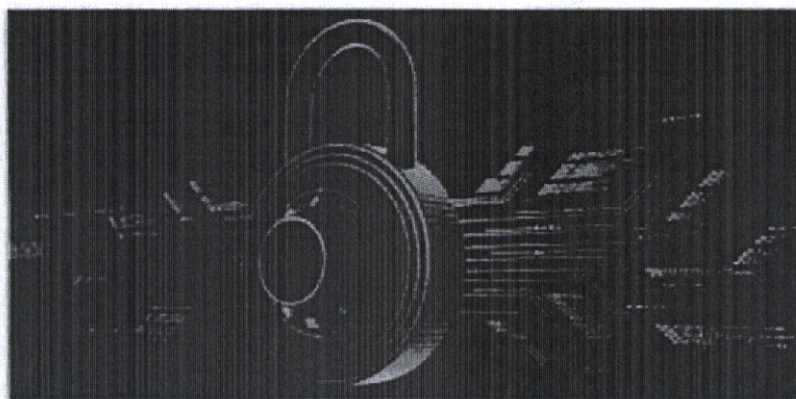


Più nel dettaglio, lo scopo dichiarato della riforma é - tra l'altro - di diminuire la burocrazia, aumentare *"leadership e management"* degli AWFs, standardizzare le procedure, aumentare la flessibilità nella distribuzione dei carichi di lavoro, facilitare la possibilità di trasferimento dei dati da un AWF all'altro, aumentare la capacità d'individuazione di *"trend"* e strutture criminali, supportare con maggiore aderenza le competenti Autorità di polizia, accrescere la qualità delle risposte diminuendo i tempi di attesa.

E' stato altresì osservato che l'incremento degli AWF (23 al momento della massima espansione), ai quali deve necessariamente essere assegnato un certo numero di analisti, stava *"diluendo"* il potenziale degli specialisti di analisi dell'agenzia. Nella *"Europol review"* del 2012, un rapporto generale annuale sull'attività dell'Agenzia, Europol dichiarava una presenza di 92 analisti su un totale di 777 elementi dello *staff* che, nel vecchio sistema, dovevano essere ripartiti tra 23 AWFs. Con il nuovo concetto gli AWFs si riducono a due: *Serious and Organized Crime* e *Counter Terrorism* e i *database* già denominati AWFs assumono ora la collocazione visualizzabile in figura, interna ai due nuovi archivi, e vengono ridenominati *Focal Point* (23 *Focal Point* in due AWFs: SOC e CT). Gli analisti, ripartiti tra i due nuovi AWFs, vengono dedicati ai *Focal Point* secondo esigenza superando le vecchie e complesse procedure autorizzatorie cui era, in passato, subordinato il loro transito da un AWF all'altro.

**6. Sicurezza delle informazioni**

Un altro importante aspetto in connessione con i *database* di Europol è la sicurezza delle informazioni. Le misure di sicurezza sono reputate essenziali non appena dati personali o sensibili strategici vengono trattati. Sotto il regime dell'ECD Europol ha l'obbligo di accrescere le tecnologie e le misure organizzative necessarie per proteggere i suoi dati (art. 35 ECD). Conseguentemente sono stati realizzati alcuni dispositivi tecnologici ad Europol per prevenire l'accesso o l'uso non autorizzato dei dati. Sono altresì garantite protezioni concrete contro la perdita di dati o il malfunzionamento dei sistemi.

L'accesso alle informazioni e il loro maneggio è definito e ristretto da una classificazione applicabile. L'agenzia individua tre tipi di informazioni Europol:

*Europol public information;*

*Europol Unclassified - Basic Protection Level Information;*

*Europol classified information.*

Le *Europol classified information* sono ulteriormente suddivise in quattro sottocategorie a seconda del potenziale impatto che potrebbe essere causato da un accesso non autorizzato:

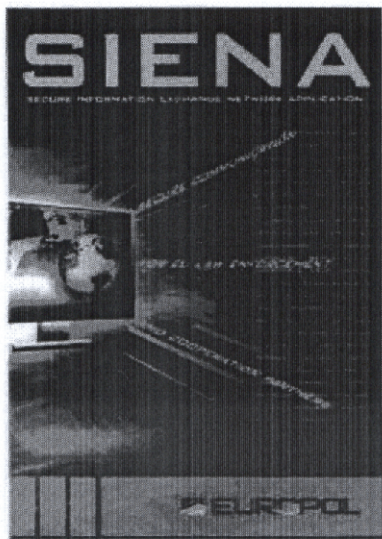
**EU RESTRICTED;**

**EU CONFIDENTIAL;**

**EU SECRET;**

**EU TOP SECRET.**

A ciascun tipo d'informazioni si affianca un *set* di misure di sicurezza che deve essere applicato per proteggerle contro gli accessi non autorizzati. Per esempio, le informazioni catalogate come *EU Confidential* o superiori possono solo essere create o riprodotte attraverso ufficiali appositamente autorizzati utilizzando speciali e sicuri equipaggiamenti in modo da assicurare la piena tracciabilità dei testi scritti.

