Parere del Comitato economico e sociale europeo sulla: «Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE (frontiere e visti) e che modifica la decisione 2004/512/CE del Consiglio, il regolamento (CE) n. 767/2008, la decisione 2008/633/GAI del Consiglio, il regolamento (UE) 2016/399 e il regolamento (UE) 2017/2226»

[COM(2017) 793 final — 2017/0351 (COD)]

e sulla

«Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro per l'interoperabilità tra i sistemi d'informazione dell'UE (cooperazione giudiziaria e di polizia, asilo e migrazione)»

[COM(2017) 794 final — 2017/0352 (COD)]

(2018/C 283/07)

Relatrice: **Laure BATUT**

Consultazione	Commissione europea, 18.1.2018
	Parlamento europeo, 28.2.2018
Base giuridica	Articolo 304 del Trattato sul funzionamento dell'Unione europea
Sezione competente	Occupazione, affari sociali, cittadinanza
Adozione in sezione	25.4.2018
Adozione in sessione plenaria	23.5.2018
Sessione plenaria n.	535
Esito della votazione (favorevoli/contrari/astenuti)	160/3/2

1. **Conclusioni e raccomandazioni**

1.1. Il CESE considera utile e positiva la proposta della Commissione europea tesa a migliorare l'interoperabilità dei sistemi d'informazione dell'UE in materia di frontiere e visti, di cooperazione giudiziaria e di polizia nonché di asilo e di migrazione.

1.2. A giudizio del CESE, tale interoperabilità deve costituire un obiettivo strategico dell'UE affinché essa rimanga uno spazio aperto, che garantisce i diritti fondamentali e la mobilità. L'UE e gli Stati membri hanno l'obbligo di proteggere la vita e la sicurezza di tutti gli esseri umani. Occorre rispettare pienamente il principio del non respingimento.

1.3. Tanto maggiore sarà la comprensione delle misure in materia di interoperabilità quanto più esse:

— garantiranno, nell'ambito della strategia dell'UE in materia di migrazione, condizioni di equilibrio tra libertà e sicurezza, nel rispetto della separazione dei poteri,

— assicureranno alle persone interessate il rispetto dei loro diritti fondamentali, in particolare la protezione dei loro dati personali e della loro privacy, il diritto di accedere ai propri dati, di rettificarli o di cancellarli entro un termine ragionevole e attraverso procedure accessibili,

— riaffermeranno, anche in tutti i testi d'esecuzione, l'esigenza di integrare i principi di protezione dei dati fin dalla fase di progettazione («privacy by design»),

— non creeranno nuovi ostacoli al traffico normale di passeggeri e merci.

1.4. Per quanto riguarda l'uso dei dati a fini di contrasto, il CESE chiede procedure e garanzie che:

— prevedano di applicare in questo ambito la legge europea più protettiva (regolamento generale sulla protezione dei dati),

— permettano di determinare più rapidamente lo Stato membro autorizzato ad esaminare le domande di protezione internazionale,

— garantiscano alle persone interessate il diritto a due gradi di giudizio,

— garantiscano ai minori, in particolare quelli non accompagnati, siano essi in situazione irregolare, perseguitati o abbiano commesso delle illegalità, il diritto di ottenere un visto, di essere protetti e integrati e di beneficiare del diritto all'oblio entro un lasso di tempo più breve rispetto ai maggiorenni.

1.5. Il CESE ritiene che l'attuale base giuridica dei sistemi di informazione dovrebbe essere rafforzata e tenere conto dell'evoluzione dei sistemi di raccolta dei dati. Raccomanda pertanto di:

— rafforzare la sicurezza delle banche dati esistenti e quella dei loro canali di comunicazione,

— valutare l'impatto del rafforzamento del controllo ex ante sulla gestione dei rischi,

— assicurare un controllo e una valutazione permanente del sistema da parte delle autorità competenti in materia di protezione dei dati (GEPD); chiede ai responsabili di riferire ogni anno alle autorità decisionali e alla Commissione in merito alla sicurezza degli elementi di interoperabilità e ogni due anni in merito all'impatto delle misure sui diritti fondamentali.

