Yttrande från Europeiska ekonomiska och sociala kommittén om Förslag till Europaparlamentets och rådets förordning om inrättande av en ram för interoperabilitet mellan EU-informationssystem (gränser och viseringar) och om ändring av rådets beslut 2004/512/EG, förordning (EG) nr 767/2008, rådets beslut 2008/633/RIF, förordning (EU) 2016/399 och förordning (EU) 2017/2226

[COM(2017) 793 final – 2017/0351 (COD)] och

Förslag till Europaparlamentets och rådets förordning om inrättande av en ram för interoperabilitet mellan EU-informationssystem (polissamarbete och rättsligt samarbete, asyl och migration)

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

(2018/C 283/07)

Föredragande: **Laure Batut**

Remiss	Europeiska kommissionen, 18.1.2018
	Europaparlamentet, 28.2.2018
Rättslig grund	Artikel 304 i fördraget om Europeiska unionens funktionssätt
Ansvarig facksektion	Facksektionen för sysselsättning, sociala frågor och medborgarna
Antagande av facksektionen	25.4.2018
Antagande vid plenarsessionen	23.5.2018
Plenarsession nr	535
Resultat av omröstningen	160/3/2
(för/emot/nedlagda röster)	

1. **Slutsatser och rekommendationer**

1.1 EESK anser att kommissionens förslag om att förbättra interoperabiliteten mellan EU:s informationssystem beträffande gränser och viseringar samt beträffande polissamarbete och rättsligt samarbete, asyl och migration, är bra och positivt.

1.2 EESK anser att interoperabilitet bör vara ett strategiskt mål för EU för att unionen ska förbli ett öppet område och en garant för grundläggande rättigheter och rörlighet. EU och medlemsstaterna är skyldiga att skydda alla människors liv och säkerhet. Principen om ”non-refoulement” måste respekteras fullt ut.

1.3 Åtgärderna för interoperabilitet kommer att bli enklare att förstå om de

— inom ramen för EU:s migrationsstrategi garanterar en balans mellan frihet och säkerhet, i enlighet med principen om maktdelning,

— garanterar alla berörda personer deras grundläggande rättigheter, i synnerhet rätten till skydd av personuppgifter och av den personliga integriteten och rätten till åtkomst till personuppgifter samt rättelse och radering av dessa inom rimlig tid genom tillgängliga förfaranden,

— bekräftar kravet på inbyggda mekanismer för skydd av den personliga integriteten (inbyggt integritetsskydd), även i samtliga genomförandeakter,

— inte skapar nya hinder för normal gods- och persontrafik.

1.4 EESK efterlyser förfaranden och garantier avseende användningen av uppgifter för brottsbekämpande ändamål som

— innebär att man tillämpar den mest skyddande EU-lagstiftningen (den allmänna dataskyddsförordningen),

— gör det möjligt att påskynda processen för att avgöra vilken medlemsstat som är ansvarig att pröva ansökningar om internationellt skydd,

— garanterar de berörda personerna deras rätt till prövning i två instanser,

— garanterar minderåriga, särskilt ensamkommande – oavsett om de har uppehållstillstånd eller inte, om de är utsatta för förföljelse eller står åtalade – rätten att få ett visum, skyddas och integreras och att åtnjuta rätt att bli bortglömd inom en kortare tidsrymd än vuxna.

1.5 EESK anser att den nuvarande rättsliga grunden för informationssystemen bör förstärkas och ta hänsyn till att systemen för datainsamling utvecklas. Kommittén förespråkar

— ökad säkerhet i befintliga databaser och deras kommunikationskanaler,

— en utvärdering av konsekvenserna av den stärkta förhandskontrollen av riskhanteringen och

— att dataskyddsmyndigheterna (Europeiska datatillsynsmannen) genomför en fortlöpande kontroll och utvärdering av strukturen. Kommittén kräver att de ansvariga varje år till de beslutsfattande myndigheterna och kommissionen rapporterar om säkerheten hos interoperabilitetskomponenterna, samt vartannat år om vilken inverkan åtgärderna får på de grundläggande rättigheterna.

1.6 EESK anser att kompetent personal är en förutsättning för projektet och efterlyser

— ordentliga utbildningsprogram för de berörda myndigheterna och de anställda vid eu-LISA och

— en strikt kontroll av kompetensen hos personer som är anställda vid denna byrå och personer som söker arbete där.