**7. SIENA**

Dopo la presentazione del principale sistema di Europol per il trattamento dei dati e il suo approccio generale verso la sicurezza delle informazioni occorre chiarire come queste informazioni prendano la loro via nel sistema Europol.

Poiché l'agenzia è essenzialmente concentrata sullo scambio d'informazioni, la sicurezza e la velocità di trasmissione dei dati di pertinenza è ritenuta essenziale. Le informazioni da uno Stato membro devono poter raggiungere Europol senza rischi d'intercettazione e vice versa. Al fine di scambiare informazioni velocemente e in sicurezza, è stato progettato da Europol un sistema *ad hoc* denominato *Secure Information Exchange Network Application* – SIENA.

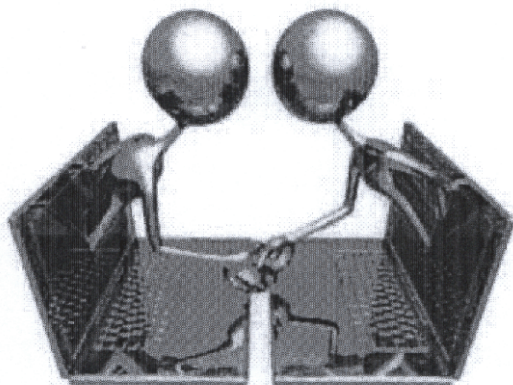
Così come avviene per la custodia e l'analisi dei dati, la trasmissione dei dati da e verso Europol deve avvenire nel rispetto dei principi di protezione dei dati e della salvaguardia della sicurezza delle informazioni. La piattaforma informatica SIENA, ospitata in un ambiente sicuro del nuovo Quartier Generale di Europol, permette agli Stati membri, alle parti terze e ad Europol di comunicare velocemente e in modo sicuro attraverso un canale di comunicazione di agevole uso. Europol è obbligata a tenere registrazioni della trasmissione dei dati. In forza di tale esigenza, il SIENA documenta automaticamente tutti i processi di comunicazione. Per garantire ulteriormente il maneggio responsabile dei dati personali, l'informazione è trasmessa da Europol ad altri *partners* solo se il ricevente dà assicurazione che i dati saranno usati per gli scopi per i quali sono stati trasmessi<sup>23</sup>.

<sup>23</sup> Art. 24 (2) ECD.

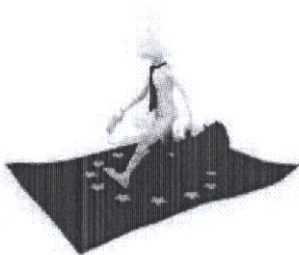
**8. Gli uffici di collegamento - LB**

Le disposizioni tecniche per lo scambio di informazioni sono ottimizzate con il concetto unico di uffici di collegamento presso Europol. Ciascuno Stato membro invia almeno un rappresentante al Quartier Generale di Europol che, a sua volta, garantisce a ciascuno Stato membro la disponibilità dei locali necessari (art. 9 ECD). Inoltre, gli Stati terzi che hanno concluso con Europol un accordo di cooperazione sono rappresentati da almeno un Ufficiale di collegamento, come accade per INTERPOL. Complessivamente gli Ufficiali di collegamento di 36 Paesi più INTERPOL sono collocati in un'area comune di Europol, rendendo le comunicazioni tra loro e le loro rispettive autorità nazionali facili e veloci. Gli Ufficiali di collegamento sono presenti e/o reperibili 24 ore al giorno, sette giorni su sette, in contatto con le loro Unità nazionali designate (art. 8 ECD) via SIENA. Gli agenti delle forze di polizia dei Paesi partecipanti indirizzano richieste e messaggi all'Unità Nazionale che li invia agli Uffici di collegamento. In questo modo, le barriere di linguaggio sono effettivamente superate: gli Ufficiali di collegamento possono comunicare con le UNE nella loro lingua madre ricevendo una risposta nella stessa lingua. Queste capacità di traduzione unita alla prossimità degli uffici sono considerati da Europol come risorse dai risvolti estremamente positivi per l'esecuzione di ogni operazione transfrontaliera.

L'Italia, in questo momento, distacca dall'UNE quattro Ufficiali di collegamento (uno in meno rispetto allo scorso anno) presso il proprio LB (tre funzionari, rispettivamente della P di S, dei CC e della G di F, più un Ispettore della P di S).