1.6. Il CESE ritiene che il progetto debba contare su un personale competente e raccomanda:

— programmi concreti di formazione per le autorità competenti e gli agenti di eu-LISA,

— un controllo scrupoloso delle competenze di detti agenti e dei candidati ai posti dell'agenzia.

1.7. Il CESE esprime la sua preoccupazione per il finanziamento del nuovo sistema. Il monitoraggio della programmazione sarà fondamentale per evitare lo slittamento dei bilanci e garantire il completamento del progetto fino al 2029;

1.8. Il CESE raccomanda che i cittadini siano informati dei progressi compiuti in tale ambito fino al completamento del progetto, e che le persone ricevano un'informazione di tipo pedagogico sui controlli cui sono soggette. Ritiene che debba essere prevista la possibilità di mettere fine all'iniziativa qualora la libertà e i diritti fondamentali vengano messi in pericolo da un uso distorto del sistema.

2. **Introduzione**

2.1. Nel contesto internazionale del 2017, considerato come instabile tanto sul piano geopolitico quanto su quello della sicurezza interna degli Stati membri, il Consiglio ha chiesto ripetutamente alla Commissione di mettere in atto i mezzi per rintracciare le persone giudicate «a rischio» e già oggetto di schedatura in uno degli Stati membri. Individuarne i passaggi alle frontiere, i viaggi e gli spostamenti in Europa potrebbe rivelarsi cruciale per la sicurezza all'interno dell'UE.

2.2. Nella risoluzione del 6 luglio 2016 il Parlamento ha invitato la Commissione europea ad assicurare le necessarie garanzie in materia di protezione dei dati.

2.3. I testi all'esame rientrano nell'obiettivo «Preservare e rafforzare Schengen» ([1]). L'Unione si è già dotata di diverse normative e servizi digitalizzati di informazione nei settori legati al controllo dell'attraversamento delle frontiere di persone e merci.

2.4. Promemoria:

— **SIS: Sistema d'informazione Schengen**, uno dei meccanismi più vecchi, riveduto, che gestisce un ampio spettro di segnalazioni riguardanti le persone e le merci,

([1]) COM(2017) 570 final.

— **Eurodac: Sistema europeo per il confronto delle impronte digitali** dei richiedenti asilo e dei cittadini dei paesi terzi in situazione irregolare alle frontiere e negli Stati membri, e per la determinazione dello Stato membro responsabile delle domande (CESE 2016-02981, relatore: Moreno Díaz ([2])),

— **VIS: Sistema di informazione visti** (codice dei visti), che gestisce i visti per i soggiorni di breve durata (CESE 2014-02932, relatori: Pezzini e Pariza Castaños ([3])),

— **EES: Sistema di ingressi/uscite**, attualmente in attesa di decisione, che dovrebbe gestire elettronicamente i dati dei passaporti e le date di ingresso/uscita dei cittadini di paesi terzi che si recano nello spazio Schengen (CESE 2016-03098, SOC/544, relatore: Pîrvulescu ([4])),

— **ETIAS: Sistema europeo di informazione e autorizzazione ai viaggi**, attualmente in attesa di decisione, che dovrebbe costituire un ampio sistema automatizzato di stoccaggio e verifica ex ante dei dati dei cittadini di paesi terzi esentati dal visto per circolare nella zona Schengen (CESE 2016-06889, SOC/556, relatore: Simons ([5])),

— **ECRIS-TCN: Sistema europeo di scambio di informazioni sui casellari giudiziali dei cittadini di paesi terzi**, attualmente proposto dalla Commissione, un sistema digitale di scambio di informazioni sulle sentenze già pronunciate dai giudici nazionali.

