.

L'analisi del contenuto del formulario dell'OEI evidenzia ancora la presenza di formule generiche che possono portare a diverse applicazioni in ogni sistema giuridico nazionale.

Si pensi, a titolo esemplificativo, al concetto di "*atto d'indagine*" che presenta delle peculiarità di principio e in fase operativa nei diversi Stati membri[503].

Eurojust, quale organo europeo di collegamento, si è dotato di un regime linguistico che considera le tipologie di atti ufficiali emessi, la prassi dei rapporti tra i suoi membri nazionali ed il personale che collabora dall'interno e le relazioni con le autorità nazionali.

L'assetto normativo, con particolare riferimento all'art. 31, prevede che gli atti esterni ed ufficiali di Eurojust, diretti alle autorità nazionali, siano tradotti in tutte le ventitre lingue ufficiali degli Stati membri.

In inglese invece è tutta la corrispondenza, sempre ufficiale, intrattenuta da Eurojust con le altre Agenzie (Olaf e Europol), con il Consiglio, la Commissione ed il Parlamento europeo e nelle relazioni tra i vari membri nazionali.

Quanto al rapporto con le autorità degli Stati, ciascun membro si esprime nel proprio idioma quando dialoga con la corrispondente autorità statale e viceversa.

In base alla nuova decisione di Eurojust, all'art. 5 a), è prevista l'istituzione del *on call coordination system* per i casi urgenti. Tramite la composizione del numero dedicato é possibile entrare in contatto diretto con il proprio membro nazionale e dunque rivolgersi nella lingua comune e, a richiesta si può ottenere il collegamento telefonico con il membro nazionale interessato all'esecuzione di un provvedimento o di una rogatoria utilizzando, in tal caso, la lingua inglese.

Nelle ipotesi in cui le autorità giudiziarie nazionali convengano presso Eurojust per una riunione di coordinamento, possono utilizzare la lingua nazionale ed avere un interprete in simultanea[504].

---

[503] Altre possibili problematiche di natura linguistica ed interpretativa sono rinviabili a quanto già espresso in relazione al mandato europeo di ricerca della prova poiché i formulari, con le dovute eccezioni e particolarità, presentano uno schema ed uno stile molto simile. Inoltre si ribadisce che, ad oggi, l'iniziativa di un ordine europeo d'indagine è ancora tale poiché la correlata direttiva non è stata ancora pubblicata sulla Gazzetta Ufficiale e, dunque, è ancora prematuro fare delle considerazioni più analitiche sull'istituto. Il Gruppo "*Cooperazione in materia penale*" si è riunito il 7 e l'8 febbraio 2011 e ha proseguito l'esame dell'iniziativa per una direttiva relativa all'ordine europeo di indagine penale, discutendo in particolare degli articoli da 1 a 18, con esclusione dei soli articoli 8 e 10 e sull'art. 32.
Per un approfondimento si rinvia alla lettura integrale del testo dell'iniziativa e del fascicolo interistituzionale correlato, consultabili sul sito www.dirittopenaleeuropeo.it (consultato il 30 giugno 2011).

Eurojust offre, dunque, un buon banco di prova e un buon punto di riferimento per testare gli aspetti positivi e l'efficacia dell'uso della lingua inglese come lingua di comune comprensione e dialogo, affiancata all'esperienza del multilinguismo. Il vero valore aggiunto di questo organismo di crescente importanza risiede nella capacità dei diversi rappresentanti nazionali di sapere dialogare in lingua inglese, attenuando le barriere interstatali.

Anche Europol, nello svolgimento delle sue funzioni principali, è particolarmente attento al ruolo della lingua utilizzata, affinché la comunicazione sia rapida ed effettiva. L'approccio linguistico non è disciplinato dalla Decisione quadro istitutiva dell'Ufficio, ma è lasciato alla sovranità legislativa dei singoli Stati membri[505].

In base, però, a quanto previsto dall'art. 47, a Europol si applicano le disposizioni del regolamento n. 1 del Consiglio, del 15 aprile 1958, che stabilisce il regime linguistico della Comunità Economica Europea. Il Consiglio di Amministrazione decide all'unanimità l'organizzazione linguistica interna ad Europol. I servizi di traduzione necessari per i lavori dell'Ufficio sono assicurati dal centro di traduzione delle istituzioni dell'Unione europea.

In base al menzionato Regolamento, le lingue utilizzate sono le ventitre lingue ufficiali dell'Unione europeo.

Europol dunque rappresenta un valido esempio di applicazione del plurilinguismo, non senza rilevare la necessità dell'affiancamento di personale esperto in lingua, traduzione e interpretazione.

La Decisione del 1999 istitutiva di Olaf, Ufficio Europeo per la Lotta Antifrode, composta di poche disposizioni, non prevede nulla in particolare sul regime linguistico utilizzato da questo organo nello svolgimento delle sue attività. Per via indiretta si deduce che nei rapporti con Eurojust è utilizzata la lingua inglese.

Dalla lettura del manuale operativo del personale di Olaf[506], si evince che nel caso di attività d'indagine nei confronti dell'indagato o in contraddittorio, i soggetti interessati devono poter dialogare in una delle lingue ufficiali dell'Unione europea.

Anche nel caso di Olaf, dunque, si osserva una propensione alla garanzia del multilinguismo, con eccezioni nei rapporti tra organi comunitari in cui è d'uso la lingua inglese.

---

[504] L'interpretariato simultaneo è sicuramente un mezzo utile messo a disposizione della magistratura ma questo non solleva dai problemi di trasposizione efficace di termini ed istituti rispondenti ad un sistema giuridico con tradizioni diverse.

[505] Il riferimento è all'art. 12 della Decisione 2009/371/GAI.

[506] Il manuale è consultabile all'indirizzo internet http://ec.europa.eu/dgs/olaf/legal/manual/short/ IT.pdf (consultato il 10 giugno 2011).

Nel novero degli organismi atti ad agevolare la cooperazione giudiziaria, un ruolo importante va assegnato alla Rete Giudiziaria Europea (*European Judicial Network*)[507]. Tale Organo è composto da intermediari attivi che hanno il compito di agevolare la cooperazione giudiziaria tra gli Stati membri attraverso un'organizzazione facente capo ad una sede centrale che si dirama in uno o più punti di contatto nazionali. Questi punti di contatto hanno lo scopo di fornire alle autorità giudiziarie degli Stati membri tutte le informazioni utili per dare avvio ad una procedura di cooperazione o per migliorare l'attività di cooperazione già in corso.

Le capacità linguistiche richieste ai componenti della Rete permettono di superare le barriere di linguaggio, anche giuridico ed il *sito web* generale è strutturato per essere uno strumento di supporto ad una traduzione giuridica corretta.

Anche i Magistrati di Collegamento assumono un ruolo determinante nelle procedure di cooperazione e nell'agevolazione della collaborazione, superando le differenze linguistiche e le difficoltà di comprensione reciproca [508].

2. *Le modalità per una genuina acquisizione della prova digitale ai sensi della disciplina comunitaria ed alcune emblematiche normative nazionali*

Le Corti nazionali hanno un diverso approccio alla prova digitale, cioè vi sono giudici che richiedono dei requisiti più stringenti per la sua ammis sibilità, altri invece che acquisiscono tale prova bilanciandone la potenzialità probatoria in sede di valutazione.

L'ordinamento comunitario, ad oggi, non offre un supporto in materia, non essendo state emesse delle norme precise e specifiche sulla prova digitale e sui relativi parametri di giudizio di genuinità.

Il problema, però, è ancora più a monte se si considera che non esistono degli *standard* comuni che dettino le *best practices* di *computer forensics*.

Non basta considerare la genuinità della prova in sede processuale ma, prima ancora, l'elemento probatorio non deve essere stato compromesso nella fase d'indagine[509].

---

[507] Questo organo è stato istituito con l'Azione comune n. 98/428/GAI pubblicata sulla G.U.C.E., L. 191/4 del 7 luglio 1998.

[508] Il Consiglio dell'Unione europea ha adottato il 22 aprile 1996 un'azione comune relativa ad un quadro di magistrati di collegamento, diretto a migliorare la cooperazione giudiziaria fra gli Stati membri dell'Unione europea. Tale atto è stato pubblicato in G.U.C.E., L. 105/1 del 27 aprile 1996.

[509] Sulla genuinità della prova raccolta nella fase delle indagini si rinvia al capitolo Secondo, paragrafo 2.2.

Soltanto una prova digitale raccolta e poi acquisita mantenendone la genuinità può costituire, dal punto dell'idoneità epistemologica, un valido supporto scientifico per la ricostruzione del fatto.

Non ogni conoscenza può e deve entrare indiscriminatamente nel processo penale ma occorre un vaglio preventivo e anche successivo, in fase di valutazione da parte del giudice. È pertanto necessario procedere ad un controllo, all'interno del processo, sui metodi scientifici utilizzati sulla prova da acquisire.

Per l'ordinamento giuridico italiano, il riferimento è all'art. 190 c.p.p. che richiede, per così dire, due fasi di valutazione: un primo contraddittorio per la disamina dell'effettiva scientificità del mezzo di prova richiesto e, superata questa fase, un contraddittorio per vagliare la concreta rilevanza del mezzo di prova ai fini della decisione sulla *re giudicanda*.

In nessuno di questi momenti viene violata la regola della neutralità metodologica del giudice, che mantiene la sua valutazione sulla scientificità del mezzo, senza entrare nel merito dell'attendibilità.

Diverso invece il caso in cui si la prova digitale, come le altre prove scientifiche, sia qualificata come prova atipica per cui, ai sensi dell'art. 189 c.p.p., al giudice resta la scelta discrezionale e personale sull'acquisizione o meno della prova al processo[510].

La ricostruzione delle due possibilità offerte dall'ordinamento processuale penale italiano è rappresentativa di una diatriba aperta tra i sostenitori della prova scientifica come prova atipica *tout court* e coloro che, diversamente, valutano la prova scientifica, quindi anche della prova digitale, come un mezzo di prova nominato, caratterizzato da alcune peculiarità[511].

Anche nel sistema giuridico francese, come in quello italiano, non esiste una definizione normativa di prova digitale, né tantomeno delle disposizioni *ad hoc* che ne regolano la raccolta, l'archiviazione e l'acquisizione. Semplicemente all'art. 427 del codice di procedura penale francese è prevista la libertà per il giudice di ammettere qualsiasi forma di prova, nel rispetto dell'attinenza con i fatti in decisione. Questo principio di prova atipica trova il

[510] Si pensi, per esempio, al già menzionato caso di Garlasco nel cui processo il Giudice presso il Tribunale di Vigevano, nonostante i pareri contrastanti di esperti nominati dalle parti, ha ritenuto di acquisire la prova informatica costituita dai dati estratti dal computer di Alberto Stasi, indipendentemente dai dubbi sollevati sulla scientificità delle operazioni di *computer forensics*, ritenendo che in sede di valutazione si sarebbe potuto bilanciare il valore probatorio effettivo.

[511] Si rinvia, sul punto, a L. DE CATALDO NEUBURGER *op.cit*.; AA.VV. *La prova scientifica*, *op.cit.* Più in generale, sulla prova scientifica, si invita alla lettura di G. CANZIO, *Prova scientifica, ragionamento probatorio e libero convincimento del giudice penale,* in *Dir. pen. proc*., 2003, p. 1193, in cui l'Autore qualifica il metodo seguito dal giudice come "retroduttivo"; ID., *Prova scientifica, ricerca della "verità" e decisione giudiziaria nel processo penale*, in AA. VV., *Decisione giudiziaria e verità scientifica*; Milano, 2005, p. 55. Sul punto, si veda anche C. BRUSCO, *La valutazione della prova scientifica*, in *Dir. pen. proc*., 2008, *Dossier: La prova scientifica nel processo penale*, p. 23.

suo limite nel rispetto delle norme penali sostanziali e processuali e nel rifiuto di ammettere prove raccolte secondo metodologie pseudo-scientifiche. L'art. 429 del codice di procedura penale francese impone tre condizioni di ammissibilità della prova: l'indagine deve essere stata effettuata legittimamente; la persona deve aver agito in adempimento alle sue funzione ed in una materia di propria competenza; il personale intervenuto deve avere riportato in maniera precisa quanto visto e trovato e le procedure utilizzate[512].

In base all'esperienza dell'ordinamento giuridico tedesco, affinché un dato digitale possa divenire una *e-evidence* valida per un processo penale è necessario che: il dato sia sicuro, la fonte sia identificata, la raccolta sia stata eseguita mediante l'applicazione del metodo scientifico informatico.

Anche in Germania, dunque, non esiste una definizione e delle disposizioni specifiche che regolano la prova digitale ma, applicando principi generali del processo, il tentativo della prassi e della giurisprudenza è quello di adattarli alla peculiarità della prova elettronica.

Le stesse autorità investigative tedesche sono consce dell'evoluzione continua di nuove forme di prova digitale. Si pensi, a titolo esemplificativo, all'archivio della polizia di Amburgo ove sono annotati dati di peso e sulla pelle delle persone al fine di identificare un guidatore d'auto o ancora i nuovi *laser scan* in grado di produrre una foto realistica che può essere utilizzata in giudizio e che rappresenta un cammino virtuale sulla scena del crimine[513].

Affinché la prova digitale possa essere acquisita al processo devono essere certi l'origine dei dati, i metodi di raccolta, di archiviazione e di analisi e tutti i soggetti coinvolti deve essere messo nelle condizioni di comprendere le tecniche utilizzate e di poterne valutare il grado di scientificità.

Le caratteristiche strutturali del processo penale europeo di tipo continentale sono il portato di un'adesione calibrata al modello accusatorio che coniuga la separazione delle fasi processuali e il metodo del contraddittorio con l'adozione di un principio dispositivo temperato e con l'attribuzione del potere di acquisizione della prova e di decisione al giudice togato.

Il sistema attuale mostra una sostanziale disomogeneità nell'analisi e nell'ammissibilità della prova digitale che ancora sconta un ritardo nella definizione e nella disciplina. Non ogni giudice, non ogni tribunale, anche all'interno della stessa nazione, acquisisce la prova digitale alle stesse condizioni e con gli stessi presupposti. Questo si riflette in una disparità del materiale probatorio in processi diversi e, quindi, in una differenza di elementi

[512] Si rinvia alla lettura del codice di procedura penale francese, consultabile liberamente nel web. Altre indicazioni sono state raccolte dalla relazione fatta da David Benichou in occasione dell'incontro di studi "*The use of new technologies in criminal proceedings*".

[513] Queste curiosità ed insieme tecnicismi della realtà tedesca sono stati riportati da Joackim Eckert nel seminario di studi di cui alla precedente nota.

valutativi a disposizione del giudice. La decisione finale, di conseguenza, potrebbe risultare fallace o comunque manchevole perché basata su elementi non genuini ovvero per l'assenza di elementi probatori di natura informatico-telematica.

Il problema dell'acquisizione della prova elettronica genuina non riguarda per ciò solo l'elemento che è stato raccolto da un'autorità investigativa territorialmente competente per la *notitia criminis*. Come si è già avuto modo di sottolineare[514], a motivo dell'espansione della criminalità transnazionale, la prova in generale e la prova digitale nello specifico costituiscono un important e oggetto di cooperazione e di circolazione delle informazioni non solo tra zone territorialmente distante del medesimo Stato, ma ancora di più tra diversi Paesi, siano essi membri dell'Unione europea o nazioni terze.

Questo nuovo paradigma di riferimento richiede un approccio ancora più complesso ed analitico rispetto al controllo sulla genuinità della prova digitale e sulla sua ammissibilità. Non è sufficiente valutare l'autenticità della prova sulla base delle sole modalità di raccolta e di archiviazione e sul metodo scientifico utilizzato e descritto da chi ha materialmente provveduto alla cristallizzazione dell'elemento probatorio.

L'idoneità gnoseologica della prova elettronica non può prescindere da una stima delle procedure e dei mezzi utilizzati per la sua trasmissione, quando provenga da uno Stato estero. È alto il rischio di corruzione, manipolazione, perdita dei dati nella fase di circolazione della *e-evidence* tale da dubitare della sua genuinità e dunque acquisibilità al processo, nel momento in cui giunge all'autorità straniera richiedente.

Queste problematiche scontano un grave ritardo normativo sia in sede nazionale sia in ambito comunitario.

Nell'ordinamento UE non troviamo delle disposizioni che regolano la prova digitale ed anzi la prima e unica legge di riferimento è la Convenzione di Budapest sul *cybercrime* del Consiglio d'Europa.

La Convenzione offre degli spunti di riferimento a cui si devono adattare gli Stati ratificatori del testo normativo, specie dal punto di vista delle procedure da seguire nella ricerca e nella raccolta della prova elettronica, di cui alla sezione 2[515].

Gli *standard* di salvaguardia e le condizioni genericamente indicate sono comunque soggette a modifiche ed implementazioni anche parziali in base alla normativa e alla tradizione giuridica nazionale.

---

[514] Il rinvio è a tutto il capitolo Seconda.

[515] Il testo della Convenzione di Budapest è consultabile al sito internet del Consiglio d'Europa (www.coe.int). In particolare gli articoli 20 e 21 della Convenzione si riferiscono, rispettivamente, alle intercettazioni informatico-telematiche e alla raccolta dei dati *real-time*.

L'Accordo di Budapest disciplina genericamente la preservazione dei dati, la loro produzione in base ad un ordine di un'autorità di *law enforcement*, la ricerca e il sezionamento dei dati raccolti, le intercettazioni e la raccolta di dati digitali *real-time* e le modalità di cooperazione internazionale, attraverso la previsione dell'estradizione (art. 24), della mutua assistenza (art. 25) e del trasferimento spontaneo di informazioni (art. 26).

Nessuna regola è prevista con riferimento all'acquisizione genuina di una prova digitale ma è rimessa ad ogni Stato la scelta delle modalità specifiche di svolgimento delle attività investigative legittimate dalla Convenzione e anche delle procedure di circolazione della *e-evidence* al fine della garanzia di autenticità.

L'ordinamento comunitario tuttavia ha più volte mostrato un interesse allo sviluppo di una regolamentazione della prova digitale sotto ogni profilo, dalla raccolta alla sua circolazione, secondo le forme più rapide ed efficienti di cooperazione di polizia e giudiziaria, mediante la trasmissione di dati e informazioni tra gli Stati UE[516].

In data 11 novembre 2009 è stato definito il Libro Verde della Commissione europea sulla ricerca della prova in materia penale tra gli Stati membri e sulla garanzia della loro ammissibilità[517]. Un testo che, partendo dalla necessità di agevolare la raccolta e la circolazione transfrontaliera della prova, si propone di consultare gli Stati sul tema per rafforzare la cooperazione.

Il Libro Verde si è occupato genericamente dell'istituto della prova penale, non senza fare riferimento alla Comunicazione della Commissione intitolata "*Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini*"[518] nella parte in cui prevedeva la realizzazione di un progetto di sviluppo della ricerca della prova transfrontaliera, con indicazione probabilistica di una normativa *ad hoc* della prova elettronica (mai concretizzatasi).