**9. Acquisizione d'informazioni extra Europol**

Le regole di protezione dei dati sono applicate a tutte le forme di scambio di dati personali tra Europol e gli Stati membri. Tuttavia, la rete d'informazioni di Europol si estende oltre i Paesi dell'UE. Riconoscendo come le informazioni delle parti terze possano essere in molti casi benefiche, Europol mantiene numerosi contatti esterni e accordi di cooperazione. Per ciascun sistema di comunicazione di dati con entità esterne sono state realizzate nell'ECD regole forti per garantire che i suoi *standard* siano applicati anche in questi casi. Per esempio, i dati non possono essere trasmessi a entità terze senza il preventivo consenso del legittimo proprietario (art. 24, comma 1 ECD). Poiché le parti terze non sono soggette al regime di protezione dei dati dell'ECD, Europol deve assicurare che sia comunque attuato un adeguato livello di tutela delle informazioni; tanto con riferimento alla protezione dei diritti e delle libertà fondamentali dei soggetti cui le informazioni si riferiscono quanto con riguardo al trattamento di tali dati, così come ai rischi in tema di sicurezza nel trasferimento d'informazioni classificate.

**Istituzioni dell'UE**

Per quanto riguarda lo scambio di dati tra istituzioni europee, l'art. 22 dell'ECD prevede una base per Europol per stabilire e mantenere relazioni di cooperazione con una serie d'istituzioni e agenzie europee, come Eurojust, la BCE o l'Ufficio europeo antifrode (OLAF). Dove accordi non

sono ancora stati conclusi, Europol può ancora scambiare informazioni, inclusi dati personali, attestando che lo scambio è necessario per i compiti dei destinatari.

### Parti terze



Le relazioni di Europol non sono limitate agli Stati membri e alle istituzioni dell'UE. Tenuto conto della transnazionalità dei fenomeni criminali Europol ritiene vitale cooperare con Stati o istituzioni al di fuori dell'area europea. Queste relazioni con Parti terze sono regolate dall'art. 23 dell'ECD.

In generale, ci sono due tipi di accordi di cooperazione che Europol può avviare con Stati o entità terze: strategici e operativi.

Gli accordi strategici permettono lo scambio delle c.d. *general intelligence* e sono stati conclusi con Albania, Bosnia – Erzegovina, Colombia, FYROM, Moldavia, Montenegro, Russia, Serbia, Turchia e Ucraina<sup>24</sup> (art. 23 comma 8 ECD). Europol ha anche concluso un accordo con l'Ufficio delle Nazioni Unite contro la droga e il crimine e l'Organizzazione mondiale delle dogane.

I dati personali possono, tuttavia, essere scambiati solo dove è in atto un accordo di cooperazione operativo. Europol può concludere tale accordo con una parte terza che deve però garantire un adeguato livello di protezione dei dati.

Il processo per concludere un accordo di cooperazione operativo con parti terze comporta una preventiva valutazione finalizzata a comprendere se la parte terza sia in grado di assicurare il necessario regime di protezione dei dati e se le regole sulla riservatezza delle informazioni sono state realizzate e sono effettivamente in uso.

Gli Stati con i quali sono stati conclusi accordi di cooperazione operativa sono l'Australia, il Canada, la Croazia, FYROM, l'Islanda, Monaco, la Norvegia, la Svizzera e gli USA. Europol ha inoltre un accordo di cooperazione operativa con Interpol e Eurojust. Accordi di cooperazione operativa già conclusi per i quali pende ancora un processo di ratifica in accordo con l'applicabilità della legislazione nazionale esistono con la Colombia<sup>25</sup>.

Eccezionalmente, e in assenza di accordi di cooperazione operativa, i dati personali possono solo essere trasmessi sotto le più strette condizioni. Uno scenario particolare è quello c.d. della *"ticking bomb"* (ticchettio della bomba) finalizzato a gestire una minaccia imminente là dove Europol non possa reagire in tempo perché le informazioni non possono essere scambiate per mancanza di un accordo di cooperazione operativa. Il regime di protezione dei dati di Europol tiene conto di questa situazione individuandola come caso specifico di esenzione dai limiti vigenti. Europol può comunque trasmettere dati personali se il Direttore ritenga assolutamente necessario salvaguardare gli interessi essenziali degli Stati membri nell'ambito degli obiettivi di Europol o al

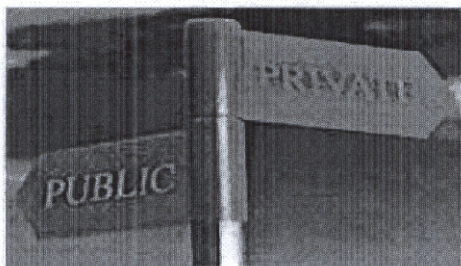
<sup>24</sup> Situazione a novembre 2012.

<sup>25</sup> Situazione novembre 2011.

fine di evitare un pericolo imminente associato alla criminalità o a reati terroristici (art. 23 comma 8 ECD).

E' anche possibile che un flusso d'informazioni a senso unico da Parti terze a Europol possa essere consentito prima dell'entrata in vigore dell'accordo di cooperazione operativo. Tuttavia, la Parte terza in questione, deve almeno essere inclusa in una predefinita lista del Consiglio di potenziali futuri *partner* di cooperazione con Europol.