2.5. Si può fare un'analogia tra i mezzi attuali di un'autorità abilitata e uno smartphone con diverse applicazioni, tutte separate tra loro e ciascuna che fornisce le «proprie» informazioni.

2.6. Ad eccezione del SIS, tali sistemi sono incentrati sulla **gestione dei cittadini di paesi terzi**. Esistono sei sistemi, complementari e decentrati. La somma delle informazioni richieste è quella delle diverse risposte ottenute nelle diverse banche dati dai servizi di investigazione, in funzione delle loro autorizzazioni di accesso.

2.7. La Commissione si propone di rispondere alla seguente domanda:

— in che modo, senza cambiare le strutture già acquisite e mantenendone la complementarietà, collegare tra loro tutte le banche dati allo stesso tempo affinché, in uno specifico punto di entrata sul territorio europeo e tramite una sola interrogazione del sistema, tutte le informazioni già raccolte nelle basi esistenti convergano verso l'autorità di controllo autorizzata a richiederle, rispettando nel contempo le disposizioni in materia di protezione dei dati e i diritti fondamentali.

2.8. La Commissione europea, nelle proposte in esame:

2.8.1. desidera aggiungere le ulteriori possibilità offerte da un accesso alle banche dati di Europol e di Interpol, che già cooperano con le autorità di controllo europee;

2.8.2. vorrebbe «sincronizzare» le ricerche di informazioni per ridurre i tempi di risposta per quanto concerne il dossier dei migranti, e accelerare la risposta di sicurezza in caso di necessità. A tal fine, propone di creare nuove entità, il che consentirebbe di fare funzionare in simbiosi le banche dati esistenti.

2.9. **I suoi obiettivi sono i seguenti:** rimediare il più possibile alle carenze dei diversi sistemi; migliorare la gestione delle frontiere esterne dello spazio Schengen; contribuire alla sicurezza interna dell'Unione; gestire le frodi d'identità; risolvere i casi di identità multiple; ritrovare le persone sospettate o già condannate e verificarne l'identità nello spazio Schengen.

2.10. Per riprendere l'immagine dello smartphone, non solo l'autorità abilitata avrebbe a sua disposizione numerose applicazioni, ma potrebbe anche raccogliere simultaneamente e nel quadro della stessa ricerca (attraverso i propri codici di accesso) i dati memorizzati in tutti i suoi supporti: computer, laptop, telefono, tablet, notebook ecc.

([2]) GU C 34 del 2.2.2017, pag. 144.
([3]) GU C 458 del 19.12.2014, pag. 36.
([4]) GU C 487 del 28.12.2016, pag. 66.
([5]) GU C 246 del 28.7.2017, pag. 28.

3. **Funzionamento del sistema**

3.1. La Commissione ha proceduto ad una serie di consultazioni e ha riunito un gruppo di esperti ad alto livello sui sistemi di informazione e l'interoperabilità ([6]), nominati dagli Stati membri, dai paesi del gruppo Schengen e da agenzie europee come eu-LISA ([7]) e FRA ([8]), con il coordinamento della DG HOME.

Il metodo: interconnettività o interoperabilità?

3.1.1. L'**interconnettività** dei sistemi di informazione è la possibilità di collegarli tra loro in modo che i dati di uno possano essere consultati automaticamente da un altro.

3.1.2. L'**interoperabilità** ([9]) è la capacità di diversi sistemi di comunicare, scambiare dati e utilizzare le informazioni scambiate, rispettando le autorizzazioni di accesso ai sistemi.

3.2. *La scelta dell'interoperabilità*

3.2.1. Per la Commissione, questa opzione non stravolge quanto già creato tramite le strutture e le competenze attuali, e i dati resteranno in compartimenti stagni. Nonostante la maggiore divulgabilità, tale opzione comporterebbe un vantaggio in materia di sicurezza per i sistemi e i dati, nessuno dei quali, evidentemente, sarà accessibile via Internet. I testi sottoposti a parere presentano forti analogie e riguardano:

— uno, COM(2017) 793, l'interoperabilità dei sistemi di informazione relativi alle frontiere e ai visti,

— l'altro, COM(2017) 794, la cooperazione giudiziaria e di polizia, l'asilo e la migrazione.