Le norme sull'acquisizione delle prove in materia penale vigenti nell'Unione appartengono a due categorie. Da un lato si distinguono strumenti basati sul principio dell'assistenza giudiziaria, come disciplinati dalla Convenzione europea di assistenza giudiziaria in materia penale, cui si aggiungono l'accordo di Schengen e la Convezione relativa all'assistenza giudiziaria in materia penale col relativo protocollo. Dall'altro si annoverano

[516] La normativa comunitaria, lo stesso Trattato di Lisbona ed il Programma di Stoccolma, ma non solo, sono l'immagine forte di un'Europa che vuole sviluppare la cooperazione, anche travalicando il sistema di assistenza reciproca per giungere al consolidamento del principio del mutuo riconoscimento, fondato su solide basi di fiducia reciproca e sulla prospettiva di un'armonizzazione delle legislazioni nazionali, almeno nei valori fondanti, attraverso l'individuazione della cd. norme minime.
[517] COM(2009) 624 definitivo.
[518] Comunicazione della Commissione al Parlamento e al Consiglio: COM(2009) 262 definitivo.

strumenti basati sul principio del reciproco riconoscimento, regolati dalla Decisione quadro relativa al mandato europeo di ricerca delle prove .

Gli strumenti di assistenza giudiziaria e i relativi protocolli riguardano la cooperazione in generale ma contengono anche alcune norme specifiche quali quelle sulle intercettazioni di comunicazioni e sull'uso delle videoconferenze[519].

Al fine di garantire l'ammissibilità della prova acquisita, le autorità dello Stato richiesto devono rispettare le formalità e le procedure indicate dalle autorità dello Stato richiedente, purché non siano contrarie ai principi fondamentali del diritto dello Stato richiesto.

In relazione al mandato europeo di ricerca della prova, le autorità dello Stato di emissione devono accertare l'ammissibilità della prova acquisita, in base alle norme del proprio diritto nazionale, nonché la necessarietà e proporzionalità rispetto al procedimento trattato.

Attualmente in ambito europeo coesistono strumenti di acquisizione della prova penale basati sull'assistenza giudiziaria con strumenti che realizzano il principio del reciproco riconoscimento. Questa impostazione può ingenerare confusione tra gli operatori del diritto che non sono sempre in grado di individuare lo strumento più adeguato da applicare per la prova ricercata. Tali fattori rischiano quindi di compromettere l'efficacia della cooperazione transfrontaliera. Inoltre gli strumenti basati sull'assistenza giudiziaria e non sul mutuo riconoscimento risultano molto macchinosi perché non sono basati su formulari *standard* per la richiesta.

Come si è già avuto modo di sottolineare[520], anche i *format* non risolvono completamente i problemi di dialogo tra le autorità e di interpretazione di quanto richiesto, non essendoci una base comune di valori e di istituti di riferimento tra gli Stati. Le procedure di mutuo riconoscimento, inoltre, sono limitate a determinate e specifiche tipologie di prove.

Il menzionato Libro Verde si è proposto di avanzare una consultazione tra gli Stati membri per cercare di avere un quadro sulla prova penale negli ordinamenti nazionali e valutare l'opportunità di introdurre uno strumento unico di mutuo riconoscimento che coinvolga ogni categoria di prova. L'attuazione di questa prospettiva di sviluppo è avvenuta per il tramite dell'iniziativa di creazione dell'Ordine d'Indagine Europeo che, ad oggi, non è ancora attuato[521].

---

[519] Per un approfondimento su questo sintetico riferimento al quadro di cooperazione e di ricerca della prova nell'Unione europea, si rinvia al capitolo I di questo lavoro.

[520] Il rinvio è al paragrafo 1 del Capitolo Terzo.

[521] Per un approfondimento sull'Ordine Investigativo Europeo come mezzo di cooperazione, si rinvia al Capitolo I, paragrafo 5.

L'ordine riguarderebbe quelle prove che – sebbene già esistano – non sono direttamente disponibili senza ulteriori indagini o esami, ad esempio analisi di oggetti, documenti o dati esistenti.

Questo elemento di novità e di rivoluzione nella prospettiva di agevolazione della cooperazione potrebbe costituire, una volta entrato in vigore, un mezzo essenziale per combattere la criminalità transnazionale.

Ad oggi il *considerandum* 14 dell'iniziativa sull'OEI e le disposizioni interne prevedono che per alcuni tipi di atti d'indagine, come il trasferimento temporaneo di persone detenute, l'audizione mediante videoconferenza o teleconferenza, l'acquisizione di informazioni su conti bancari o operazioni bancarie o le consegne controllate, sono necessarie disposizioni supplementari.

Si torna a ribadire che, anche rispetto alla prova digitale, sarebbe necessario prevedere un regime particolare di raccolta, archiviazione, circolazione e acquisizione.

Gli atti d'indagine che implicano l'acquisizione di prove in tempo reale, in modo continuo e per un tempo determinato sono coperti dall'OEI, ma è opportuno che all'autorità di esecuzione sia concessa flessibilità con riguardo a tali atti in considerazione delle differenze esistenti tra le legislazioni nazionali degli Stati membri.

Il diritto delle prove è un contenitore tanto vasto che racchiude in sé elementi molto diversi e ricchi di peculiarità che meriterebbero ciascuno un trattamento diversificato in relazione ad ogni categoria di prova, tenuto conto delle esigenze di prosecuzione, definizione del processo e non dispersione del materiale, ma anche delle garanzie dei diritti fondamentali, come enunciati nelle Carte europee e internazionali e dalle Corti.

Uno dei principi cardine che accomuna i sistemi europei si sostanzia nella presunzione d'innocenza.

L'intimo convincimento dell'organo giudicante si fonda sull'interpretazione dei fatti, in base alle prove acquisite al processo le quali, in quasi tutti i sistemi processuali penali europei[522], possono essere libere se pertinenti.

Si consideri inoltre che in Francia, così come in Inghilterra, non esiste un'interdizione totale all'utilizzo di prove ottenute illegalmente.

[522] Le diversità di sistema tra gli Stati membri in materia di prova sono visibili anche rispetto al principio di libertà della prova, se si considera che ordinamenti come quello olandese, all'art. 338 del codice di procedura penale, obbliga il giudice a fondare il suo convincimento su un sistema di "prova legale" (*wettige bewijsmiddelen*).
Per un approfondimento sulle procedure penali in Europa, si rinvia a M. DELMAS-MARTY *Procédures pénales d'Europe,* Press Universitaires de France, 1995.

3. *La circolazione di prova digitale: organi e soggetti legittimati*

Il ricorso all'assistenza giudiziaria non presenta in sé caratteri di illegittimità, poiché non esiste una norma che vieta alle autorità di un Paese di chiedere collaborazione a un altro Paese, indipendentemente dalle norme nazionali, comunitarie ed internazionale e agli eventuali accordi bilaterali o multilaterali stipulati a tale scopo [523].

Sulla circolazione della prova, in particolare, l'Unione europea si è dotata dello strumento di cooperazione del mandato europeo di ricerca della prova [524].

Questa procedura prevista dalla Decisione quadro adottata dal Consiglio G.A.I. dell'U.E. il 18 dicembre 2008, si fonda su un rapporto diretto tra autorità richiedente e autorità nazionale richiesta, senza precisare alcunché. Sussiste, dunque, un certo grado di discrezionalità da parte dello Stato membro per l'individuazione nella legislazione interna di recepimento degli organi competenti allo svolgimento di queste attività e dei requisiti dei soggetti coinvolti nell'esecuzione materiale del mandato di ricerca della prova.

Tale procedura è tesa ad integrare le disposizioni contenute nella Decisione quadro sulla esecuzione extraterritoriale dei provvedimenti – a carattere provvisorio – di blocco dei beni o di sequestro probatorio, adottata dal Consiglio dell'U.E. il 22 luglio 2003 (2003/577/GAI), costituendo un meccanismo unico, efficace e rapido per la ricerca delle prove "precostituite" ed il loro conseguente trasferimento allo Stato di emissione.

La Decisione quadro 2003/577/GAI, infatti, tende ad attuare il principio del reciproco riconoscimento in relazione alle decisioni giudiziarie volte a prevenire atti di distruzione, trasformazione, trasferimento o alienazione dei mezzi di prova, emesse in una fase d'urgenza, lasciando inevitabilmente scoperto il successivo trasferimento delle relative acquisizioni probatorie, ancora disciplinato formalmente dalle tradizionali procedure di assistenza giudiziaria.

I presupposti su cui si fonda il nuovo sistema di collaborazione tendono a delineare una nuova forma di assistenza *"non rogatoriale"*, direttamente instaurabile tra le diverse autorità giudiziarie interessate, con la tendenziale

[523] Si pensi che in Italia, la Corte di Cassazione, nella sentenza 20131 del 2 aprile 2009 ha affermato che "*in materia di rogatorie internazionali, ove lo Stato richiesto ecceda, nella concessione dell'assistenza, i limiti imposti a propria garanzia dalle convenzioni internazionali, nessuna nullità può essere eccepita da parte del soggetto avanti all'autorità giudiziaria italiana in ordine all'atto eseguito all'estero, poiché i limiti posti a garanzia della Stato riguardano esclusivamente i rapporti interstatali e, in mancanza di una esplicita previsione, non possono far sorgere diritti soggettivi in capo ai singoli all'interno dei rispettivi ordinamenti*".

[524] Sulla nozione e sul funzionamento del mandato europeo di ricerca della prova si rinvia al capitolo Primo.

scomparsa del ruolo di "filtro" delle autorità centrali, che viene limitato ormai ad una funzione di mero supporto tecnico-amministrativo.

In tal senso, l'art. 8, paragrafo 2, della Decisione quadro affianca all'ordinaria modalità di trasmissione diretta del mandato (ossia, direttamente tra l'autorità di emissione e quella di esecuzione, con ogni mezzo che consenta di conservare una traccia scritta in modo da stabilirne l'autenticità) la possibilità di affidare alle rispettive autorità centrali – se necessario, alla luce del tipo di organizzazione dell'ordinamento giudiziario interno – le attività di trasmissione e ricezione amministrativa del mandato e della relativa corrispondenza ufficiale.

Ripercorrendo uno schema definitorio già adottato in occasione dell'analogo strumento del mandato d'arresto europeo, anche il mandato europeo di ricerca delle prove costituisce una "decisione giudiziaria" circolante sul territorio dell'UE, alla quale le competenti autorità degli Stati membri debbono dare esecuzione in base al principio generale del reciproco riconoscimento e nel rispetto dei principi giuridici fondamentali sanciti dall'art. 6 TFUE.

Quello che muta, ovviamente, è la finalità dello strumento, orientato all'acquisizione di specifici elementi di prova ai fini del loro utilizzo nell'ambito di procedimenti penali avviati da un'autorità giudiziaria dello Stato di emissione, ovvero nell'ambito di procedimenti avviati da autorità amministrative in relazione a fatti comunque sanzionati dalla legislazione dello Stato di emissione, quando la decisione possa dare luogo ad un procedimento dinanzi ad un organo giurisdizionale competente in materia penale (*ex* art. 5 della Decisione quadro)[525].

Il limite del mandato europeo di ricerca della prova è rappresentato sicuramente dal suo ambito di applicazione circoscritto: esso non può riguardare le prove dichiarative, la prova scientifica, i risultati delle intercettazioni, i tabulati telefonici e telematici, per i quali dovranno continuare ad applicarsi i tradizionali strumenti di assistenza giudiziaria.

È significativo, peraltro, che il mandato europeo di ricerca delle prove, nonostante queste limitazioni di ordine generale, possa comunque essere emesso per l'acquisizione degli oggetti, dei documenti e dei dati sopra indicati, qualora gli stessi siano già in possesso dell'autorità di esecuzione prima dell'emissione dell'euromandato (art. 4, paragrafo 4).

Ciò a dire che, almeno parzialmente le autorità competenti per la richiesta e l'esecuzione del mandato sono coinvolte anche in riferimento alla prova digitale[526].

---

[525] Per un approfondimento sul Mandato europeo di ricerca della prova si rinvia a G. DE AMICIS I*l mandato europeo di ricerca della prova*, *op.cit.*

[526] Quanto alla nozione non istituzionalizzata di prova digitale si rinvia al capitolo Secondo.

Il mandato europeo di ricerca della prova legittima e regola i rapporti tra le competenti autorità giudiziarie degli Stati membri fatta salva la scelta, del tutto eventuale, della designazione di un'autorità centrale responsabile per le attività di trasmissione e ricezione del mandato, come anche della rispettiva corrispondenza ufficiale.

L'attività di trasmissione del mandato può essere agevolata dal ricorso ai punti di contatto della Rete Giudiziaria Europea (art. 8, paragrafi 3 e 4), al fine di ottenere le necessarie informazioni dallo Stato di esecuzione.

Il mandato europeo di ricerca della prova si affianca o concorre col regime tradizionale di cooperazione, basato sulla Convenzione europea di assistenza giudiziaria in materia penale del 29 maggio 2000, il quale, mediante lo strumento rogatoriale, coinvolge le autorità giudiziarie dei Paesi Parte [527].

Questo stato dei fatti potrebbe a breve assoggettarsi ad un nuovo ed innovativo regime, come ideato dall'iniziativa sull'ordine europeo d'indagine, che sostituirebbe le precedenti procedure di cooperazione in materia di prova, per giungere ad una piena attuazione del principio del mutuo riconoscimento in ambito UE. L'OEI, in base al testo degli atti preparatori attualmente redatti, coinvolge, quale "autorità richiedente", un giudice, un magistrato inquirente o un pubblico ministero competente nel caso interessato; o qualsiasi altra autorità giudiziaria definita dallo Stato di emissione che, nel caso specifico, agisca in qualità di autorità inquirente nei procedimenti penali e sia competente a disporre l'acquisizione di prove in base alla legislazione nazionale; come "autorità di esecuzione" indica un'autorità competente a riconoscere o a eseguire un OEI conformemente alla Direttiva.

Il testo ad oggi mutuato, pur nel suo carattere di non ufficialità, lascia ancora libero spazio di discrezionalità e si piega alle politiche di procedura penale che caratterizzano i diversi sistemi giuridici nazionali, nella consapevolezza delle differenze e peculiarità di ciascuno Stato.

Al fine di dare completezza e sistematicità alle procedure di cooperazione, con l'Azione Comune 96/277/GAI del 22 aprile 1996 è stata istituita la figura del Magistrato di Collegamento per agevolare i rapporti tra le autorità giudiziarie nazionali e per far sì che i risultati dell'attività compiuta

[527] Con l'azione comune 98/427/GAI il Consiglio dell'Unione europea stabilì che tutti gli Stati membri avrebbero dovuto depositare presso il segretariato generale dello stesso Consiglio una cosiddetta dichiarazione sulla buona prassi nell'assistenza giudiziaria in materia penale, indicando le modalità, ispirate a criteri di celerità ed efficienza, che ciascuno Stato si sarebbe obbligato a rispettare nel dare esecuzione alle domande di assistenza giudiziaria. L'Italia ha depositato la sua dichiarazione sulla buona prassi indicando per le richieste di rogatoria provenienti dall'estero, il Ministero della giustizia si è impegnato a garantire un inoltro celere a tutte le commissioni rogatoriali. È previsto che il Ministero debba invitare il procuratore generale presso la competente corte d'appello ed il giudice delegato per l'esecuzione a dare tempestiva informazione anche telefonica all'autorità straniera.

possano essere utilizzati nel procedimento penale dello Stato richiedente [528]. Il Magistrato di Collegamento é inserito nella struttura organizzativa del Ministero della Giustizia del Paese destinatario [529].

Anche l'istituzione della Rete Giudiziaria Europea (più nota come EJN – *European Judicial Network*) con l'azione comune 98/428/GAI del 29 giugno 1998 ha lo scopo di agevolare la cooperazione giudiziaria internazionale. Questo *network*, facente capo ad uno o più soggetti che conoscano sufficientemente almeno una lingua dell'Unione europea diversa dalla propria lingua nazionale, fornisce informazioni di ordine giuridico o pratico riguardo il sistema giudiziario comunitario o degli Stati membri[530].

Il ruolo assunto da Eurojust è centrale per una più efficace circolazione della prova. Questo Organo si compone di tante unità quanti sono gli Stati dell'UE, i cui membri sono scelti possibilmente tra i magistrati (siano essi giudici o magistrati del pubblico ministero) o tra i funzionari di polizia. Tali componenti sono riuniti in collegi, all'interno dei quale è scelto un Presidente affiancato da un Segretario diretto da un funzionario amministrativo [531].

Sono previste delle attività di cooperazione o di semplice collaborazione tra Eurojust, Europol ed Olaf.

Anche Olaf, pur nella sua natura di organo tipicamente amministrativo, per mezzo dei suoi funzionari, rappresenta una pedina importante nello scacchiere europeo della lotta alla criminalità e della cooperazione transnazionale, mediante indagini e trasferimento di dati.

Quanto all'Europol, Ufficio europeo di polizia, occupandosi principalmente di effettuare e coordinare operazioni investigative congiunte tra i corpi di polizia di due o più Stati dell'Unione, nutre e sviluppa la circolazione di dati, informazioni e prove. Ogni Paese ha una sua unità nazionale che rappresenta l'unico organo di collegamento tra Europol e i

---

[528] L'Italia ha avviato programmi per l'attuazione di tale forma di collegamento con la Francia, la Spagna ed il Regno Unito.

[529] Per un approfondimento sull'istituzione, il ruolo ed il funzionamento dei magistrati di collegamento si rinvia a E. APRILE, *op.cit*. pagg. 37 ss.

[530] In tema, E. SELVAGGI *La rete giudiziaria europea: uno strumento per migliorare la cooperazione giudiziaria in materia penale* in *Doc.giust*., 2000, pagg. 1123 ss.; P.L.M. DELL'OSSO *Rapporto sulla rete giudiziaria europea* in *Riv.it. dir.proc.pen*., 2005, pagg. 1540 ss.

[531] L'Italia ha dato attuazione alla decisione del Consiglio dell'unione del 2002 con la legge 14 marzo 2005 n. 41, secondo cui il membro nazionale italiano distaccato presso Eurojust viene nominato – con un mandato di quattro anni, prorogabile di due – con decreto del ministro della giustizia e scelto tra i giudici o i magistrati del pubblico ministero che esercitano funzioni giudiziarie o che si trovino temporaneamente collocati fuori ruoli, ma che abbiano almeno vent'anni di anzianità di servizio. La scelta viene effettuata in base ad una lista di candidati sui quali esprime la sua valutazione il Consiglio Superiore della Magistratura.
Per un approfondimento sui contenuti della menzionata legge italiana si veda G. DE AMICIS – G. SANTALUCIA *L'attuazione di Eurojust nell'ordinamento italiano: prime riflessioni sulla legge 14 marzo 2005, n. 41* in *Cass.pen*., 2005, pagg. 726 ss.

servizi nazionali competenti. Ciascuna unità nazionale invia all'Europol uno o più ufficiali di collegamento, in base a quanto deciso all'unanimità dal Consiglio di Amministrazione. Oltre agli organi di natura e ruolo finanziario (il controllore finanziario e il comitato finanziario), Europol è costituito al Consiglio di amministrazione, composto da un membro per ciascuno Stato UE, guidato da un Direttore, il quale esplica il suo ruolo nello svolgimento delle funzioni proprie di Europol.[532]

Nell'ambito della cooperazione di polizia, per far fronte all'internazionalizzazione del crimine, è stata costituita l'Organizzazione Internazionale di Polizia Criminale, meglio nota come Interpol la quale, per lo svolgimento del suo ruolo di agevolazione della mutua assistenza tra Autorità di polizia, è composta da un'organizzazione centrale e da una periferica[533]. Interpol svolge un ruolo di rilievo specie nelle richieste di rogatoria internazionale, laddove l'autorità giudiziaria nazionale competente, ai sensi dell'art. 15 della Convenzione del 1959 può, nei casi d'urgenza, trasmettere queste richieste direttamente all'autorità giudiziaria richiesta, mediante il servizio Interpol[534].

Anche la previsione della costituzione delle squadre investigative comuni (JIT – *Joint Investigation Team*) rappresenta un valido strumento di sviluppo della cooperazione extraterritoriale da parte delle autorità nazionali.