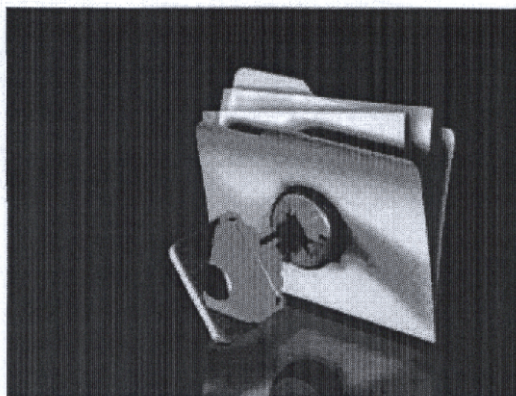
### Parti private



Oltre agli Stati e alle istituzioni come Interpol e Eurojust, Europol può anche ricevere informazioni dalle Parti private come ad es. entità od organi costituiti secondo la legge di uno Stato, società, associazioni professionali e organizzazioni senza scopi di lucro. Come per ogni altro trasferimento di dati personali, anche questo processo è soggetto al controllo sulla protezione dei dati. In particolare, la possibilità di stabilire il percorso delle informazioni da una parte privata a Europol dipende da quale tipo di legge è chiamata in causa. Se la parte privata è istituita sotto la legge di uno Stato membro (per esempio una *GmbH* tedesca o una *Ltd.* Britannica), i dati personali della parte potranno essere trattati solo se sono stati trasmessi attraverso le rispettive UNE (in questo caso il *Bundeskriminalamt* tedesco o il britannico *Serious Organised Crime Agency*). Questa pratica assicura che le rispettive legislazioni nazionali siano state rispettate, incluse ogni tipo di salvaguardia della protezione dei dati. In modo corrispondente, dove una parte privata è stata istituita sotto la legge di uno Stato membro con il quale Europol ha concluso un accordo di cooperazione operativa, i dati personali possono solo essere incanalati attraverso il punto di contatto designato dello Stato. Dove non c'è accordo un accordo di tal tipo in atto, Europol può solo trattare il dato sulla base di un *memorandum* d'intesa che è esso stesso soggetto a un certo numero di requisiti di sicurezza. L'opzione di ottenere informazioni da parti private viene considerata da Europol una significativa risorsa per il concreto sviluppo delle investigazioni. Reputa ancora Europol che, con tali relazioni, l'organizzazione possa accrescere le sue capacità di *expertise* e di conoscenza ed esplorare nuovi metodi ed approcci. La cooperazione con specialisti esterni provenienti da aree diverse come il mondo accademico, associazioni di categoria e aziende private, come previsto dal programma di *Outreach* di Europol, secondo quest'ultima, presenta vantaggi inestimabili per la continua evoluzione dell'Agenzia.

**Fonti disponibili pubblicamente**

Sotto l'ECD Europol può anche ricercare direttamente e trattare informazioni che includono dati personali da fonti d'informazioni disponibili pubblicamente, come *media* e dati pubblici di fornitori commerciali d'*intelligence*. L'attività principale di questa branca di analisi sono i criminali e i gruppi terroristici, in particolare poiché spesso essi comunicano attraverso siti pubblici. Questi gruppi argomentano minacciosamente, rivendicano il merito di attacchi o la diffusione di materiali d'indottrinamento via *internet* e diffondono i c.d. "*terror manuals*" che offrono istruzioni dettagliate su come organizzare attacchi o costruire armi e ordigni esplosivi. Europol ha la capacità di monitorare questi siti ed analizzare le loro informazioni. Europol ritiene la capacità di visualizzare questi fenomeni da una prospettiva dell'UE, un significativo valore aggiunto. La valutazione di grandi quantità di dati e l'approfondito esame d'innomerevoli pagine *web* in differenti linguaggi, sostiene Europol, richiedono considerevoli risorse umane e tecniche che potrebbero non essere disponibili a un singolo Stato membro. L'Agenzia ha perciò aggiunto il portale *Check the Web* ai suoi AWFs, dove vengono raccolte e trattate rilevanti informazioni tratte da siti pubblici per offrire agli esperti nazionali una visione globale delle attività terroristiche di matrice islamica. Simili iniziative riguardanti altri fenomeni criminali sono al vaglio.

**10. L'Ufficio di protezione dei dati - DPO**

Il quadro di protezione dei dati in vigore presso l'Europol è uno dei più forti al mondo. Tuttavia, il fatto di avere un robusto set di norme e regolamenti non è sufficiente a garantire un'efficace protezione dei dati nella pratica. Di conseguenza, diverse entità monitorano e garantiscono il rispetto delle norme sulla protezione dei dati a Europol.