3.3. *I nuovi strumenti*

3.3.1. Per funzionare in interoperabilità, una nuova architettura composta da quattro nuovi strumenti dovrà completare le sei banche dati per lavorare rapidamente interrogando il sistema solo una volta, mantenendo delle persone abilitate all'origine delle richieste.

3.4. *Il PER (EPS), Portale europeo della ricerca*

3.4.1. L'autorità di controllo autorizzata (utente finale) dovrebbe disporre di un accesso unico all'intero sistema. Invece di sei ricerche, essa ne lancerebbe solo una (polizia, dogane ecc.), per interrogare contemporaneamente diverse banche dati sui dati ricercati, senza però conservarne alcuno. Se i dati esistono, il sistema li troverà. In caso di sospetto di reato o di attività terroristiche, il primo tentativo potrà avere esito neutro per la persona controllata («no-hit»), ma se il dato concorda con una seconda informazione («hit») presente nelle banche dati quali SIS, EES, ETIAS, ciò potrà indurre ad effettuare ricerche approfondite e a lanciare un'indagine.

3.5. *Il BMS comune (servizio comune di corrispondenza biometrica)*

3.5.1. Tale piattaforma condivisa di confronto consentirà la ricerca e la comparazione simultanee di dati matematizzati, biometrici, impronte digitali e fotografie di identità, a partire dalle diverse banche dati, come SIS, Eurodac, VIS, *EES* ([10]), *ECRIS*, ma non *ETIAS*; i loro dati dovranno essere compatibili.

3.5.2. I dati matematizzati non verranno conservati nella loro forma originale.

3.6. *Il CIR (registro comune di identità)*

3.6.1. Un «registro comune di identità» riunirà i dati relativi all'identità biografica e biometrica delle persone controllate di paesi terzi, che si trovino alla frontiera o negli Stati membri (di Schengen). Un indicatore di concordanza delle informazioni nelle diverse banche dati accelererà le ricerche. Sotto la responsabilità e con i mezzi di sicurezza dell'agenzia eu-LISA, tali dati saranno conservati in modo che nessuno possa accedere a più di una linea alfanumerica alla volta. Sviluppato a partire dall'EES e dall'ETIAS, il CIR non dovrebbe determinare una duplicazione dei dati. Il registro potrà essere utilizzato anche per ricerche civili.

([6]) DG HOME, unità B/3; decisione C/2016/3780 della Commissione del 17 giugno 2016; http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=IT.

([7]) Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia.

([8]) FRA: Agenzia dell'UE per i diritti fondamentali.

([9]) Comunicazione della Commissione europea *Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza* (COM(2016) 205 final).

([10]) Il corsivo indica che i testi riguardanti tali organi non sono ancora stati adottati.

3.7. *Il MID (rivelatore di identità multiple)*

3.7.1. Esso avrà il compito di verificare la vera identità delle persone in buona fede e di combattere le frodi di identità, attuando una ricerca in tutte le banche contemporaneamente. Nessuna amministrazione ha ancora utilizzato uno strumento di questo tipo, che dovrebbe consentire di evitare le usurpazioni di identità.

3.8. *Il ruolo dell'agenzia eu-LISA* ([11])

3.8.1. L'agenzia, istituita nel 2011, ha il compito di facilitare le politiche dell'UE nei settori della giustizia, della sicurezza e della libertà. Essa ha sede a Tallinn (Estonia) e garantisce già lo scambio di informazioni tra le diverse autorità di contrasto degli Stati membri e il funzionamento senza interruzioni dei sistemi informatici su vasta scala, nonché la libera circolazione delle persone nello spazio Schengen.