In base alla Decisione quadro del Consiglio dell'Unione del 13 giugno 2002, le suddette squadre sono costituite, di comune accordo dalle autorità competenti di due o più Stati membri, individuate dai rispettivi governi nazionali. Della squadra comune possono far parte non solo i rappresentanti degli Stati membri interessati, ma anche terzi soggetti, e segnatamente, funzionari di organismi istituiti ai sensi del Trattato sull'Unione europea. I soggetti che ne fanno parte, ovvero funzionari di polizia e/o pubblici ministeri, sono guidati da un Direttore della squadra. Gli agenti cd. distaccati potranno essere incaricati dell'esecuzione di alcune attività specifiche su mandato ufficiale del Direttore[535].

---

[532] Eurojust, Europol ed Olaf hanno stabilito la possibilità di realizzare delle forme reciproche di cooperazione o collaborazione con un comune *Memorandum of Undrstanding* sottoscritto da tutti e tre gli organi nel 2003.
Per un approfondimento si rinvia a F. PRATO *I rapporti di Eurojust con Europol, Olaf e gli Stati terzi* in www.cosmag.it (sito consultato il 10 febbraio 2010).

[533] In Italia il servizio Interpol ha una composizione interforze, essendo composta da personale appartenente all'Arma dei Carabinieri, alla Guardia di Finanza e alla Polizia di Stato.

[534] Per un approfondimento sulle funzioni, gli scopi ed i mezzi utilizzati da Interpol nello svolgimento delle sue funzioni, si rinvia al capitolo Primo.

[535] Di rilievo l'esempio del funzionamento delle squadre investigative comuni, costituite in base all'Accordo italo-svizzero concluso a Roma il 10 settembre 1998 ed in particolare della previsione di cui all'art. 22 laddove è data la possibilità di una più stretta collaborazione tra le autorità giudiziarie dei due

Il quadro dei soggetti ed organi legittimati ed interessati dall'attività di circolazione della prova potrebbe trovare una cornice ideale con l'auspicata istituzione della Procura europea e, dunque, della figura del Pubblico Ministero europeo[536]. Il *Corpus Juris*[537] ne prevedeva già la costituzione ed il Libro verde sulla tutela penale degli interessi finanziari[538] ne fa menzione. La Procura europeo dovrebbe essere costituita da un ufficio centrale, con sede a Bruxelles e facente capo ad un procuratore generale europeo con poteri di avocazione, e da una serie di uffici periferici, siti nelle capitali degli Stati membri dell'Unione europea, in cui operano altrettanti procuratori europei a cui il procuratore generale può delegare le sue funzioni. I membri saranno nominati dal Parlamento europeo: il procuratore generale verrà nominato su proposta della Commissione, i procuratori delegati su proposta degli Stati membri.

A causa della complessità di concetto ed applicazione delle procedure di circolazione della prova, anche gli organi e soggetti coinvolti sono scelti in base a determinate caratteristiche personali o funzionali, previste dalla normativa comunitaria oppure con vaglio di discrezionalità lasciato a ciascuno Stato membro, in base al proprio sistema.

Stati, e anche delle autorità di polizia se è volontà delle Parti, operando congiuntamente in seno a gruppi di indagine comuni, previa informazione al Ministero di Giustizia.
Sul tema delle squadre investigative comuni e del ruolo nelle procedure della cooperazione di polizia, si rinvia al capitolo Primo.

[536] La previsione dell'istituzione di una Procura europea trova formulazione all'art. 86 TFUE.

[537] Il *Corpus juris* è stato redatto da un gruppo di esperti, presieduto dalla prof.ssa Mareille Delmas Marty, nominati dalla Commissione e varato in una prima formulazione nel 1997 e poi integrato nel 2000 (con la cosiddetta "versione di Firenze" o *Corpus Juris* 2000). Pur trattandosi di testo privo di rilevanza giuridica, in quanto non recepito in alcun testo vincolante dell'Unione (benché richiamato in diverse risoluzioni del Parlamento europeo), il *Corpus juris* costituisce ancora oggi un punto di riferimento importante, come prima bozza di un codice penale e di procedura penale europeo. Il *corpus juris* è composto da due sezioni: una di diritto penale sostanziale e una contenente delle disposizioni di carattere processuale. In questa seconda parte, preliminarmente il territorio di tutti gli Stati membri dell'Unione europea è considerato, ai fini della competenza penale, come uno spazio unico, denominato "spazio giudiziario europeo". E' prevista l'istituzione di un Pubblico Ministero europeo, l'affermazione di un doppio grado di giurisdizione di merito, la garanzia del diritto al silenzio e del principio del contraddittorio, in tema di prova è enunciato il principio della presunzione d'innocenza e di utilizzabilità del risultato di prova, intesa come legalità della sua assunzione, che diviene oggetto di valutazione secondo le norme dell'ordinamento giuridico del paese nel quale la prova è stata assunta.
Sul tema, si veda AA.VV. *Corpus juris, pubblico ministero europeo e cooperazione internazionale,* Giuffré, 2003; AA.VV. *Il corpus juris* 2000. Un modello di tutela penale dei beni giuridici comunitari, Giuffré, 2003.

[538] COM 2003/128 definitivo testo nel quale sono stati meglio definiti i contorni degli illeciti penali di cui la Procura europea si dovrebbe si dovrebbe occupare e taluni aspetti riguardanti lo status giuridico e la relativa struttura organizzativa.
Per un approfondimento ed una interessante visione trasversale dell'istituzione della Procura europea relativamente allo sviluppo dei rapporti con la difesa, si rinvia a AA.VV. *Il difensore e il pubblico ministero europeo* (a cura di A. LANZI – F. RUGGIERI – L. CAMALDO), Cedam, 2002.

Le autorità giudiziarie e di polizia, in prima persona, costituiscono, giustamente, i principali attori della circolazione della prova poiché da costoro é raccolta, archiviata e utilizzata per i fini di una decisione.

L'importanza e la delicatezza di queste operazioni meriterebbe tuttavia un maggior rigore nella selezione dei soggetti da coinvolgere, anche all'interno di organi che, a livello di presupposti di conoscenza, sono da ritenere funzionalmente idonei. Questo vale ancora di più in rapporto con la prova digitale per il suo carattere intrinseco di novità, manipolabilità e volatilità.

Invece, ad oggi non sono previsti dei percorsi formativi particolari per il personale coinvolto in queste procedure, indipendentemente dallo *status* di magistrato o di membro di un'autorità di polizia.

L'attività di cui trattasi può sembrare, dalla sola valutazione delle procedure, tanto semplice da potere essere esplicata senza troppe difficoltà e senza la necessità di un precedente iter formativo specifico.

Invero, le sole difficoltà di dialogo tra Stati diversi, le differenze di sistema processuale e del diritto delle prove, del modo e del grado di garanzia dei diritti fondamentali, richiedono certamente una conoscenza approfondita delle normative che governano queste procedure, anche al fine di un vaglio di legittimità preliminare delle richieste e per la corretta individuazione del materiale ricercato.

Si noti che nella Decisione quadro 2008/978 sul mandato europea di ricerca della prova e nel formulario allegato, è richiesto che lo Stato di emissione garantisca la correttezza dei dati e delle informazioni indicate nel *format* e che siano rispettate le condizioni generali previste dall'art. 7 e dal *considerandum* 11, ovvero la proporzionalità del tipo di prova richiesto, un'analoga possibilità di acquisizione della prova secondo le proprie regole nazionali. Sul versante passivo della procedura, invece, in base al *considerandum* 12, l'autorità d'esecuzione è tenuta soltanto a ricorrere ai mezzi "*meno intrusivi possibili*" per acquisire gli oggetti, i documenti e i dati ricercati. Non sono previsti degli ordini vincolanti per l'acquisizione e per la garanzia del trasferimento di una prova, mantenendone il grado di autenticità originario[539].

Qualsiasi problema legato alla trasmissione o alla genuinità di un documento è affrontato direttamente tra le autorità, al più, se necessario, mediante l'intervento dell'autorità centrale, per facilitare la comunicazione e la comprensione reciproche.

Le perplessità sono amplificate nel trattamento della prova digitale, poiché richiede un'attenzione ancora più peculiare e specifica, oltre a un elevato grado di tecnicismo per comprendere se e come far circolare tale

[539] Le stesse condizioni sono ribadite anche nel testo attuale dell'iniziativa sull'Ordine d'Indagine Europeo.

tipologia di prova, rispettando un corretto bilanciamento tra esigenze contrapposte e garantendo la conservazione del grado di attendibilità [540].

Il diverso grado di coinvolgimento di organi e soggetti nelle procedure di circolazione della prova digitale in particolare, dipendono, in base ad un primo rilievo, dal fatto per cui si procede, dalla tipologia di reato, dalla pluralità di ambiti ontologici coinvolti[541].

La scelta del personale coinvolto deve essere ponderata anche sulla base del sistema di cooperazione informativa utilizzato, ovvero nel rapporto tra un sistema centralizzato ove la procedura di circolazione della prova si realizza nel concreto tramite l'intervento delle autorità centrali e il sistema basato sul principio di disponibilità, cioè di accesso diretto mediante un dialogo ed un interscambio tra le autorità coinvolte[542].

4. *La circolazione dei dati e la struttura delle banche di raccolta. Dal sistema centralizzato al principio di domanda diretta nel iure condito comunitario: una svolta nella cooperazione informativa*

La mutata competenza delle norme comunitarie, in grado di incidere anche sulla materia penale, e la necessità di sviluppo delle procedure di cooperazione giudiziaria e di polizia, ha portato all'incremento del numero delle banche dati UE (la quali hanno, in taluni casi, un omologo negli Stati membri).

Per lungo tempo, la ritrosia ed insieme la gelosia dei legislatori nazionali ha creato un ostacolo alla libera e rapida circolazione dei dati e alla nascita di meccanismi collaborativi a cui non è più possibile rinunciare.

L'istituzionalizzazione della cooperazione in materia penale nel Terzo Pilastro dell'Unione ha portato i primi risultati, grazie all'impiego di procedure, comunque vetuste ed insufficienti, tipiche del diritto internazionale e modellate sulle Convenzioni elaborate in seno al Consiglio d'Europa.

---

[540] Questo, ad avviso di chi scrive, non vale soltanto per la prova digitale ma per varie categorie di prove che, per la complessità, per il particolare grado di sensibilità dei dati, per il tecnicismo ontologico ovvero per il rischio elevato di inquinamento, dispersione o distruzione, richiede delle professionalità superiori alla media di soggetti che già, per titoli acquisiti, si ritengono idonei *per tabulas*.

[541] Si pensi, in particolare, alla complessità del fatto e al grado di plurioffensività del reato, come può accadere per i cd. *serious crimes* che, a differenza di altre fattispecie penali transnazionali di minore allarme sociale, coinvolgono una pluralità di organi e soggetti per le attività di prevenzione e repressione.

[542] Il modello di scambio d'informazioni secondo il principio di disponibilità è in via di sviluppo nell'ordinamento comunitario, quale strumento verso una piena attuazione del mutuo riconoscimento.
Sul principio di disponibilità si veda AA.VV. *Cooperazione informativa e giustizia penale nell'Unione europea*, *op.cit*.

L'inefficacia di questi strumenti di cooperazione, lo sviluppo di forme di criminalità transfrontaliera a seguito della creazione di uno spazio comunitario senza frontiere, ha portato dapprima ad un rafforzamento dei meccanismi cooperativi di carattere intergovernativo e poi allo sviluppo di procedure comunitarizzati[543].

L'importanza del sistema di banche di raccolta di dati e lo sviluppo della cooperazione informativa sono attestate non solo dal numero sempre crescente, dalle dotazioni degli organi comunitari per la cooperazione[544] e dalla emanazione di disposizioni che ne regolano il funzionamento, le modalità d'accesso, l'archiviazione dei dati.

Il rilancio dell'integrazione europea prende le mosse dalla fiducia reciproca tra gli Stati ma anche dalle politiche di rafforzamento della sicurezza interna ed esterna dell'Unione europea che possono essere agevolate da un sistema di scambio transnazionale di informazioni. [545]

Lo sviluppo tecnologico che caratterizza la società globalizzata ormai da alcuni lustri, ha facilitato lo sviluppo di tracce digitali, facilmente conservabili in archivi e banche dati informatiche, senza problema di spazi e volumi, e soggette al trasferimento per finalità di contrasto alla criminalità [546].

Sul piano del diritto comunitario, il tema dello scambio di informazioni tra le autorità di *law enforcement* era già stato affrontato a partire dagli Anni '90, tramite l'applicazione dell'accordo di Schengen del giugno 1990 che prevedeva l'istituzione di un Sistema di Informazione Schengen (SIS), anche ai fini dello

---

[543] *Ibidem*.

[544] Il riferimento, in particolare, è alle banche dati di Eurojust, Europol e Olaf.

[545] Sul punto si condivide il pensiero di L. HEMPEL – M. CARIUS – C. ILTEN *Exchange of information and data between law enforcement authorities within the European Union* in *www.statewatch.org/news/2009/apr/Study_Exchange%200f%20information%20and%20data%20between%20law%20lawenforcement%20authorities%20within%20the%20EU_EN.pdf* (consultato in data 30 novembre 2009).

[546] Il riferimento, per esigenze di circoscrizione dell'ambito di interesse della ricerca, è alle banche dati informatiche, senza affrontare l'opportunità ed insieme le problematiche connesse ad una possibile soluzione di gestione degli archivi di dati *on line*, secondo un modello *cloud* che meriterebbe una trattazione a sé stante.

Il "paradiso telematico" del *cloud computing*, di cui l'Unione europea si sta occupando da mesi, osservandone il crescente sviluppo e operatività, ad oggi è privo di una norma regolatrice specifica. Come si è avuto modo di osservare in occasione dell'intervento fatto al seminario di studi in tema di *cloud computing* e *privacy*, le banche dati UE contengono dati tanto importanti quanto sensibili che richiedono uno standard elevato di sicurezza nelle procedure di raccolta, archiviazione e trattamento. Pensare ad una possibile e futuribile gestione delle banche dati UE in un ambiente *cloud*, se da un lato potrebbe permettere un rapido accesso alle informazioni, da qualunque luogo ci si trovi, d'altro lato è ancora troppo vulnerabile, incontrollabile e troppo poco protetto per affidare dati dal carattere particolarmente sensibile.

Il menzionato convegno è stato organizzato nell'ambito del Progetto Winston Smith a Firenze, in data 3-4 giugno 2011, dal titolo "*e-privacy 2011. Cloud computing e privacy*". L'audio dell'intervento fatto in occasione di questo seminario si può ascoltare all'indirizzo internet: http://e-privacy.winstonsmith.org, nella sezione dedicata al 2011, accanto al nome Eleonora Colombo.

scambio spontaneo e diretto di dati tra le autorità di polizia[547]. A seguire è stato creato Europol, quale organo deputato all'agevolazione dello scambio di informazioni tra le autorità di polizia.

Successivamente, la materia della cooperazione informativa è stata inclusa nel testo della Convenzione sull'assistenza giudiziaria in materia penale (art. 7) e nella decisione istitutiva di Eurojust.

La vera svolta, tuttavia, si è attuata soltanto a seguito dell'allarme sociale diffuso dagli attentati terroristici dell'11 settembre 2001 e dagli attentati di Madrid e di Londra.

La centralità del ruolo della cooperazione informativa si è realizzata più compiutamente con il Programma dell'Aia del 2005[548], più precisamente per il tramite del progetto per la realizzazione del principio di disponibilità delle informazioni e per lo scambio di informazioni di *law enforcement* tra le autorità di polizia.

La cooperazione informativa si caratterizza per un modello centralizzato di stampo comunitario, il quale è imperniato su banche dati europee centralizzate, gestite da un organismo sovranazionale: si pensi al SIS e SIS II, al SID, al TECS di Europol, all'EPOC-III di Eurojust.

Il Consiglio europeo ha investito nello sviluppo dei sistemi informativi centralizzati, in particolare mediante l'attuazione del sistema di informazione sui visti (VIS), con l'incorporazione dei dati biometrici e la massimizzazione dell'efficacia di questo stesso sistema, del SIS II e di Eurodac, secondo un programma di reciproca interoperabilità.

La Comunicazione del Consiglio alla Commissione e al Parlamento europeo per l'incremento dell'efficacia e lo sviluppo dell'interoperabilità delle banche dati UE per i fini di sicurezza interna del 2005, definisce questa come l'abilità di un sistema informatico di supportare lo scambio dei dati e rendere possibile la conoscenza e la circolazione delle informazioni[549]. Il concetto di interoperabilità ha un valore anche di scelta politica e non di scelta meramente tecnica come, più cautamente, la Commissione ha dichiarato nella menzionata Comunicazione[550].

L'adeguamento del funzionamento delle banche dati al principio di interoperabilità non deve comunque compromettere la garanzia del diritto alla *privacy* e dovrebbe legittimare l'accesso soltanto agli organi competenti, per

[547] Il riferimento è agli artt. 39 e 46.
[548] Il Programma dell'Aia è stato pubblicato in GUUE, C 53, 3 marzo 2005, pagg. 1 ss.
[549] Per un approfondimento sul testo della Comunicazione e sul tema dell'interoperabilità di sistema, si rinvia a P. DE HERT – S. GUTWIRTH *Interoperability of police databases within the EU: an accountable political choice?* in *http://ssrn.com/abstract=971855* (consultato in data 15 gennaio 2011).
[550] Il sistema di interoperabilità tra le banche dati, in realtà non rappresenta nulla di nuovo ma semplicemente un'applicazione più estesa di quanto era già stato proposto in Germania nel 1977 da Herold per agevolare lo scambio di informazioni tra autorità di polizia e pubblici ministeri.

finalità predefinite e nei soli casi in cui ciò coadiuvi il buon funzionamento della giustizia.

Ogni sistema di archiviazione e trattamento di dati necessiterebbe di una revisione della disciplina per ragioni di coerenza con le disposizioni della Direttiva comunitaria 95/46/CE[551] e della Convenzione europea dei Diritti dell'Uomo.

La seconda direttrice fondamentale di profilo dinamico della cooperazione informativa coincide con il riconoscimento esplicito del principio di disponibilità, riconducibile alla stessa matrice del principio di mutuo riconoscimento che rappresenta la più grande sfida dell'Europa contemporanea.

Un ulteriore aspetto del principio di accessibilità, già abbozzato con il Programma dell'Aia, è rappresentato dalla possibilità di acquisire informazioni contenute in *databases* centralizzati, istituiti per finalità di sicurezza o per finalità miste.

Il Consiglio ha approvato molteplici strumenti normativi diretti a concretizzare il canone della libera circolazione delle informazioni. Con particolare riguardo alle attività del Terzo Pilastro, il testo cardine è delineato dalla Decisione quadro 2006/960/GAI sulla disponibilità delle informazioni; il regolamento CE n. 1987/2006 del Parlamento europeo e del Consiglio sull'istituzione, l'esercizio e l'uso del sistema Schengen di seconda generazione (SIS II) e la parallela Decisione 2007/533/GAI; il Regolamento CE 767/2008, concernente il sistema di informazione visti e lo scambio di dati tra Stati membri sui soggiorni di breve durata; la Decisione 2008/633/GAI sulla consultazione del VIS da parte degli organi legittimati degli Stati membri e da parte di Europol; la Decisione 2008/615/GAI sul potenziamento della cooperazione transfrontaliera, in particolare per la lotta al terrorismo e alla criminalità transfrontaliera e la contestuale Decisione 2008/616/GAI, volta a stabilire le disposizioni amministrative e tecniche necessarie all'attuazione della decisione 2008/615/GAI, in particolare per regolare lo scambio automatizzato di dati del DNA[552], di dati dattiloscopici e di dati di

[551] Si ricorda che le limitazioni al campo di applicazione delle norme della cd. Direttiva *Privacy* non permetteva che fosse vincolante anche per le attività di quello che era il Terzo Pilastro dell'Unione europea, prima dell'avvento della novella di sistema con l'entrata in vigore del Trattato di Lisbona.