L'Ufficio della protezione dei dati (DPO) è parte integrante di Europol e il punto iniziale di contatto per questioni relative alla protezione di tutti i dati. Il gruppo è presieduto dal responsabile della protezione dei dati, che è nominato dal consiglio di amministrazione di Europol, su proposta del direttore. Il compito principale del responsabile della protezione dei dati è quello di garantire la legalità e il rispetto dell'ECD per quanto riguarda la protezione dei dati in questione (Art. 28 ECD). La parte centrale di questo ruolo è di fornire orientamenti e consulenza indipendente, in particolare al Dipartimento delle Operazioni. L'applicazione del quadro a volte può essere un compito complesso e giuridicamente difficile, ad esempio per determinare se i dati possono essere inviati a terzi, o al momento di negoziare accordi di cooperazione operativa. Inoltre, il DPO è il punto di contatto principale per i suoi supervisor esterni di protezione dei dati. La sua unicità all'interno dell'architettura di Europol consente al DPO di essere coinvolto in processi di pianificazione fin dall'inizio: in questo modo, il DPO non solo fornisce il monitoraggio *ex post*, ma partecipa allo sviluppo di sistemi, all'esecuzione delle operazioni in corso e alla formazione del personale. Allo stesso tempo, il DPO è anche una parte funzionalmente indipendente dell'organizzazione. Opera come consulente informato ma indipendente. In caso d'inosservanza, il DPO può innalzare di livello la questione in una procedura predefinita, affrontando prima il direttore, il consiglio di amministrazione e, successivamente, l'autorità di vigilanza esterna, se necessario (Art. 28 comma 4 ECD). Ciò che sembra essere una contraddizione a prima vista è in realtà un concetto molto efficace: il DPO come parte dell'organizzazione lavora per l'autorizzazione degli affari operativi conformemente con l'applicabilità del quadro legale di

protezione dei dati. In questa impostazione, il DPO offre servizi professionali, consulenza ritenuta affidabile e orientata alle soluzioni a tutte le unità.

Viene reputato d'interesse per l'organizzazione avere un membro interno – ancorché indipendente – in grado di tracciare una linea tra le necessità operative e il limite dei diritti costituzionali di protezione dei dati personali. Europol, con riferimento a se stessa, dichiara di non potere e di non dover avere un interesse a fornire prestazioni eccedenti l'applicabilità del quadro legale di riferimento.

Per garantire la legittimità e il rispetto dell'ECD, il DPO può impiegare diversi metodi e strumenti. Ad esempio, un elemento centrale del lavoro relativo alla protezione dei dati è quello di condurre verifiche periodiche sulle banche dati di Europol. A tal fine, il DPO ha accesso a tutti i dati trattati da Europol e a tutti i locali di Europol. Dati errati, informazioni non aggiornate o voci non necessarie vengono registrate in modo che possano essere successivamente rettificare con il proprietario dei dati. Sono perciò ancora le tecnologie di elevato *standard* che giocano un ruolo importante in quest'aspetto del lavoro di Europol. Lo stato dell'arte dei *software* di analisi viene utilizzato per condurre i controlli; vengono inoltre generate automaticamente registrazioni di accessi o altre azioni compiute con i *file* di Europol. Per mezzo di questi *log*, ogni recupero o modifica dei dati personali, si può far risalire al suo autore, e ciò consente al DPO di verificare la necessità e la legittimità del processo (Art. 18 ECD). Ancora, gli specialisti del DPO, esaminano regolarmente l'entità della sicurezza delle informazioni per i progetti pianificati o esistenti. Dovunque dati personali vengano trattati, una valutazione del rischio è ritenuta essenziale e deve essere creato un adeguato livello di salvaguardia dei dati. Ciò comporta che per ogni nuova infrastruttura tecnica che la progettazione sia adeguata al già richiamato concetto di "*privacy by design*". L'attuazione delle misure di sicurezza deve essere verificata e mantenuta attraverso tutto il ciclo di vita dei *database*.

Dal momento che questi progetti coinvolgono spesso complessi processi tecnologici, personale del DPO ha anche competenze informatiche. Inoltre, il DPO è coinvolto in qualità di consulente nei negoziati con Stati terzi e, in particolare, per verificare se il futuro *partner* sia in grado di garantire un adeguato livello di protezione dei dati. Ad esempio, i funzionari del DPO non solo esaminano le relazioni obbligatorie sulle disposizioni nazionali per la protezione dei dati, ma compiono anche visite di studio per valutarne la loro attuazione *in loco*. Il DPO documenta anche tutte le operazioni di trattamento dei dati personali, compresi i dati del personale. Tutte le unità sono tenute a notificare al DPO ogni singola operazione. Questa notifica consente al DPO di essere a conoscenza di tutti i processi in corso e programmati per garantire che le opportune garanzie di protezione dei dati siano in atto. In particolare, nel delicato settore delle indagini in materia di criminalità grave e organizzata o terrorismo, la protezione dei dati personale è vitale. Le regole di protezione dei dati assicurano allo *staff* che informazioni che riguardano loro e le loro famiglie non siano accedibili liberamente nell'ambito dell'organizzazione o divulgate a persone esterne non autorizzate. Ritiene Europol che, in particolar modo il personale delle forze di polizia, debba poter fare affidamento sul fatto che le informazioni che li riguardano rimangano private.