3.8.2. L'agenzia sta lavorando al progetto «Frontiere intelligenti» e, nella nuova architettura di scambio di dati, svolgerà un ruolo di conservazione degli elementi connessi alle persone come di quelli relativi alle autorità, alle indagini e agli investigatori. Essa verificherà le autorizzazioni dei richiedenti e garantirà la sicurezza dei dati, anche in caso di «incidente» (articolo 44 delle proposte (2017) 793 e 794).

3.8.3. **L'uso dell'UMF (formato universale dei messaggi)**, non ancora creato, dovrebbe rendere più facile lavorare con i nuovi sistemi, che saranno obbligatori, imponendo la creazione di interfacce negli Stati membri che non ne sono ancora dotati e un sistema di traduzione temporanea da un linguaggio all'altro.

3.9. *La protezione dei dati personali (artt. 7 e 8 della Carta):*

3.9.1. La proposta di regolamento riconosce la possibilità di incidenti in materia di sicurezza. Gli Stati membri e i loro sistemi di dati devono rispettare per primi i principi di protezione dei dati previsti dai testi, dal trattato, dalla Carta dei diritti fondamentali e dal regolamento generale sulla protezione dei dati RGPD ([12]), che entrerà in vigore il 25 maggio 2018.

4. **Dibattito**

4.1. *Valore aggiunto dell'interoperabilità in democrazia*

4.1.1. L'Unione ha bisogno di una legislazione e di mezzi di indagine che la proteggano dalla criminalità. L'interoperabilità dei sistemi di informazione è un'opportunità di far valere la preminenza del diritto e la difesa dei diritti umani.

4.1.2. L'*EES* e l'*ETIAS*, combinati con il BMS e il CIR, permetteranno di controllare il passaggio alle frontiere delle persone sospette, conservando i loro dati. Tuttavia, la possibilità di agevolare e semplificare «alle autorità di contrasto l'accesso ai sistemi di informazione estranei al settore del contrasto a livello dell'UE» (articolo 17, CIR, proposte (2017) 793 e 794) non può essere compatibile con gli obiettivi indicati come base delle proposte all'esame. In tale contesto, il Comitato (articolo 300, paragrafo 4, del TFUE) è tenuto ad invocare il principio di proporzionalità e chiede alla Commissione di scongiurare qualsiasi schema tipo «Grande Fratello» ([13]) e la creazione di ostacoli alla libertà di circolazione dei cittadini europei (articolo 3 del TUE).

4.1.3. Il modello proposto per la raccolta e l'utilizzo dei dati personali ottenuti alla frontiera e nel territorio dell'Unione durante i controlli dei movimenti e dei documenti viene presentato come un modello «a tenuta stagna», accessibile solo alle persone autorizzate e per scopi di sicurezza e di gestione, e consentirà una maggiore fluidità delle procedure.

4.1.4. Il Comitato nutre una serie di dubbi sull'impermeabilità: sussisteranno delle lacune, la costruzione che si estende su un arco di nove anni si basa su «fondamenta» ancora inesistenti, come le banche dati EES ed ETIAS o le interfacce nazionali. Essendo il contesto tecnologico in costante evoluzione, il progetto si basa necessariamente sullo stato della tecnica e non prevede, finanziariamente parlando, la gestione dell'obsolescenza che potrebbe manifestarsi in alcuni settori digitali.

([11]) Regolamento (UE) n. 1077/2011 del Parlamento europeo e del Consiglio, del 25 ottobre 2011, che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia.

([12]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Pareri del CESE: GU C 229 del 31.7.2012, pag. 90, e GU C 345 del 13.10.2017, pag. 138.

([13]) Da *1984*, di George Orwell.

4.1.5. Inoltre, la proposta avrebbe potuto tener conto della rapida evoluzione nell'utilizzo dei cosiddetti algoritmi dell'intelligenza artificiale (IA) sia come strumento di controllo dei sistemi sia come chiave di sicurezza da affidare alle autorità decisionali per garantire un uso democratico del sistema.