[552] La circolazione della prova genetica richiede particolare rigore per la particolare sensibilità del dato trattato.
Nel giugno del 1997 venne fatta la scelta politica d'istituire una banca dati del DNA pan-europea, contenente i profili di persone condannate per reati di abuso sessuale su bambini, con l'intento di velocizzare l'omologazione e la standardizzazione delle tecniche di rilevazione del DNA. Nel 2001 fu fissato uno standard europeo, poi recepito da una Risoluzione del Consiglio europeo del 25 giugno 2001.
Da un approccio comparatistico tra i diversi sistemi nazionali di acquisizione e analisi del DNA emergono differenze tali che non consentono l'istituzione di una banca dati europea.

immatricolazione dei veicoli; la Decisione quadro 2008/876/GAI sul mutuo riconoscimento delle decisioni penali; la Decisione quadro 2008/977/GAI sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale; la Decisione quadro 2009/315/GAI, relativa all'organizzazione e al contenuto dello scambio fra gli Stati membri di informazioni estratte dal casellario giudiziario e la Decisione 2009/316/GAI che istituisce il sistema europeo di informazione sui casellari giudiziari (ECRIS)[553].

La politica dell'*information sharing* coinvolge trasversalmente una pluralità di organi, come l'Interpol, e di materie, come la Convenzione ONU contro il crimine organizzato transnazionale (meglio nota come Convenzione di

---

Al di là dei possibili sviluppi futuri, ad oggi la cooperazione internazionale resta limitata al Gruppo Europeo dei Profili di DNA (EDNAP) e alla Rete Europea degli Istituti di Scienze Forensi.
Lo scambio tradizionale di dati riguardanti il DNA è supportato da Europol e dal suo archivio, nonché dalla banca dati di Interpol.
La circolazione delle informazioni, dunque, avviene sostanzialmente per il tramite di un'autorità centrale la quale può stabilire particolari condizioni di accesso a livello transnazionale, rendendo così, di fatto, tali procedure complesse ed inefficaci.
Su invito espresso già nel Programma dell'Aia, ai sensi dell'Allegato II della Proposta di Decisione quadro del Consiglio europeo sullo scambio d'informazioni, in virtù del principio di disponibilità, possono essere ottenuti, alle condizioni previste nella suddetta Decisione, fra l'altro, profili di DNA. Conseguentemente il Consiglio europeo invitava la Commissione a presentare, entro la fine del 2005, proposte volte ad attuare il principio di disponibilità. Si precisava che lo scambio d'informazioni sarebbe dovuto avvenire secondo le più innovative tecnologie, tenendo conto della diversa tipologia dei dati, tramite l'accesso reciproco o l'interoperabilità di base di dati nazionali, oppure l'accesso diretto (on line), anche tramite le basi di Europol e del SIS.
Per un approfondimento si rinvia a C. FANUELE op.cit.; S. CAMERON *California's DNA databank joins the modern trend of expansion* in *Mc George Law Rieview*, 219, 2002.

[553] Un problema ancora diverso è quello che riguardo il profilo statico della cooperazione informativa, cioè il principio di conservazione dei dati che, come comprensibile, è direttamente connesso alla possibilità di scambio.
L'attività normativa dell'Unione in materia si è tradotta in alcuni casi nell'introduzione di specifici obblighi di conservazione per gli Stati membri, in altri casi si è configurata come diretta a garantire l'uniformità delle scelte già operate dai singoli ordinamenti giuridici nazionali.
E' significativa sul punto la decisione 2008/615/GAI che, nel recepire i contenuti del Trattato di Prum, non implementa solo il canone di disponibilità con riguardo ai dati genetici e biometrici, ma prescrive a monte che gli Stati membri si impegnino a creare e gestire schedari nazionali di analisi del DNA per le indagini penali (art. 1). Altrettanto rilevante la decisione quadro 2009/315/GAI, relativa all'organizzazione e al contenuto delle informazioni estratte dal casellario giudiziario, che prevede l'obbligo per lo Stato di cittadinanza del condannato di conservare integralmente le informazioni trasmesse dallo Stato di condanna.
Sempre in materia di conservazione dei dati, rilevano sia la direttiva 2004/82/CE del Consiglio con la previsione che gli Stati membri dovessero prescrivere ai vettori aerei di comunicare le informazioni anticipate sui passeggeri (*Advance Passenger Information* – API) per la lotte all'immigrazione clandestina e la proposta di decisione quadro sull'uso dei dati del codice di prenotazione (*Passenger Name Record* – PNR) nelle attività di contrasto (COM (2007) 654 definitivo).
Altro ambito d'intervento dell'Unione sul *data retention* riguarda i dati generati dalle comunicazioni elettroniche, in particolare con riferimento alla proposta di direttiva del Parlamento europeo e del Consiglio COM (2005) 438 definitivo, che modifica la direttiva 2002/58/CE.

Palermo del 15 novembre 2000), insieme ai tre Protocolli allegati[554], nonché la Convenzione del Consiglio d'Europa sulla criminalità informatica (cd. Convenzione di Budapest del 23 novembre 2001). Il denominatore comune è rappresentato dalla condivisione di *law enforcement informations*.

Dal punto di vista strettamente individualistico, questo approccio si scontra con l'interesse del singolo a mantenere la propria *privacy* o, almeno, ad essere informato della raccolta dei dati, con possibilità di accedervi per verificare la completezza e la correttezza, sollecitando l'eventuale rettifica, modifica, aggiornamento o cancellazione.

Percorrendo le linee di sviluppo della cooperazione informativa, il modello offerto da TECS di Europol, dall'EPOC-III di Eurojust, dal SIS e dal SIS II e dal SID è, in estrema sintesi, raffigurabile tramite una struttura radiale, organizzata intorno ad una banca dati centrale (gestita, sia pure con modalità e obiettivi a volte diversi, da organismi sovranazionali[555]) collegata a plurime unità nazionali, dislocate nei singoli Paesi UE[556].

Accanto a queste forme di cooperazione accentrata, si può collocare un secondo e diverso paradigma, ispirato alla logica di agevolazione della maggiore diffusività, cioè di scambio o accesso immediato ai dati.

La strategia della condivisione capillare di *law enforcement informations* è già rintracciabile, seppure in nuce, nella Convenzione sull'assistenza giudiziaria in materia penale del 20 maggio 2009, adottata dal Consiglio dell'Unione col dichiarato intento di sviluppare le modalità cooperative delineate dalla Convenzione di Strasburgo del 20 aprile 1959.

Il principio trova poi affermazione nel Programma dell'Aia, la cui terza parte è riservata specificamente al rafforzamento della sicurezza e, in particolare, alla prospettiva di miglioramento dello scambio di informazioni. Lo stesso Programma sancisce che lo scambio di informazioni dovrebbe avvenire attraverso l'accesso reciproco o l'interoperabilità di basi di dati nazionali, mentre, solo in alternativa, è contemplato l'accesso diretto *on line* alle basi di dati centrali dell'UE già esistenti, quali il SIS. La creazione di nuove banche dati centralizzate a livello europeo viene subordinata all'elaborazione di studi che ne dimostrino il valore aggiunto.

Meno esplicito il riferimento testuale all'interoperabilità fra i *database* nazionali.

---

[554] I protocolli allegati sono dedicati alla lotta contro la tratta delle persone, al traffico di migranti e a quello delle armi da fuoco.
Si ricorda che la Convenzione di Palermo è stata ratificata dall'Italia con legge 16 marzo 2006, n. 146.

[555] Europol e Eurojust rappresentano l'unità centrale del SIS e del SID (rispettivamente, C-SIS e C-SID).

[556] Nel caso di Eurojust, è il membro nazionale a raccogliere informazioni nel Paese d'origine per veicolarle all'Aia.

Il piano di azione del Programma dell'Aia, di cui alla Comunicazione del 10 maggio 2005 della Commissione al Consiglio e al Parlamento europeo[557], ha previsto, in uno spazio di libera circolazione, l'agevolazione delle procedure di scambio di informazioni, pur nel rispetto dei diritti fondamentali, in particolare del diritto alla *privacy* e alla tutela dei dati personali, da bilanciare col principio di disponibilità.

Su queste solide basi di principio sono state predisposte prima la proposta di Decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale[558] e poi la proposta di Decisione quadro relativa allo scambio di informazioni in virtù del principio di disponibilità[559].

Il testo della proposta 475 del 2005 si contraddistingue per l'area di applicazione allargata, tale da comprendere sia le autorità di polizia e doganali, sia le autorità giudiziarie. È chiaro, dunque, che nella sua innovatività questa Proposta si candida a pervadere trasversalmente l'ambito della cooperazione di polizia e della cooperazione giudiziaria in materia penale. Come chiarito dal *considerandum* 20, le disposizioni non si applicano, invece, al trattamento di dati personali effettuato dall'Ufficio europeo di Polizia (Europol), dall'Unità europea di cooperazione giudiziaria (Eurojust) e dal Sistema di Informazione delle Dogane (SID), in quanto i relativi circuiti informativi sono interessati da una disciplina *ad hoc*, a tutela dell'autodeterminazione informativa.

Gli Stati sono sollecitati a rispettare il principio di finalità limitata nelle operazioni di trattamento dei dati[560], a distinguere i dati in categorie, a secondo del grado di accuratezza del trattamento e di affidabilità delle fonti.

Queste indicazioni si coniugano perfettamente con la disciplina dello scambio *cross border* di informazioni, per cui è imposto agli Stati di provvedere ad un controllo preliminare sulla qualità dei dati personali, prima di procedere alla trasmissione o alla messa a disposizione.

Il principio di disponibilità potrà poi attuarsi mediante il meccanismo di domanda-risposta oppure dell'accesso immediato e diretto *on line*.

---

[557] COM (2005) 184 definitivo.
[558] COM (2005) 475 definitivo.
[559] COM (2005) 490 definitivo.
[560] Ai sensi dell'art. 2 lett. b) della proposta di decisione quadro 475/2005, per "*trattamento*" dei dati personali si intendono tutte le operazioni o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, in relazione ai dati in parola.
Quanto ai limiti di finalità, i dati devono essere rilevati per finalità determinate, esplicite e legittime, nonché, successivamente, trattati in modo non incompatibile con tali finalità. Dovranno, inoltre, risultare adeguati, pertinenti e non eccedenti rispetto alla finalità per le quali sono stati rilevati e trattati; dovranno sempre rispettare il carattere di correttezza e, quando necessario, dovranno essere aggiornati. In generale, le informazioni devono permettere di identificare chiaramente il soggetto interessato e devono essere conservati per un tempo congruo ed insieme limitato agli scopi rilevati.

Secondo un vaglio a posteriori, invece, lo Stato che ha già trasmesso o reso accessibili determinati dati, nel caso in cui accerti degli errori o delle imprecisioni nelle informazioni, deve informare immediatamente l'autorità ricevente e rendere disponibili i nuovi dati, invitando alla cancellazione o all'aggiornamento dei precedenti in base alle modifiche effettuate.

La Commissione, nella proposta di Decisione quadro, ha sposato la logica della differenziazione, per cui agli Stati membri è richiesto che i dati raccolti risultino chiaramente distinguibili in base allo *status* soggettivo degli interessati: sospettati, condannati e persone che danno adito a ritenere che commetteranno un reato[561].

Gli Stati membri sono chiamati a garantire che i dati personali raccolti e trattati non restino archiviati a tempo indeterminato, ma vengano cancellati se non sussistono i presupposti per la loro circolazione, se è trascorso un certo tempo massimo determinato dalle legislazioni nazionali, ovvero se sono venuti meno o sono stati già evasi gli scopi per cui erano stati acquisiti.

La Commissione precisa inoltre che ogni spostamento, ogni trasmissione ed ogni modifica del dato debba lasciare una traccia elettronica che permetta di rintracciarlo, correggerlo o cancellarlo in ogni momento[562].

Una serie di regole sono poi riservate a legittimare le ulteriori trasmissioni di dati, cioè quelle che intervengono tra l'originario istante-ricevente (che ora diviene trasmittente) e i nuovi interessati.

La Commissione europea è molto attenta a che i dati non siano esposti oltremodo al rischio di accessi indebiti, modifiche ad opera di soggetti non autorizzati e cancellazione non voluta.

Tutte le persone che operano in un'autorità di uno Stato membro competente per le attività di raccolta, archiviazione e trasmissione di dati e informazioni sono vincolato al rispetto della riservatezza.

La proposta di Decisione quadro della Commissione sullo scambio d'informazioni in virtù del principio di disponibilità prende corpo dall'analisi delle contingenze storiche di prevenzione e repressione dei reati di natura transnazionale nello spazio giudiziario UE[563].

Con questo testo, gli Stati membri sono chiamati a condividere tra loro e con Europol i dati, superando le barriere delle distanze fisiche.

---

[561] In questa categoria sono compresi tutti i soggetti che sono stati già raggiunti in passato da una *notitia criminis* a carico, soggetti ritenuti pericolosi e per i quali sussiste un sospetto che possano delinquere.
La locuzione utilizzata nel testo della proposta di decisione quadro, anche così inquadrata, desta perplessità per l'ambiguità espositiva e perché categorizza (e quasi stigmatizza) dei soggetti in base a dei labili sospetti.

[562] L'art. 10 della proposta di decisione quadro prevede che gli Stati assicurino la registrazione di qualsiasi trasmissione automatica di dati personali, specie se effettuata mediante l'accesso diretto, precisando i dati inoltrati, i motivi addotti, le autorità coinvolte, le persone che hanno collaborato allo svolgimento della procedura.

[563] COM (2005) 490 definitivo.

Più precisamente, il progetto intende garantire alle singole autorità nazionali di contrasto, oltreché ai funzionari di Europol, l'accesso alle informazioni di *law enforcement* detenute da altri Paesi, permettendone l'integrale consultazione *on line*, ovvero assicurando *on line* l'accesso ai soli dati di indice a cui potrà seguire una richiesta delle informazioni correlate, senza violare il diritto alla *privacy*.

La proposta in commento privilegia i canali diretti per lo scambio di informazioni e prevede un obbligo generale di *information sharing*, fatti salvi limitati motivi di rifiuto già tipizzati nel testo.

In base al *considerandum* 6, lo scambio di informazioni transfrontaliero è finalizzato tanto alla prevenzione del crimine, quanto all'individuazione e alla repressione dei reati "*prima che venga avviato il procedimento giudiziario*".

In questo modo sono escluse, dal punto di vista soggettivo, le autorità giudiziarie e, dal punto di vista funzionale, la fase processuale in senso stretto.

Da ciò si desume che, di regola, salvo espressa indicazione differente da parte dell'autorità giudiziaria, l'informazione ottenuta oltre confine sarà utilizzata più ai fini della prevenzione dei reati o per le operazioni d'*intelligence*[564] che non come prova nel corso del processo.

Una modalità alternativa per la circolazione delle informazioni è data dal sistema delle banche dati nazionali, contenenti informazioni accessibili *on line* dalle autorità di polizia degli Stati membri, da Europol ovvero dal sistema nazionale di circolazione delle informazioni, senza la previsione dell'accesso telematico diretto. In quest'ultima ipotesi sono accessibili *on line* soltanto i dati di indice relativi ai contenuti generali degli archivi, a cui potrà seguire il trasferimento dell'informazione a seguito di una richiesta espressa.

La contrapposizione che si genera dal rapporto tra questi due diversi sistemi di circolazione del dato è rappresentata dalla tensione tra *visibility* (nel caso di accesso al solo indice) e *readability* (nel caso di accesso diretto all'informazione).

La proposta di Decisione quadro 490/2005 si presenta, sotto questo aspetto, molto audace nel sostenere la prospettiva dell'accesso rispetto a quella della visibilità.

Meritano un giudizio positivo *in parte qua* anche gli accordi di Prum e la Decisione 2008/615/GAI[565], le quali prevedono la procedura di consultazione o comparazione dei dati per il tramite dei punti di contatto.

---

[564] Per le dovute puntualizzazioni su cosa si debba intendere con il concetto di *intelligence* nelle fonti europee si rinvia a M.L. DI BITONTO *Raccolta di informazioni e attività di intelligence* in R.E. KOSTORIS – R. ORLANDI (a cura di) *Contrasto al terrorismo interno e internazionale*, Giappichelli, 2006.

[565] Decisione quadro del 23 giugno 2008 sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera.

Il Trattato di Prum si contraddistingue per la previsione di una disponibilità selettiva di dati, ove cioè non siano visibili tutte le informazioni ma soltanto determinate categorie scelte. In questo caso, in particolare, l'attenzione è polarizzata sui profili di DNA, le impronte digitali e i dati attinenti i veicoli. Il Trattato contempla espressamente per i firmatari un obbligo di istituzione di tre banche dati centralizzate (a livello nazionale) ove sono archiviati tutti i menzionati tipi di dati, mentre l'iniziativa della Commissione affianca alla ricerca su archivi che raccolgono i *reference index*, la possibilità dell'accesso immediato *on line* alle informazioni disponibili.

La procedura di trasferimento transfrontaliero delle informazioni deve comunque rispettare le regole sulla protezione dei dati nei casi di trattamento automatizzato, secondo i criteri fissati dalla Convenzione del Consiglio d'Europa del 28 gennaio 1981, n. 108, che trovano diretta applicazione anche per gli archivi di Europol, Eurojust e SID.

Nel giugno del 2004 il Regno di Svezia ha previsto un'iniziativa[566] indirizzata a garantire lo scambio rapido di informazioni e d'*intelligence*, per la prevenzione dei reati o le indagini in materia criminale.

L'attenzione si concentra sulle autorità di polizia, senza escludere *in toto* le autorità giudiziarie.

Nell'iniziativa svedese è agevolato il principio di disponibilità dei dati, concedendo l'accesso alle autorità di contrasto straniere alle stesse condizioni delle autorità di contrasto nazionali, incentrato sul meccanismo della domanda e della risposta e non su quello dell'accesso *on line* delle informazioni.

L'art. 7 prevede che il flusso di informazioni e *intelligence* abbia luogo tramite gli uffici SIRENE, tramite uffici centrali o le unità nazionali di Europol o le unità N-SID, senza escludere qualsiasi alternativa stabilita con accordi bilaterali o multilaterali. L'ulteriore soluzione offerta si sostanzia nello scambio diretto tra autorità centrali o locali incaricate dell'applicazione della legge.

Nel dicembre 2006 è stato varato il testo della Decisione quadro sul principio di disponibilità[567], il quale, anche a causa delle contingenze storiche, ha ricevuto immediatamente un ampio consenso, pur riguardando una materia (quella delle operazioni di polizia e giudiziarie in materia penale) caratterizzata da un radicato sentimento di gelosia da parte degli Stati.

---

[566] L'iniziativa del Regno di Svezia è pubblicata in GUUE, C 281, 18 novembre 2004.

[567] Decisione quadro 2006/960/GAI, entrata in vigore il 30 dicembre 2006. In tema, merita attenzione il parere reso dal Garante europeo per la protezione dei dati del febbraio 2006 (pubblicato in GUUE, C 116, 17 maggio 2006) laddove chiamato ad esprimersi sull'allora proposta di decisione quadro, esordiva spiegando che la molteplicità di iniziative avanzate sconsigliava di esaminare quel testo in maniera isolata, dovendosi piuttosto tener conto dell'esistenza di altre strategie di avvicinamento al tema dello scambio di informazioni di *law enforcement* e, soprattutto, non potendosi trascurare le tendenze, già emerse in seno al Consiglio, a preferire queste ultime rispetto all'approccio generale della Commissione.