Il DPO aumenta di conseguenza la consapevolezza sui rischi connessi alla manipolazione incurante dei dati personali. Un altro compito affidato al DPO è quello di garantire che gli interessati siano informati dei loro diritti. Un individuo può chiedere di conoscere se i dati personali che lo riguardano siano trattati nei sistemi di Europol e di avere tali dati comunicati a lui o lei, o controllati secondo le condizioni previste nell'ECD (Art. 30 ECD). A tal fine, l'interessato può presentare una domanda a Europol tramite l'autorità competente di uno Stato membro.

I controlli dei sistemi di Europol sono eseguiti dal DPO. Le decisioni di accesso sono condizionate alla stretta consultazione tra Europol e le competenti autorità degli Stati membri.

L'ECD permette esenzioni sulla risposta alle procedure di accesso se il rigetto è necessario per:

- permettere a Europol l'assolvimento dei suoi compiti;
- tutelare la sicurezza e l'ordine pubblico negli Stati membri o prevenire la criminalità;
- garantire che nessuna indagine nazionale sia compromessa;
- proteggere i diritti e le libertà di terzi (Art. 30 comma 5 ECD).

In tal caso l'Agenzia comunicherà al richiedente che ha effettuato i controlli, ma non rivelerà il risultato. Se la persona che effettua la richiesta non è soddisfatta della risposta di Europol, potrà ricorrere all'autorità di controllo comune (Art. 32 ECD). Se i dati errati o trattati in violazione dell'ECD sono stati trasmessi a Europol direttamente dagli Stati membri, gli Stati membri interessati devono rettificare o cancellare tali dati in collaborazione con Europol.

Europol inoltre ha un obbligo d'immediata notifica agli Stati membri o altre fonti dei dati in questione, così come ad ogni altro destinatario (art. 31 ECD).

L'interessato ha anche il diritto di ottenere il risarcimento dei danni subiti in conseguenza di dati illeciti o non corretto uso dei dati a Europol (Art. 52 ECD).

Tale regola è un'altra forma di salvaguardia per assicurare che Europol e gli Stati membri si attengano al regime di protezione dei dati. Un'efficace protezione dei dati viene interpretata da Europol anche come uno strumento concreto per proteggere l'organizzazione e gli Stati membri da tali richieste.

Nei suoi primi anni, Europol ha ricevuto un numero relativamente basso di richieste, con una media di circa 15 casi all'anno. Nel 2007, tuttavia, c'è stato un notevole aumento del numero di richieste, con più di 120: questa tendenza è continuata, con un picco di 560 nel 2012. I cittadini europei sono diventati chiaramente più consapevoli dei loro diritti: ad esempio, i siti *web* delle autorità di protezione dei dati degli Stati membri contengono informazioni su come esercitare tale diritto; campagne gestite da gruppi o individui forniscono consigli su come affrontare le organizzazioni a tale riguardo, il sito *web* dell'autorità di controllo comune mette in evidenza i diritti della persona sotto l'ECD. Il DPO funge anche da collegamento con il controllo comune. In questa funzione, il DPO informa gli organi delle autorità competenti sulle attività di Europol in materia di misure di protezione dei dati e favorisce un proficuo scambio di opinioni su questi temi.

**11. L'Autorità di Controllo Comune – ACC/JSB**

Mentre il DPO, sebbene indipendente nell'esecuzione dei suoi compiti, sia una parte integrante dell'organizzazione, il JSB provvede al controllo esterno (art. 34 ECD).

L'Autorità di controllo comune è composta da una rappresentativa delle autorità nazionali di protezione dei dati dei 27 Paesi. Si tratta di esperti con ampia competenza nel particolare campo della protezione dei dati negli ambiti delle forze di polizia. Il loro compito è di controllare le attività di Europol da una prospettiva di protezione dei dati. A tal fine, il JSB ha il potere di ispezionare tutti i file di Europol riferiti ad ogni epoca. Esso ha il diritto, almeno una volta all'anno, di ispezionare tutti i locali di Europol in stretta cooperazione con il DPO. Tale ispezione copre tutti le operazioni trattate da Europol e si conclude con la consegna di un dettagliato rapporto comprensivo di conclusioni e raccomandazioni. Se ritenuto necessario vengono eseguite anche ispezioni *ad hoc*.

Finora, queste visite ispettive sono state considerate un utile strumento per l'ulteriore sviluppo della cornice di protezione dei dati di Europol, dimostrando la validità e la produttività di una cooperazione tra le due istituzioni. In accordo con il JSB, Europol ha riconosciuto l'importanza della protezione dei dati non solo come elemento necessario di incontro tra obblighi connessi ai diritti umani ma anche come un mezzo per fornire rassicurazione agli Stati membri contribuenti (art. 33 ECD).