4.1.6. Il sistema elaborato nella proposta è stato pensato per soggetti in buona fede, rispettosi della legge. Il fatto che ai comandi vi siano esseri umani è rassicurante, ma il fattore umano può rivelarsi anche un anello debole. Il Comitato propone di aggiungere un articolo che preveda una serie di «disgiuntori differenziali», per i casi di crisi politica e/o di «gestione», poiché qualsiasi problema in una banca dati potrebbe rappresentare un rischio per l'intero sistema ([14]). L'applicazione generalizzata dell'UMF potrebbe condurre ad un uso internazionale, indubbiamente molto positivo ma molto rischioso per la protezione dei dati. Le autorità abilitate avranno una pesante responsabilità. Tali aspetti non sono trattati nei testi in esame.

4.2. *Tutela dei diritti fondamentali*

4.2.1. I diritti fondamentali sono assoluti: possono subire limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità d'interesse generale riconosciute dall'Unione, ma sempre nel rispetto del loro contenuto essenziale (artt. 8 e 52, paragrafo 1, della Carta). Il Comitato si chiede in che modo possa essere valutata la proporzionalità delle misure di controllo in caso di migranti in fuga dalle persecuzioni e in cerca di asilo sulle coste dell'Unione [COM (2017) 794 final, Relazione — Diritti fondamentali]. La ricerca di sospetti al fine di prevenire azioni criminali, in particolare attentati terroristici, **non deve spingere le nostre democrazie verso la presunzione di reato**: è essenziale che vi sia una differenza tra le «attività» tali da turbare l'ordine pubblico e le «opinioni».

4.2.2. Il rispetto per tutti dei diritti sanciti dalla Carta deve garantire un equilibrio tra sicurezza e libertà, pena la morte della democrazia. Il Comitato ritiene che questo equilibrio sia fondamentale e debba rappresentare un obiettivo costante per tutte le autorità, comprese quelle di controllo, a livello sia nazionale che europeo.

4.2.3. Il sistema conserverà traccia sia delle varie autorità associate a una ricerca sia dei metadati ad essa collegati. Alle stesse autorità competenti vanno garantiti i diritti fondamentali a proposito dei dati generati, in particolare per quanto concerne la loro sicurezza e la loro privacy, in caso di intrusione dolosa nella struttura e di uso improprio dei dati tra il momento in cui vengono inseriti e la loro cancellazione.

4.3. *Protezione dei dati*

4.3.1. Le proposte riconoscono il principio della protezione dei dati personali fin dalla fase di concezione e d'ufficio, benché nella relazione si sottolinei che, secondo la Corte di giustizia (CGUE), non si tratta di una prerogativa assoluta. Il Comitato riconosce i benefici di misure preventive a favore della sicurezza, della lotta contro la falsificazione di identità e della garanzia del diritto di asilo. Desidera tuttavia sottolineare i limiti della matematizzazione dei dati e del loro carattere anonimo: le persone interessate potrebbero aver ancora bisogno dei loro dati.

4.3.2. Sottolinea inoltre che il tipo di dati memorizzati, biometrici e biologici, è di particolare interesse per alcune imprese e per la criminalità. In questo contesto la sicurezza informatica ha la stessa importanza della sicurezza fisica, ed è menzionata troppo raramente nelle proposte. I dati memorizzati verranno immagazzinati in un unico luogo fisico; anche adottando misure estreme di tutela e di sicurezza, esso potrebbe risultare vulnerabile.