L'*incipit* della Decisione ribadisce che, per assicurare un maggiore grado di sicurezza dei cittadini dell'Unione europea, è necessario sviluppare una più stretta cooperazione fra le autorità degli Stati membri "*incaricate dell'applicazione della legge*".

Le informazioni ottenute in virtù del principio di disponibilità potranno essere utilizzate per attività di *intelligence* e nel corso delle indagini preliminari, mentre, per costituire una prova nel corso del processo è richiesto il ricorso agli strumenti tradizionali di cooperazione e, se del caso, il consenso dello Stato d'origine.

Per il Consiglio UE, il principio di disponibilità si esplica mediante la libera comunicazione di informazioni e *intelligence* alle autorità competenti di altri Stati membri, a condizioni non più rigorose di quelle applicabili a livello nazionale.

La Decisione quadro si basa sullo strumento della richiesta motivata. Lo scambio, in base all'art. 6 paragrafo 1, può avere luogo tramite qualsiasi canale esistente ai fini della cooperazione internazionale, avendo cura di coinvolgere anche Europol e Eurojust ogniqualvolta si tratti di un reato di loro competenza[568].

Le *Draft Guidelines* presidenziali dell'ottobre 2008 fanno riferimento, *claris verbis*, ai canali più importanti ai fini della *law enforcement cooperation,* quali *SIRENE; ENU/EUROPOL Liason Officer; INTERPOL NCB; Liason officers; Mutual Administrative International Customs Assistence (Naples II Convention); Bilateral Cooperation Channels*. Segue l'indicazione di una serie di criteri che devono essere seguiti al momento della scelta del canale più idoneo da utilizzare per l'obiettivo da raggiungere.

Questa politica di canalizzazione verso gli strumenti già esistenti, in base ad un meccanismo di domanda-risposta, enfatizza il ruolo dell'accesso reciproco o dell'interoperabilità tra le basi di dati nazionali, già insito nel Programma dell'Aia[569].

Elementi di novità nello scambio di informazioni e dati si trovano nel testo della Convenzione di Budapest del 2001 del Consiglio d'Europa, in particolare per i lavori delle reti di contatto, attive ventiquattrore su ventiquattro e sette giorni su sette, nel settore della criminalità ad alta

[568] Lo scambio di informazioni può avvenire anche spontaneamente, senza la necessità di alcuna richiesta preventiva, qualora sussistano ragioni di fatto per ritenere che i dati siano utili all'individuazione, alla prevenzione o all'indagine riguardanti i reati di cui all'art. 2, paragrafo 2, della decisione quadro 2002/584/GAI.

[569] Non si esclude che la scelta effettuata dal Consiglio sia stata dettata da un principio di economicità e risparmio di risorse, dato che il meccanismo di *hit/no hit* e il ricorso a SIS e SIS II, SID, Europol, Interpol evita agli Stati l'ingente investimento per costituire archivi di dati di indice e assicurare alle autorità di tutti i Paesi europei l'accesso diretto *on line* ai propri *database* nazionali, secondo il modello prospettato dalla Commissione nell'ottobre 2005.

tecnologia internazionale, a cui aderiscono molti Stati in tutto il mondo, tra i quali la maggiori parte degli Stati membri UE[570].

Accanto a questo efficace sistema per la trasmissione delle informazioni, la Convenzione prevede anche la possibilità degli Stati di scambiarsi dati spontaneamente e di poter acquisire dati in tempo reale[571].

L'Unione europea, e in particolare la Commissione, partecipa con interesse ai dibattiti sulla cooperazione internazionale, tra cui il G8, Gruppo Roma-Lione ,sulla criminalità ad alta tecnologia.

La rete G8 è un meccanismo che permette di accelerare i contatti tra gli Stati partecipanti, grazie a punti di contatto consultabili giorno e notte per casi implicanti la produzione di prove elettroniche o richiedenti l'assistenza urgente di autorità di contrasto straniere[572].

Lo sviluppo delle reti elettroniche di comunicazioni e dei sistemi di informazione e l'evoluzione da un sistema centralizzato nella prospettiva di accesso diretto, costituiscono un beneficio per i cittadini UE e per l'attuazione concreta di uno spazio di libertà, sicurezza e giustizia.

Tuttavia, per giungere ad un sistema efficiente ed efficace di scambio di informazioni sono necessari altri interventi normativi in gradi di far fronte alle minacce di attacchi intenzionali a questi sistemi, con tutti i rischi connessi alla sicurezza e alla *privacy*[573].

La Comunicazione della Commissione, COM(2010) 385 definitivo, sulla gestione delle informazioni in uno spazio di libertà, sicurezza e giustizia, auspica la creazione di un sistema di informazioni unico e globale a livello UE, con finalità multiple, che possa consentire la massima condivisione delle informazioni, non senza precisare che questo tipo di struttura potrebbe costituire una limitazione del diritto alla vita privata e alla protezione dei dati. Una gestione compartimentata, invece, come quella sviluppata negli ultimi decenni, è sicuramente meno efficace dal punto di vista della circolazione dei dati ma certamente più garantista dei diritti e delle libertà fondamentali dei cittadini.

Resta ancora incerto il destino della cooperazione informativa in ambito UE proprio a causa di questa irrisolta tensione tra l'interesse alla sicurezza e alla giustizia, nella prevenzione e repressione dei reati, e il diritto alla riservatezza della persona e dei suoi dati trattati.

---

[570] Il riferimento, in particolare, è all'articolo 35 della Convenzione del Consiglio d'Europa sulla cibercriminalità

[571] Il riferimento è agli articoli 20 e 26 della Convenzione di Budapest.

[572] Il progetto della rete del G8 Roma-Lione è riportato anche nella Comunicazione della Commissione al Parlamento europeo, al Consiglio e al Comitato delle Regioni "*Verso una politica generale di lotta contro la cibercriminalità*" (COM(2007) 267 definitivo).

[573] Questo concetto rappresenta l'incipit della proposta di decisione quadro del Consiglio europeo relativa agli attacchi contro i sistemi di informazione (COM(2002) 173 definitivo).

CAPITOLO QUARTO

La cooperazione giudiziaria e di polizia in prospettiva *de iure condendo*: riforma del sistema e della circolazione della prova digitale ai fini di giustizia

SOMMARIO: 1. L'incremento dei poteri degli organi comunitari per una cooperazione più efficace: il (nuovo) ruolo centrale di Europol, Eurojust e Olaf - 2. La genuinità della prova digitale in Unione Europea e negli Stati membri: prospettive di armonizzazione e di incremento della cooperazione nello spazio giudiziario europeo – 3. La definizione di standard minimi di garanzia dei diritti fondamentali nelle procedure di circolazione della prova

1. *L'incremento dei poteri degli organi comunitari per una cooperazione più efficace: il (nuovo) ruolo centrale di Europol, Eurojust e Olaf*

L'entrata in vigore del Trattato di Lisbona è un segno tangibile del bisogno crescente di un approccio europeo e comune, specie per poter sfruttare appieno le potenzialità dell'Unione.

Nell'ultimo decennio l'Unione europea ha cercato di ottimizzare gli strumenti a sua disposizione e di potenziare le proprie capacità d'intervento.

Al tempo stesso gli Stati membri sono chiamati a collaborare nelle materie di maggiore interesse per l'Unione e per il cittadino, quale la criminalità di natura transnazionale, ed *in primis* il terrorismo.

La personalità giuridica unica dell'UE implica che il Terzo Pilastro nel campo della giustizia e degli affari interni scompare definitivamente, trascorso il periodo di transizione di cinque anni, e le politiche comuni nello spazio di libertà, sicurezza e giustizia, incluso Schengen, rientreranno nel Primo Pilastro o nel metodo comunitario. Il diritto di iniziativa della Commissione in materia di giustizia e affari interni viene tuttavia condiviso con un quarto degli Stati membri.

Con l'entrata in vigore del nuovo Trattato, l'Unione europea non avrà più bisogno e non cercherà il trasferimento di nuove competenze da parte degli Stati membri.

Ai sensi dell'articolo 67 TFUE (*ex* articolo 61 del TCE ed *ex* articolo 29 del TUE), l'Unione realizza uno spazio di libertà, sicurezza e giustizia nel rispetto dei diritti fondamentali nonché dei diversi ordinamenti giuridici e delle diverse

tradizioni giuridiche degli Stati membri. e si adopera per garantire un livello elevato di sicurezza attraverso misure di prevenzione e di lotta contro la criminalità, attraverso la previsione di misure di coordinamento e cooperazione tra forze di polizia e autorità giudiziarie e altre autorità competenti, nonché tramite il riconoscimento reciproco delle decisioni giudiziarie penali e, se necessario, il ravvicinamento delle legislazioni penali.

L'interesse dell'ordinamento comunitario verso lo sviluppo delle politiche di cooperazione nella materia penale è attestata dal contenuto dell'intero capo IV del Trattato sul funzionamento, il quale fonda l'azione dell'UE in materia sul principio del mutuo riconoscimento. Si pensi che questi principio è nato nel contesto del I Pilastro dell'Unione , escludendo dunque l'ambito criminale ove risulta essere un contenuto di nuova applicazione.

Accanto a questo, proprio al fine espresso di facilitarne la concreta attuazione, sempre l'art. 82 TFUE prevede che il Parlamento europeo e il Consiglio possono stabilire norme minime deliberando, mediante direttive, secondo la procedura legislativa ordinaria.

Uno degli obiettivi principali dell'Unione è rappresentato dal tentativo di facilitazione della cooperazione tra le autorità giudiziarie o autorità omologhe degli Stati membri in relazione all'azione penale e all'esecuzione delle decisioni, nella materia penale di interesse transnazionale.

Nel contesto dello sviluppo dell'efficace della cooperazione, l'Unione, a seguito dell'entrata in vigore del Trattato di Lisbona, agevola l'instaurazione di una cooperazione rafforzata tra gli Stati membri intese a promuovere la realizzazione degli obiettivi comunitari, a proteggere i suoi interessi e a rafforzare il suo processo di integrazione[574].

Il fine dello sviluppo di uno spazio europeo di libertà, sicurezza e giustizia rimarrebbe lettera morta senza l'individuazione ed il rafforzamento di organismi comunitari per la cooperazione di polizia e giudiziaria. È questo il caso del nuovo ruolo assunto in particolare da Europol, Eurojust ed Olaf.

Organismi nati in fretta per far fronte a contingenze imminenti[575], sorti a seguito di sofferti compromessi tra diverse istanze ovvero costituiti per svolgere attività diverse da quella strettamente connessa alla materia penale [576].

Si è già avuto modo di trattare delle origini e dello sviluppo dei poteri di Eurojust, di Europol e di Olaf[577].

---

[574] Cfr art. 10 Trattato di Lisbona.

[575] Il riferimento in questi termini è ad Eurojust, l'organo di assistenza per le autorità giudiziarie degli Stati membri, il quale Ufficio è stato creato di fretta, a seguito dell'attacco alle Torri Gemelle.

[576] Si pensi in questi termini ad Olaf, un Ufficio nato per svolgere indagini amministrative ed ora sempre più implicato ed interessato in indagini penali.

[577] Cfr Capitolo Primo, paragrafo 6 e Capitolo Quarto, paragrafo 1.

L'Unione europea si è interessata e continua a discutere dei temi principali dalla prevenzione, alle indagini, alla repressione di un fatto di rilevanza penale transnazionale e dei loro autori.

L'art. 86 TFUE, con una formulazione molto generica, prevede che venga istituita una Procura europea a partire da Eurojust.

La necessità di definire un organo comune europeo per l'azione è da lungo sentita ed è stata oggetto di attenzione negli Anni '70 del secolo scorso da parte del Presidente De Gaulle, poi nel primo testo del Corpus Juris negli Anni '90 in cui, nella parte dedicata alla procedura penale, è stata più concretamente pensata l'attuazione della Procura europea.

Forse in ragione dei noti problemi di interpretazione e di diversità dei sistemi giuridici nazionali, la formulazione dell'art. 86 TFUE è molto (troppo) vaga e lascia aperte molteplici interpretazioni sul significato della formula "*a partire da Eurojust*".

Per accelerare i tempi di attuazione di quanto previsto dal Trattato di Lisbona, è stato confezionato uno studio che rappresenta la base del progetto da sottoporre alle istituzioni europee, in particolare alla Commissione e al Consiglio.

La scarna ed insufficiente formulazione del menzionato articolo del Trattato rappresenta un ostacolo alla formazione di questo organo, di cui non viene indicata alcuna regolamentazione o alcuna norma sulla composizione, struttura e funzionamento.

"*A partire da Eurojust*" significa che la Procura europea sostituirà *in toto* Eurojust o se ne affiancherà, mantenendo stretti rapporti di interscambio e collaborazione reciproche? Questo organo istituzionale sarà composto come Eurojust, ricalcandone gli elementi strutturali fondamentali?

Questi interrogativi restano ad oggi irrisolti ma richiederebbero un intervento concreto del Legislatore comunitario per dare certezza a questa nuova prospettiva di indagine penale per criminalità transnazionale.

L'unica certezza, attualmente, è che Eurojust, pur nel suo mutato aspetto di più forte competenza in materia di coordinamento tra le autorità giudiziarie coinvolte, non è un organo d'indagine, a differenza di ciò che dovrebbe essere il PME.

Ulteriori accuse mosse alla disciplina in trattazione, attengono la contraddizione con gli obiettivi di cooperazione giudiziaria penale realizzata attraverso Eurojust ed attraverso la messa in rete delle autorità nazionali. La Procura europea è infatti prevista come organismo centrale con poteri diretti di esercizio dell'azione penale, ciò, pertanto, in contrasto con un sistema che si fonda sulla progressiva armonizzazione ed il mutuo riconoscimento. L'istituzione di una Procura europea, qualora permanesse contemporaneamente operativo Eurojust, potrebbe generare delle

sovrapposizioni di due logiche diverse di intervento di questi due organismi su materie simili.

Manca inoltre la previsione di una garanzia giurisdizionale[578] di un giudice europeo a cui il PME possa far riferimento, anche al fine di combattere il cd. *forum shopping*.

La Procura, come ad oggi nelle previsioni del Trattato, si sovrapporrebbe inevitabilmente ad ordinamenti nazionali dove l'esercizio dell'azione penale è disciplinato in modo completamente diverso (in taluni Stati l'azione penale è obbligatoria, in altri facoltativa o soggetta all'indirizzo del governo e/o del Parlamento).

Questi nodi critici ancora irrisolti necessitano di un intervento normativo di dettaglio e/o un intervento della Corte di Giustizia che possa definire l'interpretazione autentica dell'art. 86 TFUE nella formulazione attuale.

La previsione della Procura europea rappresenta un importante passo in avanti in materia di cooperazione, muovendo da una cooperazione orizzontale basata sul consenso degli Stati, ad una cooperazione verticale che obbliga gli Stati ad agire in modo unitario e comune.

La necessità della presenza di un'agenzia investigativa comune almeno per gli Stati UE è sentita da più parti, anche dagli esponenti degli organismi europei di cooperazione, cioè da Europol, Eurojust e Olaf. Questi ultimi, infatti, pur con gli incrementati poteri, possono godere solo di informazioni frammentate che non permettono di formare un quadro completo dei fatti di interesse.

Nessun organismo attualmente operativo è in grado di prevedere e capire quando un'agenzia investigativa nazionale può possedere dei dati utili sui casi in esame. Tantomeno quest'ultima è messa nelle condizioni di sapere che un Ufficio dell'Unione europea é interessato a conoscere alcune informazioni raccolte.

La prospettata situazione è rappresentativa, prima di tutto, di un'assenza di canali di comunicazione continui e completi tra le autorità nazionali e gli organi comunitari che operano nella materia criminali, oltre a dimostrare la necessità di un intervento decisivo delle istituzioni comunitarie (la Commissione europea e il Consiglio *in primis*), volto alla definizione di una disciplina, in grado di definire la struttura, l'organizzazione e i compiti rispettivi di Eurojust, Europol, Olaf e del futuro Pubblico ministero europeo.

Secondo quanto previsto nell'agenda dei lavori della Commissione europea, agli inizi del 2013 sarà presentato una proposta di Decisione quadro

[578] La necessità di istituire un organismo giurisdizionale europeo di garanzia e controllo dell'attività della Procura europea era già sentita nel secondo progetto del Corpus Juris, curato dalla professoressa Delmas Marty.

sul PME, con la speranza che risponda alle esigenze di completezza e coordinamento appena indicate.

Ogni riforma importante di sistema, come è per la creazione di una Procura europea, per il rafforzamento della cooperazione e dei poteri degli organi comunitari, richiede anche un'analisi dell'impatto economico delle scelte effettuate e delle modalità di realizzazione di esse.

L'esempio offerto dal Trattato di Prum, sottoscritto il 27 maggio 2005 da sette Stati membri dell'Unione europea, mette in luce da un lato l'insufficienza dei sistemi di cooperazione vigenti nell'ordinamento comunitario e d'altro lato l'importanza della circolazione delle informazioni. Esso, infatti, rappresenta un caso emblematico di cooperazione rafforzata in materia di controlli di polizia, che ha coinvolti inizialmente pochi Stati interessati e a cui, in seguito, anche aderito molti altri Paesi, tra cui l'Italia. L'Accordi siglato a Prum interessa, in particolare, la cd. cooperazione informativa, prevedendo delle misure di scambio transfrontaliero di informazioni, mediante la creazione di archivi nazionali collegati tra loro, contenenti profili di DNA, dati dattiloscopici e dati relativi all'immatricolazione di veicoli.

L'auspicio, in considerazione della sua importanza per lo sviluppo della cooperazione di polizia e per la prevenzione e lotta alle più gravi forme di criminalità *cross border* e che questo strumento possa essere attuato in un numero sempre crescente di Stati, instaurando una fitta rete di scambi e collaborazione.

L'aumento e l'estensione di queste forme cooperative particolari e settoriali possono costituire un *input* valido per aprire gli orizzonti verso le nuove sfide della globalizzazione del crimine e della necessità di collaborazione tra le autorità di più Stati membri.

Questo nell'attesa e nella speranza che le istituzioni europee, sempre più sensibili al problema, si adoperino concretamente per prevedere normativamente delle procedure di cooperazione più rapide ed efficaci.

L'Unione europea, infatti, può costituire un ottimo banco di prova per lo sviluppo di un sistema di cooperazione di polizia e giudiziaria in grado di rispondere alle esigenze di prevenzione e lotta alla criminalità globale, per poi allargarsi anche nei rapporti con Paesi Terzi.

Lo spazio territoriale in cui si sviluppa un fatto penalmente rilevante, infatti, è sempre più espanso, fino a coinvolgere gli Stati che non sono membri dell'Unione europea.

Emblematicamente, è possibile menzionare i casi di *cybercrime* in cui le autorità procedenti si trovano a dovere spesso istituire rapporti diretti con i propri colleghi degli Stati Uniti d'America.

È noto il caso denominato "*Phish&chips*", che ha visto coinvolto il pool reati informatici della Procura della Repubblica presso il Tribunale di Milano,

in cui sono venuti allo scoperto tutti i limiti delle disposizioni in materia di cooperazione internazionale, in particolare nei rapporti con gli USA.

Gli accertamenti investigativi riguardanti questa fitta rete di casi di *phishing* ha preso le mosse già nel marzo 2005, a seguito di una prima denuncia-querela presentata dalla direzione degli affari legali di Banca Intesa in Milano.