**12. Gli organismi nazionali di vigilanza**

In aggiunta al controllo interno garantito dal DPO e al controllo esterno eseguito dal JSB, ogni Stato membro ha le sue proprie autorità di controllo. Queste autorità nazionali controllano indipendentemente, nel rispetto delle normative nazionali, le comunicazioni di dati personali a e da Europol (art. 33 ECD). Anche i membri di queste autorità di controllo hanno accesso ai documenti e ai locali degli Ufficiali di collegamento ad Europol (oltre che dell'UNE). Oltre ai dritti dei soggetti delle informazioni prima citati, ogni persona può richiedere alle autorità nazionali di accertare che le immissioni o le comunicazioni dei loro dati da parte degli Stati membri siano conformi alle normative nazionali e dell'UE.

L'UNE, ai sensi della legge 23 marzo 1998, n. 93, di "Ratifica ed esecuzione della Convenzione basata sull'articolo K3 del Trattato sull'Unione europea che istituisce un Ufficio europeo di Polizia EUROPOL" si deve muovere nella cornice delle previsioni delle leggi 31 dicembre 1996 n. 675 e n. 676 (abrogate a decorrere dal 1° gennaio 2004 dall'art. 183, D. Lgs. 30 giugno 2003, n. 196 e sostituite da quest'ultimo provvedimento di legge, c.d. Codice in materia di protezione dei dati personali) mentre l'autorità di controllo nazionale ai sensi dell'art. 23 della Convenzione Europol (sostituito dall'art. 33 dell'ECD) s'identifica nel Garante per la protezione dei dati personali.

### 13. L'Unità Nazionale Europol –UNE/ENU



#### **Concetto.**

L'unità nazionale è l'unico organo di collegamento tra Europol e le autorità competenti degli Stati membri. Gli Stati membri possono tuttavia consentire contatti diretti tra le autorità competenti designate e Europol, purché siano rispettate le condizioni stabilite dallo Stato membro in questione, in particolare il previo coinvolgimento dell'unità nazionale. L'unità nazionale riceve al tempo stesso da Europol tutte le informazioni scambiate nei contatti diretti tra Europol e le autorità competenti designate. Le relazioni tra l'unità nazionale e le autorità competenti sono disciplinate dalla legislazione nazionale, in particolare dalle pertinenti norme costituzionali nazionali.

#### **Quadro legislativo e regolamentare di riferimento.**

##### La legislazione dell'UNE

- Atto CE del 26 luglio 1995 (Convenzione Europol)
- DM (Interno) n. 214 del 21.02.1996
- Legge 23 marzo 1998 n. 93
- Decisione del Consiglio 6 aprile 2009, n. 2009/371/GAI

Istituita in forza di un dettato normativo che trae origine dall'Atto CE del 26 luglio 1995 (Convenzione Europol), sostituita dalla Decisione del Consiglio 6 aprile 2009, n. 2009/371/GAI che "istituisce l'Ufficio europeo di polizia (Europol)" (attuale quadro normativo di riferimento di

Europol) l'UNE trova il suo fondamento normativo, rispettivamente, nei commi 1 e 2 dell'art. 8 (Unità nazionale) dell'ECD che:

- (comma 1), fa obbligo a ciascuno Stato membro di “istituire o designare un'unità nazionale affinché svolga i compiti individuati nel medesimo articolo della decisione” e dispone, inoltre, la designazione di “un agente a capo dell'unità nazionale”;
- (comma 2), statuisce che “l'unità nazionale è l'unico organo di collegamento tra Europol e le autorità competenti degli Stati membri” affermando il carattere di esclusività dell'UNE per quanto riguarda la comunicazione con le menzionate “autorità competenti” ovvero “tutti gli organi pubblici degli Stati membri preposti alla prevenzione e alla lotta contro la criminalità in forza della legislazione nazionale” (art. 3, comma 2, ECD).

Il DM (Interno) n. 214 del 21.02.1996, collocando ordinativamente l'UNE presso l'Ufficio del Vice Direttore Generale della Pubblica Sicurezza - Direttore centrale della Polizia Criminale, recepisce integralmente l'esclusiva titolarità dell'Unità Nazionale Europol per i rapporti con le Autorità nazionali competenti stabilendo, all'articolo 2, che “l'Unità nazionale è l'unico organo di collegamento tra Europol e le competenti strutture italiane di polizia, per la gestione dei reciproci flussi informativi secondo la legislazione nazionale”.

Il Dipartimento della Pubblica Sicurezza, con circolare in data 30 dicembre 1996 a firma del Capo della Polizia, richiamando espressamente il dettato del DM del Ministro dell'Interno citato:

- ribadisce il ruolo dell'UNE quale unico organo di collegamento tra Europol (all'epoca UDE - Europol) e le competenti strutture nazionali di polizia attribuendo all'Unità nazionale lo “svolgimento esclusivo delle funzioni di collegamento, quale unico interlocutore, tra l'UDE-Europol ed i Referenti Nazionali per lo scambio d'informazioni relative alle aree di cooperazione individuate dall'Azione Comune del 10 marzo 1995”;
- individua, inoltre, gli organismi centrali delle strutture preposte alla prevenzione e alla lotta contro la criminalità, indicati quali Referenti unici dell'UNE (DIA, DCSA, SCO e i II Reparti dei Comandi Generali dell'Arma e della Guardia di Finanza).