4.3.3. Il CESE ricorda che per quanto riguarda la protezione dei dati e il diritto alla cancellazione («diritto all'oblio»), le istituzioni e gli organi dell'Unione sono tenuti al rispetto del regolamento (CE) n. 45/2001, meno protettivo del regolamento generale sulla protezione dei dati del 2016 ([15]) (che entra in vigore nel maggio 2018) che deve essere rispettato dagli Stati membri. Il Comitato sottolinea quanto sia complicato attuare tale diritto e teme che i viaggiatori, i migranti e i richiedenti asilo non siano in grado di farlo rispettare:

1) la protezione dei dati personali deve valere per tutte le banche dati esistenti, nazionali e europee, affinché l'intero sistema risulti protetto;

2) la protezione è fondamentale affinché i cittadini accettino questa immensa rete di vigilanza che incombe su di loro.

4.3.4. Le proposte non indicano chiaramente la durata di conservazione dei dati raccolti dalle autorità abilitate. I testi menzionano la procedura relativa al diritto di rettifica e/o cancellazione che fa avanti e indietro tra lo Stato membro della richiesta e lo Stato membro competente, ma non viene fissato un termine per la conservazione dei dati (articolo 47 delle proposte). Il Comitato raccomanda che tale termine venga stabilito, e che sia più breve per i minori (Carta dei diritti fondamentali, articolo 24) — tranne in caso di terrorismo -, in modo che essi possano sfruttare le loro opportunità di integrazione.

([14]) GEPD, allegato, relazione finale del gruppo di esperti ad alto livello, maggio 2017.
([15]) Regolamento generale sulla protezione dei dati [regolamento (UE) 2016/679].

4.4. *Governance e rendicontabilità*

4.4.1. Le banche dati internazionali non sono soggette alle stesse regole vigenti per i sistemi informatizzati europei. La creazione di un formato universale di accesso, che potrebbe diventare internazionale, sarà solo una componente tecnica che non uniformerà le normative, anche se certamente Interpol è tenuta a rispettare l'articolo 17 del Patto delle Nazioni Unite ([16]). Le autorizzazioni continueranno inoltre ad essere prerogativa degli Stati membri. Il CESE ritiene che le proposte dovrebbero trattare la questione.

4.4.2. Sarà sufficiente presentare un'unica richiesta, e le banche dati europee in simbiosi fra di loro daranno il loro verdetto. Il CESE sottolinea che la burocrazia generata sarà più che proporzionale alla velocità raggiunta. La governance sarà assicurata dalla Commissione nel quadro di una procedura di controllo con gli Stati membri. Il perno del sistema sarà l'agenzia eu-LISA, incaricata in particolare di definire le procedure per la raccolta delle informazioni sul funzionamento dell'interoperabilità. L'agenzia riceverà le informazioni dagli Stati membri e da Europol e ogni quattro anni presenterà al Consiglio, al Parlamento europeo e alla Commissione una relazione di valutazione tecnica. Dal canto suo, la Commissione preparerà una relazione globale un anno dopo (articolo 68 delle proposte). Per il Comitato, queste fasi procedurali sono troppo lunghe. La valutazione della sicurezza delle componenti di interoperabilità (articolo 68, paragrafo 5, lettera d) dovrebbe aver luogo almeno una volta l'anno, e quella dell'incidenza sui diritti fondamentali almeno ogni due anni (stesso articolo, lettera b).

4.4.3. Il Comitato si rammarica che questioni importantissime quali quelle oggetto delle proposte all'esame siano gestite da agenzie europee, le cui procedure di assunzione e funzionamento restano oscure per molti cittadini. Reputa necessario comparare le buone pratiche e chiedere il parere di tutte le autorità indipendenti per il controllo dell'utilizzazione dei dati (GEPD), nonché di altre agenzie come la FRA e l'ENISA.

4.4.4. La creazione di tutte queste nuove strutture e procedure avverrà mediante atti delegati e atti di esecuzione della Commissione. Il Comitato auspica che l'obiettivo del rispetto dei diritti fondamentali e della protezione dei dati personali resti iscritto in tutti questi atti nel corso del tempo, in un approccio teso a migliorare l'accoglienza delle persone alle frontiere. Il CESE raccomanda che i cittadini europei siano informati delle diverse tappe fino al completamento del progetto, e che le persone ricevano un'informazione di tipo pedagogico sui controlli cui sono soggette.