Da lì le indagini si sono susseguite incessanti, espandendosi ed interessando diversi Stati tra cui gli USA.

Nonostante le richieste di rogatorie formulate dalle autorità italiane verso quelle statunitensi, per ottenere dati e documenti presenti nel loro territorio di competenza, le risposte tardavano a giungere, con il rischio di ostacolare la prosecuzione delle indagini ed inficiare il buon esito del procedimento per intervenuta decadenza dei termini[579].

L'assoluta inefficienza delle forme di cooperazione hanno costretto le autorità procedenti a recarsi direttamente *in loco* per raccogliere quanto necessario ai fini di giustizia.

Un comportamento tenace delle autorità procedenti, che non si arresta davanti agli ostacoli, è sicuramente auspicabile ed insieme apprezzabile ma non può essere da solo sufficiente.

È necessaria la previsione di ulteriori misure normative per l'attuazione di un sistema di cooperazione di polizia e giudiziarie che, partendo dall'esistente e dai limiti riscontrati, possano valorizzare i progressi fatti ed introdurre delle riforme utili ed efficaci.

2. *La genuinità della prova digitale in Unione Europea e negli Stati membri: prospettive di armonizzazione e di incremento della cooperazione nello spazio giudiziario europeo*

L'evoluzione delle scienze ha prodotto nuove tecnologie correlate anche alla materia della giustizia penale, secondo un duplice ordine di implicazioni. Vi sono tecnologie utili per la gestione dell'attività giuridica, per la ricerca di elementi di prova o per la circolazioni di informazioni utili alle autorità procedenti. A volte, però, l'infrastruttura informatico-telematica è "soggetto" di reato, divenendo così un nemico e non un supporto per la prevenzione e la repressione della criminalità.

È fuori di dubbio che, attualmente, la maggior parte dei procedimenti penali, specie di natura transnazionale, si sostanziano in dati, informazioni e prove digitali.

[579] Per un approfondimento sul caso "Phish&chips" si rinvia a F. CAJANI – G. COSTABILE – G. MAZZARACO *op.cit.*

Le autorità investigative non devono, però, farsi accecare dalla scienza ed utilizzare frettolosamente i contenuti di dati e informazioni digitali per costruire capi d'imputazioni poco meditati.

Al contrario, l'auspicio è che la scienza forense non si sostituisca alle attività d'indagine tradizionale ma ne costituisca una guida per la migliore prosecuzione dell'investigazione e un valido supporto alla definizione del procedimento, secondo una logica della ricerca della verità processuale.

Si consideri che la prova digitale è intrinsecamente problematica sotto molteplici punti di vista e in diversi aspetti.

Una prima considerazione di natura linguistico-definitoria mostra la difficoltà di individuare i confini entro cui si snoda questo concetto, non solo all'interno di un ordinamento nazionale ma anche da una visione comparatistica d'insieme[580].

A livello UE l'idea stessa di "*prova*" non ha dei contorni definiti, chiari e condivisi da tutti gli Stati membri e non ogni ordinamento interno è dotato di un apparato classificatorio delle tipologie di prova[581].

Queste nuove prove scientifiche si scontrano anche con le limitate capacità da parte degli organi inquirenti e giudicanti di comprenderne la forma ed i contenuti, per la presenza di *gap* cognitivi, per la specificità della materia, o per delle difficoltà di approccio alla tecnologia a causa dell'età avanzata di alcuni operatori del diritto[582].

Partendo dalla genesi della prova digitale, in primo luogo si riscontra l'assenza di *best practices* comuni d'intervento che possano omogeneizzare l'attività investigativa su apparecchi informatizzati negli Stati dell'Unione.

Pur comprendendo le difficoltà di definire delle linee guida applicabili ad ogni intervento, in considerazione della diversità che si riscontrano di caso in caso, è opportuno definire dei principi che possano orientare le pratiche di *computer forensics* anche se non dettagliate su ogni campo d'indagine.

In particolare, si fa riferimento alla necessità di inquadrare i requisiti tecnici che devono possedere i *forenser*, indicare le strumentazioni utilizzabili e le certificazioni di sicurezza dei sistemi che queste devono garantire, elencare i passaggi imprescindibili d'intervento sulle macchine e le modalità di verbalizzazione delle operazioni compiute.

---

[580] Sulle difficoltà di definizione, si rinvia al Capitolo Secondo, paragrafo 1.

[581] Si pensi al diritto italiano delle prove in cui, oltre a distinguere tra prova precostituita e prova costituenda, tra prova dichiarativa e prova documentale, sono noti anche i concetti di mezzi di prova, mezzi di ricerca della prova, elementi di prova, ignoti per molti altri ordinamenti giuridici nazionali dell'Unione europea.

[582] In Italia, per esempio, i giudici della Corte d'Appello e ancor più della Corte di Cassazione sono abbastanza anziani e subiscono spesso passivamente lo scarto generazionale che li costringe a confrontarsi con dei mezzi tecnologici non noti e di difficile comprensione.

Queste norme dovrebbero consentire una valutazione oggettiva di ammissibilità ed utilizzabilità della prova digitale raccolta, ai fini della decisione del processo.

Quando si parla di *prova* in ambito comunitario, il riferimento è anche al dato probatorio, cioè al dato digitale, sensibile e non, che viene utilizzato per i fini di giustizia.

Con riferimento a questo, lo scenario UE mostra una proliferazione di archivi e banche dati in cui sono contenute le informazioni più varie, spesso anche ad insaputa dei diretti interessati.

Gli stessi organismi comunitari per la cooperazione (Europol, Eurojust e Olaf) si servono di banche dati proprie, con sezioni nel territorio di ciascuno Stato membro. Sono noti, a titolo esemplificativo, i Sistemi informativi del SIS (Sistema Informativo Schengen – oggi di seconda generazione), la banca dati del casellario giudiziario ECRIS, EURODAC, VIS, le banche dati create per la gestione delle informazioni indicate nel Trattato di Prum.

L'approccio alla prova digitale richiede delle conoscenze specifiche ed uno sviluppo tecnico continuo dei mezzi utilizzati per la raccolta e l'archiviazione dei dati, secondo i canoni di genuinità e sicurezza dei dati acquisiti.

È utile per il giudice, quando si confronta con prove di un tale tecnicismo, essere affiancato da un soggetto di comprovata esperienza che lo possa guidare nella comprensione di quanto si trova a valutare, non potendo possedere una conoscenza sufficiente, poiché la materia esula da quelle che costituiscono un patrimonio esperienziale e di concetto, proprio di un uomo medio.

Un ulteriore oggetto di discussione attiene le modalità di descrizione delle attività compiute nella fase di raccolta e archiviazione della prova digitale. Tradizionalmente vengono prodotti dei verbali che riportano, momento per momento, ogni atto compiuto. La delicatezza ed insieme la complessità di alcuni interventi, però, ha dimostrato che questa modalità è insufficiente a garantire un controllo effettivo e dettagliato rispetto agli atti di *computer forensics*.

Preso atto di ciò, crescono le ipotesi in cui i mezzi digitali sono utilizzati anche ai fini della descrizione delle operazioni compiute. In particolare, in molte situazioni gli operanti scelgono di filmare tutte le attività svolte. È definibile anche questo contenuto come prova digitale o esula da tale concetto?

Solo un intervento normativo uniforme e chiarificatore può fornire una definizione completa della locuzione "*prova digitale*".

A parere di chi scrive, la descrizione delle operazione mediante un mezzo tecnologico costituisce a tutti gli effetti una prova digitale, sia perché si riferisce ad una attività investigativa procedimentale, sia perché rappresenta in

immagine lo svolgimento dei compiti delle autorità competenti per le indagini criminali, sia per l'uso della strumentazione elettronica.

La raccolta ed archiviazione di prove digitali genuine permette un flusso rapido di informazioni nell'ambito dello sviluppo della cooperazione giudiziaria e di polizia nello spazio UE, per la prevenzione e lotta della criminalità transnazionale.

L'approccio critico e di interessamento alla *electronic evidence* nell'ordinamento comunitario è cresciuto in particolare negli ultimi quindici anni circa.

Da un iniziale intervento volto a garantire la conservazione della prova[583], il centro d'interesse si è spostato maggiormente sulla circolazione della prova tra gli Stati membri.

Con la previsione del Mandato europeo di ricerca della prova (mai implementato nella pratica) c'è stato un primo tentativo di sviluppo della cooperazione mediante la circolazione delle prove precostituite (salvo alcune eccezioni in cui è stata prevista la possibilità di avanzare una richiesta di Mandato di ricerca anche per prove costituende). La proposta di istituzione di una nuova procedura di scambio mediante l'Ordine europeo d'Indagine, rappresenta un punto di svolta molto importante. Da un lato rispecchia l'auspicato intervento normativo per l'agevolazione della circolazione della prova anche costituenda[584], d'altro lato tocca i profili più controversi relativi al principio del mutuo riconoscimento.

L'OEI risponde alle esigenze di efficienza delle misure di cooperazione e di scambio di informazioni in tempi rapidi.

In netta contrapposizione con il principio del mutuo riconoscimento, però, è previsto che siano le autorità dello Stato richiedente ad indicare alle autorità competenti dello Stato richiesto le modalità di raccolta della prova ai fini dell'ammissibilità nel procedimento penale di quello Stato.

Si nota positivamente che i motivi di rifiuto sono ridotti ai minimi termini, anche se è esclusa come ipotesi di non esecuzione l'applicazione del *ne bis in idem* europeo.

L'ordinamento comunitario, in materia di prove, presenta ancora una normativa troppo vaga, spesso insufficiente e comunque frammentata. Non risponde alle esigenze di libera circolazione di prove riconosciute in tutti gli ordinamenti interni degli Stati membri dell'UE, come auspicato.

Una presa di posizione a livello legislativo sulla prova digitale, poi, rappresenta una chimera, forse ancora troppo lontana dal realizzarsi,

[583] In questi termini, il riferimento è, in particolare, alla Decisione quadro in materia di confisca dei beni che costituiscono prezzo, profitto o provento di reato.

[584] Si pensi, in particolare, alle intercettazioni di comunicazioni anche telematiche e gli interrogatori, che costituiscono delle prove centrali in un procedimento penale.

nonostante i dati fattuali ne attestino il grado di espansione e la conseguente necessità d'intervento a regolamentazione.

3. *La definizione di standard minimi di garanzia dei diritti fondamentali nelle procedure di circolazione della prova*

Si è a lungo discusso della necessità di riconfigurare le procedure di cooperazione di polizia e giudiziaria ad oggi vigenti, avuto riguardo, in particolare, alla materia della prova penale digitale.

La creazione di basi penali comuni a tutti gli Stati membri non può prescindere dalla previsione di *standard* minimi di garanzia dei diritti fondamentali coinvolti.

Già nelle conclusioni del Consiglio europeo di Tampere del 1999, a fianco del tema centrale della sicurezza dei cittadini europei, è stato discusso, sebbene in maniera trasversale e poco dettagliata, il problema del contemperamento con le istanze di protezione delle libertà fondamentali e dei diritti degli individui. Questo tema è stato poi sviluppato con il Programma dell'Aja del 2004, parallelamente alle questioni legate al reciproco riconoscimento e al principio di disponibilità delle informazioni di polizia tra le autorità degli Stati membri. Nel testo del Programma di Stoccolma la garanzia dei diritti fondamentali ha rappresentato la materia d'interesse principale.

Il Trattato di Lisbona ha costituito un sistema di protezione dei diritti fondamentali multilivello, basato sia sul riconoscimento della Carta dei diritti fondamentali (la Carta di Nizza), sia sulla Convenzione europea dei diritti dell'uomo, improntando tutto l'agire dell'Unione sul rispetto di queste prerogative.

Se, dunque, ogni ambito di interesse dell'Unione europea si uniforma agli *standard* di tutela delle menzionate Convenzioni e delle interpretazioni che di esse è data dalla giurisprudenza comunitaria, così anche la disciplina in materia penale deve stare attenta a questa cornice di riferimento.

A partire dalla raccolta della prova penale, non è sufficiente individuare una cornice di diritti minimi in astratto ma è necessario che questi siano calati nel concreto, guidando e, se necessario, limitando l'assunzione di prove. *In primis* è il diritto di difesa, nella sua massima estensione concettuale, a dover essere garantito anche nel diritto delle prove criminali.

In secondo luogo, se la prova, specie intesa come prova digitale, è anche rappresentata dal dato probatorio, ciascun individuo deve essere messo nelle condizioni di conoscere quali informazioni di sé sono contenute nelle banche dati, come può procedere alla modifica di informazioni sbagliate o non aggiornate, quando ha diritto di chiederne la cancellazione.

Il diritto alla riservatezza e, se vogliamo, all'oblio devono essere tutelati dal controllo delle procedure di cancellazione e distruzione delle informazioni possedute, quando non si ha più un motivo legittimo per ritenerle.

Gli interventi normativi sul *data retention* in ambito comunitario sono stati e continuano ad essere di centrale importanza. Questi meriterebbero un intervento riformatore per armonizzare le disposizioni nazionali e sensibilizzare i Legislatori degli Stati membri sull'importanza del tema.

Da uno sguardo d'insieme al testo del Trattato di Lisbona emerge con chiarezza un nuovo, per così dire, diritto al dato ed alla sua protezione.

La tutela del dato deve essere garantita fin dalla sua raccolta, prevedendo dei sistemi idonei, in grado di non ledere la *privacy* del singolo individuo e di mantenere la sicurezza delle infrastrutture di archiviazione e di circolazione delle informazioni.

Il Trattato di Lisbona ed il Programma di Azione presentano un agenda ricca di iniziative, da realizzare nel periodo 2010-2014, per favorire l'individuazione concreta di *standard* minimi di protezione dei diritti fondamentali e dei diritti procedurali in materia penale.

Questo progetto incontra non solo i temi già indicati ma anche lo sviluppo delle politiche di traduzione ed interpretazione degli atti, delle prove, dei documenti e di tutte le informazioni fondamentali per cui deve essere reso edotto l'indagato/imputato, anche ai fini del diritto di difesa e del diritto ad un giusto processo.

Si richiede alle istituzioni comunitarie di intervenire nella materia penale, oggi di competenza (concorrente) dell'Unione, a seguito dell'abbattimento della divisione in Pilastri, avuto riguardo alle opposte istanze: da un lato l'interesse della collettività ad uno spazio europeo di giustizia e sicurezza, d'altro lato la volontà degli individui di vedere protetti i propri diritti fondamentali, senza pregiudizio alle libertà personali.

Queste opposte esigenze si scontrano costantemente tra loro proprio in relazione al diritto criminale, per la delicatezza della materia e degli interessi in gioco.

La previsione di disposizioni di cornice può fungere da guida per le autorità investigative e giudiziarie degli Stati membri, superando i particolarismi e le gelosie nazionali, per perseguire un obiettivo comune di lotta al crimine *cross border,* con attenzione alla protezione dei diritti fondamentali.

È fuori di dubbi che una norma scritta sul punto non potrà mai essere una norma di dettaglio, non potendosi prevedere tutte le diverse ipotesi riscontrabili nella prassi giuridica.

CONCLUSIONI

L'Unione europea, tra gli obiettivi indicati nel progetto *Europa 2020*, si prefigge di investire nell'innovazione come sfida per il futuro e come segno di rilancio di un'economia globale in crisi.

Lo sviluppo della scienza e della tecnica porta con sé nuove aspettative e traguardi importanti, ma anche la crescita della criminalità transnazionale, la quale si serve delle innovazioni tecnologiche per i propri scopi criminosi e riescono a mantenere una rete territoriale d'espansione potenzialmente infinita, proprio mediante l'uso delle strumentazioni tecnico-telematiche.

L'innovazione, dunque, richiede una risposta chiara e concreta da parte del Legislatore comunitario, poiché i rischi legati ad essa non sono parcellizzati e delimitati ma riguardano indistintamente tutti gli Stati membri.

La contromossa dell'Unione può consistere nel percorrere la via del mutuo riconoscimento, già testata per le decisioni giudiziarie e prevista anche con il MAE e il MERP, ovvero seguire la strada dell'armonizzazione, come nella Decisione quadro sull'interpretazione e la traduzione e nella previsione di diritti minimi.

In base all'art. 82 TFUE, entrambe queste due scelte sono legittime e idonee alla realizzazione di un vero spazio europeo di libertà, sicurezza e giustizia.

In alcune circostanze l'omogeneizzazione è possibile ed anche auspicabile, in altri casi non è pensabili o comunque non rappresenta una scelta idonea al perseguimento dei fini prefissati.

Il quadro di sistema ricostruito e approfondito nel corso della ricerca, presenta una situazione molto complessa perché frammentata , incompleta e disomogenea.

Delineando gli elementi normativi principali allo *status quo*, è emerso un interesse crescente dell'Unione europeo verso lo sviluppo della cooperazione anche informativa, la circolazione della prova, la velocizzazione delle procedure e la protezione dei diritti fondamentali.

In questa cornice dai tratti positivi non mancano i punti deboli e, in alcuni casi, è assente la trattazione di alcuni aspetti importanti, di talché sono state qui abbozzate delle prospettive *de iure condendo,* auspicando un intervento concreto dell'UE.

Per poter sviluppare un vero diritto penale comunitario, comprensivo degli aspetti procedurali, è necessaria la partecipazione di tutti gli Stati membri, ciascuno con i propri istituti, le proprie iniziative e tradizioni giuridiche.

Solo realizzando uno stato di democraticità è possibile creare una vera Europa, in grado di sviluppare compiutamente uno spazio di libertà, sicurezza e giustizia.

La creazione di questo spazio europeo non può prescindere dalla trattazione di alcuni aspetti fondamentali in materia criminale, sostanziale e processuale.

La presa di coscienza della globalizzazione del crimine richiede un approccio a livello normativo e una revisione di strumenti comuni e condivisi tra tutti gli Stati.

I reati *cross border* richiedono una stretta collaborazione tra le autorità competenti dei diversi Paesi, che si sostanzia non solo nella cooperazione giudiziaria e di polizia ma anche nella cooperazione informativa.

Tutte queste forme di sostegno tra Stati sono state interessate da forti impulsi di sviluppo che hanno fornito alcuni risultati confortanti, ma richiedono degli sforzi ulteriori di riforma, per far fronte alle nuove sfide del crimine.

La pratica giuridica ci mostra un incremento delle prove digitali, siano esse prodotte dallo strumento informatico che è mezzo di reato o mezzo offeso dal reato, siano esse il risultato di dati (sensibili e non) raccolti in archivi.

La discussione e le previsioni normative in materia di *digital evidence* sono così poche e così poco dettagliate da creare dei problemi di utilizzabilità a processo e di circolazione sicura.

Le prove digitali prodotte nella commissione di una grande varietà di fatti penalmente rilevanti sono importanti per i fini di giustizia che non è possibile ignorare le esigenze di integrazione e riforma normativa, secondo un approccio sovranazionale che possa trovare applicazione in tutti gli Stati membri.

Le *electronic evidences* rilevano sia nella fase statica di raccolta ed archiviazione, sia, ed in maniera preponderante, nella fase dinamica di circolazione, quando riguardano (come spesso accade) dei crimini di natura transnazionale. I reati *cross border* infatti sono spesso agevolati dall'uso della tecnologia o sono guidati dall'intento di ledere delle infrastrutture critiche, per raggiungere il proprio fine criminale.

Per questi motivi, l'interesse della materia penale verso le sfide dello sviluppo scientifico deve rivolgersi a tutto campo, su tutti i fronti interessati dalle innovazioni informatico-telematici.

Perché in ambito comunitario si è ancora restii a definire la nuova fattispecie criminosa del *cyberterrorism*?