La legge 23 marzo 1998 n. 93 (Ratifica ed esecuzione della Convenzione basata sull'articolo K3 del Trattato dell'Unione europea che istituisce un ufficio europeo di polizia Europol) statuisce (art. 3) che l'Unità nazionale svolge le funzioni elencate nell'art. 4 della Convenzione Europol (attualmente sostituito dall'art. 8 della decisione del Consiglio 2009/371/GAI) e tanto nell'attuale formulazione quanto in quella della Convenzione Europol, l'Unità nazionale viene individuata quale “unico organo di collegamento tra Europol e le autorità competenti degli Stati membri”.

#### **Ordinamento e organico.**

Il decreto del Ministro dell'Interno del 25 ottobre 2000 di riassetto, tra l'altro, della Direzione Centrale della Polizia Criminale e istitutivo del Servizio per la Cooperazione Internazionale di Polizia, operativo dal 20 settembre 2001, ha determinato invece una nuova posizione ordinativa dell'UNE che si trova attualmente collocata nel Servizio innanzi citato, articolato su cinque Divisioni (1^ Affari Generali, 2^ e 3^ Interpol, 4^ UNE e 5^ S.I.Re.N.E.). L'art. 3 del decreto attribuisce, infatti, alla “Divisione 4^” del Servizio “Unità Nazionale Europol” esclusivamente lo “svolgimento delle funzioni elencate nell'art. 4 della Convenzione Europol basata sull'art. K3 del

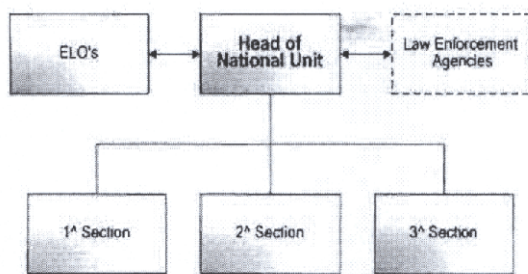
Trattato sull'Unione Europea ed adottata con atto del Consiglio del 26 luglio 1995", innanzi richiamate.

Da un punto di vista organico, l'UNE, di livello divisionale, retta con alternanza d'incarico da un Primo Dirigente della P di S o da un Ufficiale di grado equivalente (Colonnello) dell'Arma dei Carabinieri o del Corpo della G di F, è articolata in Sezioni (art. 4 DM n. 214/1996).

L'ultima previsione organica cartolarmente individuata è quella annessa al richiamato DM Interno che prevedeva:

- 1 Funzionario del Ruolo dei Commissari e 1 Ispettore della P di S;
- 1 Ufficiale e 1 Sottufficiale dell'Arma dei Carabinieri;
- 1 Ufficiale e 1 Sottufficiale del Corpo della Guardia di Finanza.

La struttura dell'UNE è visualizzabile nel sottostante organigramma che raffigura anche la posizione degli Ufficiali di collegamento distaccati ad Europol.



ELOs: *Europol liaison officers*, Ufficio nazionale di collegamento, composto dagli Ufficiali di collegamento dell'UNE distaccati all'Aia, presso il QG di Europol.  
Law Enforcement Agencies – LEAs, Referenti nazionali con i quali dialoga l'UNE.

Attualmente è retta da un Colonnello dei CC, Direttore della 4<sup>a</sup> Divisione del Servizio per la Cooperazione Internazionale di Polizia, nonché della stessa UNE.

Le Sezioni, rette da funzionari equamente ripartite tra le principali Forze di Polizia (P di S, CC, e G di F), hanno una competenza per materia che rispecchia ovviamente i reati ricadenti nel mandato di Europol e con una ripartizione interna che tiene conto dei carichi di lavoro dell'UNE nel suo complesso.

Attualmente l'organico è il seguente:

- **1<sup>a</sup> Sezione**, (retta da funzionario della P. di S.), con 5 unità tra Ispettori/Marescialli, competente per lo scambio informativo sui seguenti reati di cui all'allegato all'art. 4 della ECD: terrorismo, furti e rapine, omicidio, traffico di esplosivi e armi, traffico di sostanze radioattive, reati contro la persona, reati ambientali, rapimento, estorsione, contraffazione monetaria, traffico di opere d'arte, reati informatici, razzismo e xenofobia;
- **2<sup>a</sup> Sezione**, (retta da Ufficiale dell'Arma dei CC) e 5 unità tra Ispettori/Marescialli, competente per lo scambio informativo sui seguenti reati di cui all'allegato all'art. 4 dell'ECD: immigrazione