5. **Formazione necessaria delle autorità di controllo in tutta l'Unione**

5.1. Per il Comitato, contrariamente a quanto previsto dalla Commissione nella sintesi della valutazione d'impatto (C), nel primo periodo (dopo il 2021) bisognerà insistere sulla formazione. Si parla di 76 milioni di EUR l'anno, ma il passaggio a nuove procedure richiede sempre un aggiornamento che, in questo caso, interesserebbe tutte le frontiere dell'Unione e i sistemi nazionali. Alcuni Stati membri non si sono ancora dotati di sistemi compatibili: essi dovranno compiere uno sforzo considerevole e creare interfacce che consentano loro di partecipare. Affinché sia garantita l'interoperabilità, bisognerà appianare le disparità tra i vari Stati membri.

5.2. La formazione all'utilizzo di dati di qualità e dell'UMF sarà essenziale. Il Comitato propone di istituire un centro di formazione comune per le autorità abilitate con il CEPOL ([17]), Frontex, Europol e includendo l'eu-LISA dopo aver verificato attentamente le competenze dei suoi membri.

5.3. Il MID è uno strumento unico nel suo genere, che in caso di successo rivelerà tutta la sua potenza. Il nuovo sistema richiederà la più alta qualità dei dati. Affinché esso sia all'altezza delle aspettative del progetto, tutti gli Stati membri devono partecipare allo stesso livello, altrimenti le carenze risulteranno più gravi che in passato. In tal caso, il diritto di asilo e il diritto di accesso alla protezione internazionale verrebbero compromessi (articoli 18 e 19 della Carta).

6. **Finanziamento**

6.1. L'intera architettura proposta si basa su una serie di ipotesi: l'adozione da parte delle autorità decisionali dei sistemi *EES*, *ETIAS* e *UMF*, il corretto funzionamento del *MID* e la messa in sicurezza del *CIR*. Due organi, il CEPD e l'agenzia eu-LISA, e forse anche l'agenzia ENISA, disporranno di effettivi e mezzi finanziari sufficienti? La Commissione propone un cofinanziamento dell'UE e degli Stati membri. Il Comitato osserva che la gestione del «Semestre» avviene ancora con bilanci improntati all'austerità e che, inoltre, l'attuale utilizzo delle banche dati esistenti (SIS, VIS, Prüm, *EES*) deve ancora essere ottimizzato nel rispetto degli obblighi di legge (relazione del gruppo di esperti).

([16]) Patto internazionale relativo ai diritti civili e politici — ONU — «Articolo 17: 1. Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. 2. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese.».

([17]) Agenzia dell'Unione europea per la formazione delle autorità di contrasto (con sede a Budapest, Ungheria).

6.2. Benché il Regno Unito non appartenga al sistema Schengen, il CESE si interroga sull'impatto della Brexit sul bilancio e, più in generale, sulla futura complessità della gestione dell'interoperabilità nei paesi europei che non hanno accesso al SIS ma partecipano ad altre banche dati, come Eurodac.

6.3. Il fondo previsto è l'FSI, Fondo per la sicurezza interna e delle frontiere. L'operatività è prevista a partire dal 2023. Il Comitato si chiede se cinque anni basteranno per ridurre le disparità europee e per garantire le condizioni necessarie per il successo. Il bilancio previsto è di 424,7 milioni di EUR su 9 anni (2019-2027), suddiviso fra l'Unione (FSI) e gli Stati membri. Questi ultimi devono essere in grado di far funzionare correttamente i sistemi attuali con la nuova architettura informatica. Il Comitato ritiene che la realizzazione di tali investimenti avverrà grazie al ritorno della crescita.

Bruxelles, 23 maggio 2018.

Il presidente
del Comitato economico e sociale europeo
Luca JAHIER