I reati commessi con il mezzo informatico o sull'infrastruttura digitale possono ragionevolmente generare uno stato d'ansia e di pericolo per l'incolumità, producendo un notevole (se non incalcolabile) danno da reato.

Si pensi ad un'immagine un po' apocalittica (ma forse nemmeno troppo fantascientifica), per cui le infrastrutture critiche, per esempio, di tutti gli ospedali cessassero di funzionare per opera di un criminale informatico: che ne sarebbe della salute dei cittadini? Il danno conseguenza sarebbe assai ingente.

Eppure spesso le istituzioni tendono a minimizzare il pericolo intrinseco all'innovazione tecnologica, senza pensare che gli attacchi informatici possono essere i più vari e possono colpire in maniera silenziosa e imprevedibile ma letale.

Sarebbe opportuno che le istituzioni comunitarie si approcciassero in maniera più critica al problema della criminalità informatica, del diritto della prova digitale, della cooperazione mediante la circolazione di questa e, più in generale, della disciplina e delle garanzie procedurali.

Aggiungere la parola "*terrorismo*" alla menzionata categoria di reati informatici può aprire le maglie delle limitazioni del sistema giuridico vigente, permettendo, come nelle ipotesi tradizionali di terrorismo, di compiere delle scelte d'intervento meno limitate. Si pensi, infatti, al numero di atti normativi speciali, previsti in materia.

Si è già detto che il Trattato di Lisbona ha orientato l'agire dell'Unione verso la garanzia di questi diritti.

Nella materia criminale, specie nella lotta ai reati transnazionali e mediante l'uso degli strumenti di cooperazione, si genera ripetutamente un problema di approccio critico al fatto e di difficile contemperamento tra l'interesse a stabilire la sicurezza collettiva e le istanze di protezione dei diritti umani.

Quando si procede per reati di terrorismo questo complesso di controlimiti è molto più labile, prevalendo l'interesse della sicurezza, in considerazione del potenziale di danno insito nelle attività terroristiche.

Lo stesso discorso, sia in materia di diritti, sia in relazione all'uso di determinati strumenti d'indagine, mezzi d'intervento, circolazione delle informazioni, sarebbe valido nelle ipotesi di *cyberterrorism,* mentre così non è attualmente per i crimini informatici e per una serie di altri crimini di natura eminentemente transfrontaliera.

È possibile, però, guardare al futuro dell'Europa con fiducia, verso un processo penale europeo, in grado di vincere la mancata fiducia reciproca e le gelosie degli Stati membri.

Se le istituzioni europee saranno nelle condizioni di provvedere nei termini e modi previsti nell'*Action Plan* per l'attuazione del Programma di Stoccolma, entro il 2014 potremo davvero dire di vivere in un'Europa dei diritti, della giustizia, della sicurezza.

Le azioni fondamentali previste nelle materie che interessano per i fini di questa ricerca, riguardano molteplici aspetti: l'inclusione del settore della

cooperazione giudiziaria e di polizia in materia penale nel quadro pluriennale dell'Agenzia per i diritti fondamentali; un nuovo quadro giuridico globale per la protezione dei dati; una Comunicazione relativa agli elementi essenziali di protezione dei dati personali degli accordi a fini di contrasto tra l'Unione europea e i Paesi terzi; una Proposta legislativa in materia di informazioni sui diritti e sui capi d'imputazione; una Proposta legislativa in materia di consulenza e assistenza legale gratuita; una Proposta legislativa in materia di garanzie speciali per indagati o imputati vulnerabili; un Libro verde sulla necessità di integrare i diritti procedurali minimi di indagati e imputati contemplati dalle precedenti proposte legislative; una Proposta legislativa relativa a un sistema generale di assunzione delle prove in materia penale basato sul principio del reciproco riconoscimento e riguardante tutti i tipi di prova; una Proposta legislativa diretta a introdurre norme comuni per la raccolta delle prove in materia penale al fine di garantirne l'ammissibilità; una Proposta di regolamento che conferisce a Eurojust il potere di avviare indagini, rende più efficace la struttura interna di Eurojust e coinvolge il Parlamento europeo e i parlamenti nazionali nella valutazione delle attività di Eurojust; una Comunicazione sull'istituzione di una Procura europea a partire da Eurojust; una Rete giudiziaria europea (in materia penale), in attuazione della decisione 2008/976/GAI del Consiglio relativa alla RGE e migliorando la diffusione di informazioni aggiornate sull'attuazione degli strumenti di cooperazione giudiziaria dell'UE; una Comunicazione sugli aspetti internazionali della cooperazione giudiziaria in materia penale; una Comunicazione sul modello europeo di scambio delle informazioni, seguita da un piano d'azione; un Codice di polizia, comprendente la codificazione dei principali strumenti sull'accesso all'informazione; una Proposta di misure di attuazione del sistema europeo di informazione sui casellari giudiziari (ECRIS); una Comunicazione sulla fattibilità di un indice UE dei casellari giudiziali (EPRIS); una Comunicazione su possibili misure per promuovere lo scambio di informazioni tra Stati membri, compreso Europol, sui delinquenti violenti che si spostano sul territorio in occasione di grandi manifestazioni; una Comunicazione relativa alla valutazione di ECRIS e alla sua futura estensione allo scambio di informazioni sulle misure di sorveglianza; una Proposta di regolamento su Europol; una Proposta sullo scambio di informazioni tra Europol, Eurojust e Frontex; una Comunicazione sul miglioramento della cooperazione doganale e di polizia nell'UE, comprendente una riflessione sull'impiego di agenti infiltrati, sui centri di cooperazione di polizia e doganale, sull'approccio dell'UE a un'attività di polizia basata sull'intelligence e su azioni comuni per migliorare la cooperazione di polizia a livello operativo; una Proposta per una classificazione europea delle tipologie di reato; un'indagine sulla sicurezza nell'UE; misure per una politica rafforzata e ad alto livello in

materia di sicurezza delle reti e dell'informazione, comprese iniziative legislative come quella sulla modernizzazione dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), nonché altre misure che consentano reazioni più rapide agli attacchi informatici; Proposta legislativa relativa agli attacchi contro i sistemi informatici; la Creazione di una piattaforma di segnalazione dei reati informatici a livello europeo, per mezzo di Europol.

L'agenda delle azioni si presenta molto nutrita e si prevede anche lo sviluppo di studi giuridici, empirici e statistici sullo *status quo,* al fine di individuare gli ambiti di possibile intervento in prospettiva futura.

La presa di coscienza dell'Unione sul potenziale criminale di natura transnazionale emerge chiaramente dal Piano d'Azione e può essere di conforto per gli euro-scettici, ma non per i nazionalisti che continuano a temere una cessione di una grossa fetta di sovranità, anche dell'ultimo baluardo costituito dalla materia penale, che fin'ora aveva resistito agli incessanti tentativi di europeizzazione.

SUMMARY

The modern society is the result of a technological progress, as a sign of goodness and richness.

As Mark Mazower observes, it is necessary to consider the "dark side" of the development, in order to avoid the dangers.

The new technologies bring with them a hidden potential of violence, stressed by the relevant role in human life.

Sociologists and psychologists are afraid of the unbalanced relation between man and machine, in which the first one is the slave of the second one.

In fact, many times the computer instruments become a way for the commission (or for a better and fast commission) of a crime.

Everyone would be in condition to know and understand the risks of the progress, in order to avoid them.

This form of perception of the negatives is facilitated by the ways of communication, that allow to know hypothesis of cybercrimes, considered as the crimes committed by or on the computer (or others technological supports).

Remember, for example, the famous case ECHELON, or the case of the website *Wikileaks,* or the case of the serial killer, Matej Curko and so on.

These are only a little part of many news regarding to computer technologies.

The research is due to this social contemporary panorama, from which are developed the analysis on the transnational crimes, uses of new technologies and the problems of EU criminal justice and procedure.

In this field take importance the police and judicial cooperation (as informative cooperation too) between Member States, especially in the fight against transnational crimes, the circulation of e-evidences and the protection of data and of fundamental rights too.

The Lisbon Treaty traces the state of the project of the European space of freedom, security and justice.

The development of the police and judicial cooperation is one of the elements useful for the realization of this objective.

The European law of cooperation and the interpretation made by the European Court of Justice, provide new powers of the EU institutions and also the recognition of the fundamental rights, written in the Nice Charta and in the ECHR.

An integration of the national judicial orders needs the introduction of communitarian laws.

In cooperation material, from the Convention of 1959 to the Bruxelles Convention of 2000, many things are changed.

Out of these conventional instruments, we can consider also others important elements of development, as the Decision of EAW and the Decision of EEW.

Many communitarian bodies are involved in the cooperation and their powers are increased during the time, as Europol, Eurojust and Olaf.

These organisms are really so important in the fight against transnational and cyber crimes, in particular because they have member of every State and a good sight on the general EU space.

The use of new technologies has increased the number of digital evidence, collected and useful for a decision of a criminal proc eeding.

In the european judicial space there is not a common definition of the concept of digital evidence, but every national order use this.

In the USA were developed the first studies in this material, related to the computer forensics, a method of analysis of the e-evidence.

There is not a list of best practices in computer forensics too, but every police organism that use this method has a internal regulation (not binding).

This condition of no common rules and criteria generates many problems to the judicial authorities, called to use or not use for the decision an e-evidence.

But the digital evidence, in a context of fight against serious transnational crimes, needs to circulate between the States involved, balancing the interest of security and justice and the right to privacy.

In order to realize this objective, all the infrastructure for the collection and circulation of data must be secure and controlled by specialized staff.

In the EU (but also in the member States) there are many databases, useful for the collection of electronic evidences and for the circulation of them, in the procedure of police and judicial cooperation.

The most important are SIS II, EPOC III of Eurojust, TECS of Europol, the database of Olaf, ECRIS, VIS, EURODAC and VIS.

Each of these archives has special rules for access, collection and circulation of data and, in general, operational rules applicable.

In these field we have to consider the protection of fundamental rights and of the procedural rights too. In particular, the right of a fair trial, of translation and interpretation, of defence and of privacy.

In a multilanguage EU space, it is more difficult for the police and judicial authorities to cooperate and understand eachother. The increasing of powers of communitarian bodies (Europol, Eurojust and Olaf) and the development con common rules and principles, can realize a better collaboration between member States, as underlined in the Lisbon Treaty.

The Europen Union, as stressed in the project *Europe 2020,*intends to put money for growing up the progress, technical and economical.

The innovation needs a clear common response, by a normative way too.

In many situations is better the choice of mutual recognition, as already known in the European context, in many others is better to harmonize (as possible) the principles and the laws between member States.

Regarding the development of the EU judicial space, especially in criminal law and procedure, the communitarian order focus on the judicial, police and informative cooperation. This is stressed also in the Sthockolm Program and in the Action Plan, in which are provided reforms in these matters.

So, all the European citizen can hope in a EU space of freedom, security and justice and also in a communitarian criminal justice, with guaranties of procedural and fundamental rights, as written in Nice Charta, in ECHR and in the national Constitutions.

BIBLIOGRAFIA

- AA.VV. *Contrasto al terrorismo interno e internazionale (*a cura di R.E. KOSTORIS – R. ORLANDI), Giappichelli, 2006;
- AA.VV., *Cooperazione informativa e giustizia penale nell'Unione europea* (a cura di F. PERONI – M. GIALUZ), CRTrieste, 2009;
- AA.VV., *Corpus juris, pubblico ministero europeo e cooperazione internazionale*, Giuffré, 2003;
- AA. VV., *Decisione giudiziaria e verità scientifica*; Milano, 2005;
- AA.VV., *Enforcing International Law Norms Against Terorism*, Oxford and Portland Oregon, 2004;
- AA.VV., *Il corpus juris 2000. Un modello di tutela penale dei beni giuridici comunitari*, Giuffré, 2003;
- AA.VV., *Il difensore e il pubblico ministero europeo* (a cura di A. LANZI – F. RUGGIERI – L. CAMALDO), Cedam, 2002;
- AA.VV., *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Giuffré, 2011;
- AA.VV., *Mandato d'arresto europeo e garanzia delle persone*, Giuffré, 2004;
- AA.VV., *Prova penale e metodo scientifico*, Utet, 2009;
- ADAM R. – TIZZANO A., *Lineamenti di diritto dell'Unione europea*, Giappichelli, 2010;
- ADAM R., *La cooperazione in materia di giustizia e affari interni tra comunitarizzazione e metodo intergovernativo*, in *Diritto dell'Unione Europea*, 1998, pagg. 491-509;
- ALLEGREZZA S., *L'armonizzazione della prova penale alla luce del Trattato di Lisbona*, in *Cassazione penale*, 2008, 10, pagg. 2000 ss;
- ANODINA E., *Cooperazione-integrazione penale nell'Unione europea*, in *Cassazione penale*, 2001, pagg. 2905 ss;
- APRILE E. – SPIEZIA F., *Cooperazione giudiziaria penale nell'Unione europea prima e dopo il Trattato di Lisbona*, Ipsoa, 2009;

- APRILE E., *Diritto processuale penale europeo e internazionale*, Cedam, 2007
- AQUILA C., *La computer forensics aziendale: alcune problematiche preliminari*, in *Ciberspazio e Diritto*, n. 2, 2008, pagg. 123-131;
- ATERNO S., *La computer forensics tra teoria e prassi: elaborazioni dottrinali e strategie processuali* in *Ciberspazio e Diritto,* 2006, pagg. 67-85;
- BACCASTRINI S. – CERRAI S., *Comprendere la percezione del rischio, praticare la comunicazione sul rischio*, in *Rivista italiana di comunicazione pubblica*, 20, 2004, pagg. 120-126;
- BALAGUER CALLEJON F., *Derecho y Derechos en la Unión Europea*, in J. CORCUERA ATIENZA (a cura di), *La protección de los Derechos Fundamentales en la Unión Europea*, Dykinson, Madrid, 2002;
- BALL K. – WEBSTER F., *The Intensification of Surveillance*, Pluto Press, 2003;
- BALSAMO A., *La decisione quadro sul mandato d'arresto non viola il diritto comunitario*, in *Cassazione penale*, 2007, pagg. 881-886;
- BALSAMO A. – KOSTORIS R.E. (a cura di) *Giurisprudenza europea e processo penale,* Utet, 2008;
- BARBERINI R., *Il giudice e il terrorista*, Einaudi, 2008;
- BARTOLONI M. E., *Articolazione delle competenze e tutela dei diritti fondamentali nelle misure UE contro il terrorismo* in *Il Diritto dell'Unione Europea*, 1, 2009, pagg. 134-162;
- BASSIUONI M. C., *International Terrorism and Political Crimes*, Springfield, 1975;
- BAUCCIO L., *L'accertamento del fatto reato di terrorismo internazionale*, Giuffré, 2006;
- BAUDRILLARD J., *Lo spirito del terrorismo*, Raffaello Cortina Editore, 2002;
- BAZZOCCHI V., *Il mandato di arresto europeo e le Corti supreme nazionali*, in *Il Diritto dell'Unione Europea*, 3, 2007, pagg. 103-125;
- BECK U., *La società del rischio*, Carocci, 2000;

- BELFIORE R., *Il mandato europeo di ricerca della prova e l'assistenza giudiziaria nell'Unione europea*, in *Cassazione penale*, 2008, 10, pagg. 2804 ss;
- BERNARDI A. – GRANDI C., *Gli effetti della prescrizione e dell'amnistia sull'estradizione e sul mandato di arresto europeo*, in *Cassazione penale*, 2005, pagg. 3561-3577;
- BORRUSO R. – BUONOMO G. – CORASANITI G. – D'AIETTI G., *Profili penali dell'informatica*, Giuffré, 1994;
- BRAGHO' G., *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa* in *Diritto dell'Informazione e dell'Informatica,* 2005, fasc. 3, pag. 517 ss;
- BRAGHO' G., *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa*, in *Diritto dell'informazione e dell'informatica*, 2005, pag. 517 ss;
- BRUGALETTA F. – LANDOLFI F.M., *Il diritto nel cyberspazio*, Simone, 1999;
- BRUSCO C., *La valutazione della prova scientifica*, in *Diritto penale e processo*, 2008, Dossier: La prova scientifica nel processo penale, p. 23;
- BRUTI LIBERATI E. – PATRONE I. J., *Il Mandato di Arresto europeo*, in *Questione Giustizia*, 2002, pagg. 70-89;
- CAJANI F. – COSTABILE G. – MAZZARACO G. *Phishing e furto d'identità digitale*, Giuffrè 2008;
- CALVANESE E. – DE AMICIS G., *Commento alla decisione istitutiva di Eurojust* in *Guida al Diritto*, 2002, 24, pagg. 2-11;
- CALVANESE E. – DE AMICIS G., *La Rete giudiziaria europea: natura, problemi e prospettive*, in *Cassazione penale*, 2001, pagg. 706 ss;
- CALVANESE E., *Cooperazione giudiziaria tra Stati e trasmissione spontanea di informazioni: condizioni e limiti di utilizzabilità*, in *Cassazione penale*, 2003, pagg. 449-462;
- CAMERON S., *California's DNA databank joins the modern trend of expansion*, in *Mc George Law Rieview*, 219, 2002;
- CANZIO G., *Prova scientifica, ragionamento probatorio e libero convincimento del giudice penale,* in *Diritto Penale e Processo*, 2003, p. 1193;

- CAPRIOLI F., *Colloqui riservati e prova penale*, Giappichelli, 2000;
- CARBIN G.R. – L. McLAIN, *Does computer-generated evidences need its own Rules? Maryland adopts standards for animations simulations*, in *Computer Law Strategis*t, 2, 1998;
- CARTABIA M., *I diritti fondamentali in Europa dopo Lisbona: verso nuovi equilibri?*, in *Giornale di Diritto Amministrativo*, 3, 2010, pagg. 221-225;
- CASEY E., *Digital evidence and computer crime: forensic science, computers and the internet,* Elsevier, 2004;
- CASEY E., *Network traffic as a source of evidence: tool strenghts, weaknesses and future needs* in *Digital investigation*, 2004, 1, pagg. 28-43;
- CASTELLANETA M., *L'obbligo di conformarsi a decisioni precedenti rende difficile il contrasto all'abuso del diritto*, in *Guida al Diritto*, 37, 2009, pagg. 71-73;
- CATALANO E. M., *Molte incertezze e piccoli passi nel percorso di europeizzazione del diritto processuale penale*, in *Diritto Penale e Processo*, 4, 2007, pagg. 522-530;
- CERRI A. *Riservatezza (voce)* in *Enciclopedia Giuridica Treccani, Istituto Poligrafico e Zecca dello Stato*, 1991;
- CHIAVARIO M. (a cura di), *Nuove tecnologie e processo penale*, Giappichelli, 2003;
- CHIAVARIO M., *Cooperazione giudiziaria e di polizia in materia penale a livello europeo*, in *Rivista italiana di diritto e procedura penale*, 2005, pagg. 957 ss;
- CHIAVARIO M., *Giustizia: il mandato di cattura europeo mette a nudo le contraddizioni italiane*, in *Guida al Diritto*, 2001, pagg. 11 ss;
- CHIAVARIO M., *Giusto processo (voce),* in *Enciclopedia giuridica Treccani*, 2001;
- CHIRIZZI L., *Computer Forensics, il reperimento della fonte di prova informatica*, Laurus Robuffo, 2006;
- CIPRIANI S., *La protezione penale della riservatezza in diritto comparato italiano e francese*, in Rivista italiana di diritto e procedura penale, 1997, pag. 86 ss;

- COLOMBO E., *La sentenza del caso di Garlasco e la computer forensics: analisi di un complesso rapporto tra diritto ed informatica*, in *Ciberspazio e Diritto*, 3, 2010;
- COMOGLIO L. P., *L'informazione difensiva nella cooperazione giudiziaria europea*, in *Rivista di Diritto Processuale*, 3, 2006, pagg. 861-863;
- CONFORTI B., *Diritto internazionale*, Edizione Scientifica, 2002;
- CONTI P. (a cura di) *Intervista su privacy e libertà,* Laterza, 2005;
- COSTABILE G. – RASETTI D., *Scena criminis, tracce informatiche e formazione della prova*, in *Ciberspazio e Diritto*, 3-4, 2003;
- COSTABILE G., *Scena criminis*, *Documento informatico e formazione della prova penale*, in *Diritto dell'Informazione e dell'Informatica*, 2005, pag. 532;
- CUOMO L. – R. RAZZANTE *La disciplina dei reati informatici*, Giappichelli, 2007;
- D'ANGELO L., *La conservazione dei dati di traffico telefonico e telematico tra esigenze investigative e tutela della privacy*, in AA.VV., *Le nuove norme di contrasto al terrorismo*, (a cura di) A.A. DALIA, Giuffré, 2006;
- DAQUI G., *La prova scientifica e lo spazio del libero convincimento* in L. DE CATALDO NEUBURGER (a cura di) *Prova scientifica e processo penale*, pag. 70 ss.;
- DE AMICIS G. – SANTALUCIA G., *L'attuazione di Eurojust nell'ordinamento italiano: prime riflessioni sulla legge 14 marzo 2005, n. 41*, in *Cassazione penale*, 2005, pagg. 726 ss;
- DE AMICIS G. – VILLONI O., *Mandato di arresto europeo e legalità penale nell'interpretazione della Corte di Giustizia*, in *Cassazione penale*, 2008, pagg. 383-405;
- DE AMICIS G., *Attuazione del mandato d'arresto europeo e tutela dei diritti fondamentali: ambito di applicazione e limiti delle garanzie procedurali a favore di indagati e imputati nel territorio dell'Unione europea*, in *Quaderni del Consiglio Superiore della Magistratura*, 148, 2006;
- DE CATALDO NEUBURGER L., *La prova scientifica nel processo penale*, Cedam 2007;
- DE HERT P. – GUTWIRTH S., *Interoperability of police databases within the EU: an accountable political choice?*, in *http://ssrn.com/abstract=971855*;

- DELL'OSSO P. L. M., *Rapporto sulla rete giudiziaria europea*, in *Rivista italiana di diritto processuale penale*, 2005, pagg. 1540 ss;
- DELMAS MARTY M. – IZORCHE M. L., *Marge nationale d'appréciation et internationalization du droit* in *Revue international du droit compare*, 2000, pagg. 753 ss;
- DELMAS-MARTY M., *Procédures pénales d'Europe,* Press Universitaires de France, 1995;
- DENNING D. E., *Cyberterrorism,* Georgetown University Press, 2000;
- DESTITO V. S. – DEZZANI G. – SANTORIELLO C., *Il diritto penale delle nuove tecnologie*, Cedam, 2007;
- DI FEDE C., *Una valutazione dell'apporto della rete all'azione terroristica*, in *Rivista trimestrale di Scienza dell'Amministrazione*, n. 3, 2004, pagg. 63-69;
- DOMINIONI O., *La prova penale scientifica*, Giuffré 2005.
- DONDI A., *Problemi di utilizzazione di conoscenze esperte, come export witness testimony nell'ordinamento statunitense*, in *Rivista trimestrale di diritto processuale civile*, 2001, pagg. 1133 ss;
- DURANTE M., *Il futuro del web: etica, diritto, decentramento*, Giappichelli, 2007;
- EPIFANI M., *Analisi di telefoni cellulari in ambito giuridico*, in *Ciberspazio e Diritto*, 10, 2009, pagg. 83-98;
- EPIFANI M., *Computer forensics: percorsi formativi in Italia e certificazioni internazionali*, in *Ciberspazio e Diritto*, 3-4, 2009, pagg. 311-324;
- FABBRICATORE A., *Caso Pupino: sul riconoscimento dell'efficacia diretta delle decisioni quadro*, in *Diritto Penale e Processo*, 2006, pag. 640-646;
- FANEGO C. A., *Proposta di decisione quadro su determinati diritti processuali nei procedimenti penali nel territorio dell'Unione europea*, in *Cassazione penale*, 2008, pagg. 3042 ss;
- FANUELE C., *Dati genetici e procedimento penale*, Giuffré, 2009.
- FANUELE C., *Un archivio centrale per i profili del DNA nella prospettiva di un diritto comune europeo*, in *Diritto Penale e Processo*, 2007, pagg. 387-401;

- FERRARA R., *Premesse ad uno studio sulle banche dati della pubblica amministrazione: fra regole della concorrenza e tutela della persona* in *Diritto amministrativo*, 1997, pagg. 555 ss;
- FERRARI BRAVO L. – DI MAJO F. M. – RIZZO A. (a cura di), *Carta dei diritti fondamentali dell'Unione europea commentata*, Giuffré 2001;
- FERRARI G.F., *La legge sulla privacy dieci anni dopo,* Egea, 2008;
- FLETCHER M., *The European Court of Justice. Carving Itself an influential role in the EU's Third Pillar* in *www.unc.edu/euce/eusa 2007/papers/fletcher-m-08i.pdf*;
- FLORA G., *Profili penali del terrorismo internazionale tra delirio di onnipotenza e sindrome di auto castrazione*, in *Rivista Italiana di diritto e procedura penale*, 2008, pagg. 62-80;
- FOX R., *Someone to watch over us: back to the panopticon?*, in *Criminal Justice,* 2001, pag. 261;
- FROSINI V., *La criminalità informatica in Diritto dell'Informazione e dell'Informatica*, 1997, pag. 488;
- GALANTINI N., *Prime osservazioni sul mandato di arresto europeo*, in *Foro Ambrosiano*, 2002, pagg. 264 ss;
- GAMBINI R., *Armonizzazione dei diritti nazionali nel segno della giurisprudenza europea*, in *Diritto Penale e Processo*, 9, 2009, pagg. 1169-1174.
- GARAPPA N., *Internet e diritto penale*, in *www.diritto.it*;
- GHIRARDINI A. – FAGGIOLI G., *Computer forensics: il panorama giuridico italiano*, in *Ciberspazio e Diritto*, 3-4, 2007, pagg. 324-384;
- GHIRARDINI A. – G. FAGGIOLI, *Computer forensics*, Giuffré, 2007;
- GIUSTOZZI C. – MONTI A. – ZIMUEL E., *Segreti, spie e codici cifrati*, Apogeo, 1999;
- HARRIS D.J. – O'BOYLE M. –WARBRICK C., *Law of the European Conventionon Human Rights*, Preston Press, 1995;
- HEMPEL L. – CARIUS M. – ILTEN C., *Exchange of information and data between law enforcement authorities within the European Union*, in *www.statewatch.org/news/2009/apr/Study_Exchange%200f%20information%*

20and%20data%20between%20law%20lawenforcement%20authorities%20within%20the%20EU_EN.pdf;

- HERBOTS J. B., *La tradution juridique. Un point de vue belge*, in *Cahiers de droit*, 1987, pagg. 813-844;
- INSOLERA G., *Reati associativi, delitto politico e terrorismo globale*, in *Diritto Penale e Processo*, n. 11, 2004, pagg. 1325-1330;
- KAIESER P., *Le secret de la vie privée,* Dalloz, 1965;
- LATTANZI G., *Costretti dalla Corte di Strasburgo* in *Cassazione Penale*, 2005, pagg. 1125-1132;
- LAUDATI A., *I delitti transnazionali:. Nuovi modelli di incriminazione e di procedimento all'interno dell'Unione europea*, in *Diritto Penale e Processo*, 4, 2006, pagg. 401-405;
- LEONE L., *La manipolazione digitale dei fotogrammi*, in *Ciberspazio e Diritto*, 3-4, 2007, pagg. 289-308;
- LUHMANN N., *Sociologia del rischio*, Bruno Mondadori, 1996;
- MANES V. – ZAGREBELSKY V. (a cura di), *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Giuffré, 2011;
- MARINI A., *Il terrorismo internazionale oggi: brevi spunti di riflessione*, in *Iustitia*, 2, 2009, pagg. 133-140;
- MARTELLO S. *Sulla partecipazione e sulla comunicazione nella Rete: riflessioni operative e giuridiche*, in *Ciberspazio e Diritto*, 10, 2009, pag. 33, nota 14;
- MASON S., *Electronic Evidence*, Butterworths, 2010;
- MASSA R.G., *Le vere origini della computer forensics* in *ComputerLaw Informatica e Diritto (http://www.computerlaw.it/entry.asp?entry_ID=200*);
- MATTIUCCI M. – G. DELFINIS, *Forensic Computing* in *Rassegna dell'Arma dei Carabinieri*, 2006, 2, pag. 54;
- MAZOWER M. A., *Il lato oscuro della modernità. La violenza e lo Stato nel XX secolo*, in *Lettera internazionale*, II trimestre, 2008, pag. 25;
- MILITELLO V. –PAOLI L. – ARNOLD J. (a cura di), *Il crimine organizzato come fenomeno transnazionale*, Giuffré, 2000;

- MODUGNO F., *I "nuovi" diritti nella Giurisprudenza costituzionale,* Giappichelli, 1995, pag. 20;
- MORCELLINI M., *L'informazione e la percezione della sicurezza*, in *Rivista italiana di comunicazione pubblica*, 34, 2007, pagg. 68-80;
- MORGAN G., *The idea of a Europea super statw. Public justification and european integration*, Princeton University Press, 2005;
- MUSACCHIO V., *Le strategie di lotta al terrorismo internazionale* in *Rivista Penale*, 3, 2006, pagg. 273-280;
- NASCIMBENE B., *Cooperazione giudiziaria penale: diritto vigente e orientamenti futuri nel quadro della Costituzione europea*, in *Diritto penale e processo*, 10, 2004, pagg. 1295- 1306;
- OLIMPO G., *La testa del serpente. Tutti i segreti di Osama Bin Laden*, Nuovo Istituto Italiano d'Arti Grafiche, 2011;
- PAGALLO U., *La tutela della privacy negli Stati Uniti d'America e in Europa,* Giuffré, 2008;
- PAGOTTO A., *La cooperazione in campo investigativo* in *www.csm.it*;
- PALMER G., *Forensics Analysis in a Digital World*, in *htttp://ijde.org/archives/ gary_article.html";*
- PANUNZIO S. (a cura di), *I diritti fondamentali e le Corti in Europa,* Jovene, 2005;
- PANZAVOLTA M., *Eurojust: il braccio giudiziario dell'Unione*, in AA.VV. *Profili del processo penale nella costituzione europea*, Giappichelli, 2005;
- PAOLUCCI C. M., *Cooperazione giudiziaria e di polizia in materia penale*, Utet, 2011;
- PARISI N., *Su taluni limiti nell'attività di ricerca e acquisizione della prova penale nei reati informatici*, in *Studi in onore di Mario Pisani*, La Tribuna, 2010, pagg. 443-445;
- PECCIOLI A., *Il terrorismo quale settore chiave per l'armonizzazione del diritto penale*, in *Diritto Penale e Processo*, n. 6, 2007, pagg. 801-807;
- PERDUCA A., *Le indagini dell'ufficio europeo per la lotta antifrode (OLAF) ed i rapporti con le autorità giudiziarie*, in *Cassazione penale*, 12, 2006, pagg. 4242-4251;

- PIATTOLI B., *Mandato di arresto europeo: istanze di armonizzazione processuale, distonie applicative e tutela multilivello dei diritti fondamentali*, in *Diritto penale e processo*, 2007, 8, pag. 1108;
- PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Cedam, 2004;
- PINO M., D'ALOIA M., *La prova scientifica nel processo penale: il requisito della formazione*, in *La prova scientifica nel processo penale*, (a cura di) L. DE CATALDO NEUBURGER, Cedam, 2007, pagg. 104 ss;
- PIOMBO J. R., *Terrorism and U.S. Counter-Terrorism Programs in Africa: an overview*, in *www.centerforcontemporaryconflict.int*;
- PIRO N., *Cyberterrorismo*, Castelvecchi, 1998;
- PITSCHAS R., *Informationelle Selbstbestimmung zwischen digitaler Okonomie und Internet*, *DuD*, 2000, 1998, pag. 139;
- POLLICINO O., *Incontri e scontri tra ordinamenti e interazioni tra giudici nella nuova stagione del costituzionalismo europeo: la saga del mandato di arresto europeo come modello d'analisi*, in *http://www.ejls.eu/4/58IT.htm*;
- POZZO B. – JACOMETTI V. (a cura di), *Le politiche linguistiche delle istituzioni comunitarie dopo l'allargamento*, Giuffré, 2006;
- POZZO B. (a cura di), *Ordinary language and legale language*, Giuffré, 2005;
- PRATO F., *I rapporti di Eurojust con Europol, Olaf e gli Stati terzi*, in *www.cosmag.it*;
- QUADARELLA L., *Il nuovo terrorismo internazionale come crimine contro l'umanità*, Editoriale Scientifica, 2006;
- RIONDATO S., *Competenza penale della Comunità europea*, Cedam, 1996;
- RODOTA' S., *Tecnologie e diritti,* Il Mulino, 1996;
- ROMOLI F., *Il nuovo volto dell'Europa dopo il Trattato di Lisbona*, in *Archivio penale*, 1, 2011, pagg. 155-160.
- SALTARI L., *Il riparto di competenza tra l'Unione europea e gli Stati: ossificazione o fluidità?*, in *Giornale di Diritto Amministrativo*, 3, 2010, pagg. 231-236;

- SAMMARCO P., *Circolazione, contaminazione e armonizzazione nella disciplina delle nuove tecnologie della comunicazione*, in *Diritto dell'informazione dell'informatica*, 2008, pag. 711 ss;
- SARTORETTI C., *Contributo allo studio della privacy nell'ordinamento costituzionale,* Giappichelli, 2008, pag. 21;
- SAVINO M., *La Pesc e lo spazio di libertà, sicurezza e giustizia*, in *Giornale di Diritto Amministrativo*, 3, 2010, pagg. 226-231;
- SCHULZ W., *Verfassungrechtlicher "Datenschutzauftrag"*, in *Der Informationsgesellschaft, Die Verwaltung*, 1999, pag. 137;
- SCIARABBA V., *Misure antiterrorismo e diritti fondamentali: c'è un giudice a Lussmeburgo, ora anche due* (*intervenuta la Corte, il Tribunale si adegua*), in *Diritto pubblico comparato ed europeo*, 4, 2009, pagg. 201-207;
- SELVAGGI E., *Il mandato di arresto europeo alla prova dei fatti*, in *Cassazione penale*, 2002, pagg. 1978 ss;
- SELVAGGI E., *L'arabo, il parto, il siro in suoo sermon l'udì: riflessioni sulla Babele delle lingue nei rapporti giurisdizionali con autorità straniere*, in *Scritti in onore di Mario Pisani*, La Tribuna, 2010;
- SELVAGGI E., *La rete giudiziaria europea: uno strumento per migliorare la cooperazione giudiziaria in materia penale*, in *Documento giustizia*, 2000, pagg. 1123 ss.;
- SERRANO' A., *Le armi nazionali contro il terrorismo contemporaneo*, Giuffré, 2009;
- SIMONS A. – TUCKER D., *The Misleading Problem of Failed States: a socio-geography of terrorism in the post-9/11 era* in *Third World Quarterly*, 2, 2007, pagg. 387-401;
- SINCLAIR A., *An anatomy of terror,* Pan Books, 2003;
- SINGH S., *Codici & segreti*, BUR, 1999;
- SPRONKEN T. – VERMEULEN G. – DE VOCHT D. – VAN PUYENBROECK L. EU, *Procedural Rights*, in *The Criminal Proceedings*, Maklu, 2009;
- TADDEI ELMI G., *Informatica e diritto: un binomio irreversibile*, in AA.VV., *Il codice dei dati personali. Temi e problemi*, a cura di G. TADDEI ELMI, Giuffrè, 2006;

- TONINI P., *Manuale di procedura penale*, Giuffrè, 2005;
- TONINI P., *Progresso tecnologico, prova scientifica e contraddittorio*, in L. DE CATALDO NEUBURGER *La prova scientifica nel processo penale*, pag. 49 ss.;
- TORRE V., *La gestione del rischio nella disciplina del trattamento dei dati personali*, in AA.VV., *Il diritto penale dell'informatica nell'epoca di internet*, a cura di L. PICOTTI, Cedam, 2004, pag. 240 ss.;
- TRACOGNA C., *La tutela della libertà personale nel procedimento di consegna attivato dal mandato d'arresto europeo*, in *Rivista Italiana di Diritto e Procedura Penale,* 2007, pagg. 988-1020;
- TUMAN J. S., *Communicating terror*, SAGE Publications, 2003;
- TZOUMAS A., *Maryland sets new standard for computer-generated evidence admissibility* in *Inside Litigation*, 4, 1998, pagg. 18 ss.;
- VALVO A. L., *L'Unione europea dal Trattato costituzionale al Trattato di Lisbona*, Aracne editrice, 2008;
- VERVAELE J. A. E., *European Evidence Warrant*, Intersentia, 2005;
- VERVAELE J. A. E., *L'europeizzazione del diritto penale e la dimensione penale dell'integrazione europea*, in *Rivista Trimestrale di diritto penale dell'economia*, 2005, pagg. 142 ss;
- VIGANO' F., *Terrorismo, guerra e sistema penale*, in *Rivista Italiana di diritto e procedura penale*, 2006, pagg. 648-703;
- VILLANI U., *I diritti fondamentali tra Carta di Nizza, Convenzione europea dei diritti dell'uomo e progetto di Costituzione europea*, in *Diritto dell'Unione europea*, 2004, I, pagg. 73-116;
- WARREN S.D. – BRANDEIS L.D., *The right to privacy* in *Harvard Law Review,* 4, 1890, pagg. 193 ss;
- WEILER I., *La costituzione dell'Europa*, Il Mulino, 2003;
- ZICCARDI G. – CAPALDO, *Terrorismo internazionale e garanzie collettive*, Giuffré, 1990;
- ZICCARDI G. – L. LUPARIA, *Investigazione penale e tecnologia informatica*, Giuffré 2007;
- ZICCARDI G., *Crittografia e diritto*, Giappichelli 2003;

∂ ZICCARDI G., *Informatica, comportamenti e diritto: dalla computer ethics alla computer forensics*, in *Ciberspazio e Diritto*, 4, 2008, pagg. 395-445;

SITOLOGIA

- http://curia.europa.eu
- http://ec.europa.eu/index_it.htm
- http://eur-lex.europa.eu/it/index.htm
- http://iate.europa.eu
- www.camera.it
- www.cnil.fr
- www.coe.int
- www.computerlaw.it
- www.cordis.lu/ist
- www.cortecostituzionale.it
- www.cosmag.it
- www.csm.it
- www.diritto.it
- www.dirittopenaleeuropeo.it
- www.ec.europa.eu/dgs/olaf
- www.echr.coe.int
- www.era.europa.eu
- www.eurojust.europa.eu
- www.europarl.europa.eu
- www.european-council.europa.eu
- www.europeanrights.eu
- www.europol.europa.eu
- www.fbi.gov
- www.gocsi.com

- www.iacis.com
- www.ic3cert.it
- www.iisfa.it
- www.ists.org
- www.marcomattiucci.it
- www.mpicc.de/eucrim/
- www.penalecontemporaneo.it
- www.symantec.com/it/it/index.jsp