1.7 EESK uttrycker farhågor när det gäller finansieringen av det nya systemet. En uppföljning av planeringen är avgörande för att undvika budgetöverskridanden och för att projektet ska kunna genomföras fram till 2029.

1.8 EESK rekommenderar att medborgarna informeras om projektets förlopp tills det är slutfört, och att människorna får pedagogisk information om de kontroller som de är föremål för. Kommittén anser att det måste finnas möjlighet att avsluta hela projektet om friheten och de grundläggande rättigheterna skulle äventyras av ett missbruk av systemet.

2. **Inledning**

2.1 Mot bakgrund av den globala kontexten 2017, som ansågs instabil, såväl på det geopolitiska planet som på det inrikespolitiska planet i medlemsstaterna, har rådet vid upprepade tillfällen uppmanat kommissionen att tillhandahålla de medel som krävs för att spåra personer som bedömts ”ligga i riskzonen” och som redan registrerats i någon av medlemsstaterna. Att spåra deras gränspassager, resor och rutter i Europa skulle kunna vara av avgörande betydelse för EU:s säkerhet.

2.2 I sin resolution av den 6 juli 2016 uppmanade Europaparlamentet kommissionen att tillhandahålla nödvändiga garantier när det gäller skydd av personuppgifter.

2.3 De aktuella texterna ingår i målet om bevarande och stärkande av Schengen ([1]). EU har redan antagit flera förordningar och digitala informationstjänster på områden med koppling till kontroll av gränspassager för personer och varor.

2.4 Påminnelse:

— **SIS: Schengens informationssystem**, som är en av de äldsta mekanismerna, har reviderats och hanterar ett brett spektrum av registreringar om personer och varor.

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

— **Eurodac: europeiskt system för jämförelse av fingeravtryck** för att identifiera asylsökande och tredjelandsmedborgare som har passerat de yttre gränserna irreguljärt eller som vistas olagligt i en medlemsstat, samt för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan (CESE 2016–02981, föredragande: José Antonio Moreno Díaz ([2])).

— **VIS: Informationssystemet för viseringar** (viseringskodex), som hanterar visering för kortare vistelse (CESE 2014–02932, föredragande: Antonello Pezzini och Luis Miguel Pariza Castaños ([3])).

— **EES: in- och utresesystem** (i avvaktan på beslut), ett system som på elektronisk väg ska hantera passuppgifter och in- och utresedatum för tredjelandsmedborgare som besöker Schengenområdet (CESE 2016–03098 SOC/544, föredragande: Cristian Pîrvulescu ([4])).

— **Etias: EU-system för reseuppgifter och resetillstånd** (i avvaktan på beslut), ett mycket stort automatiserat system för lagring och förhandskontroll av uppgifter från tredjelandsmedborgare som är undantagna från viseringskravet för att röra sig fritt i Schengenområdet (CESE 2016–06889 SOC/556, föredragande: Jan Simons ([5])).

— **Ecris-TCN: Europeiskt system för utbyte av tredjelandsmedborgares kriminalregisteruppgifter** (har föreslagits av kommissionen), ett elektroniskt system för utbyte av uppgifter om domstolsbeslut som redan har fattats av nationella domstolar.

2.5 Man skulle kunna likna en behörig myndighets befintliga medel vid en smart telefon med olika appar, som var och en separat tillhandahåller ”sina” uppgifter.

2.6 Samtliga system, utom SIS, är inriktade på **hantering av tredjelandsmedborgare**. Det finns sex kompletterande och decentraliserade system. Summan av de uppgifter som eftersöks är den information som utredningstjänsterna genererar via olika databaser, beroende på deras åtkomsträtt.

2.7 Kommissionen avser att svara på följande fråga:

— Hur kan man, utan att behöva förändra de strukturer som redan byggts upp eller förlora komplementariteten, få alla databaser att samverka samtidigt, så att man vid en viss inreseplats till EU:s territorium, och med hjälp av en enda sökning i systemet, kan få fram alla uppgifter som redan samlats in i befintliga, samverkande databaser och kanalisera dem till den tillsynsmyndighet som har åtkomsträtt, samtidigt som man respekterar lagstiftningen om uppgiftsskydd och de grundläggande rättigheterna?

2.8 Genom de aktuella förslagen skulle kommissionen vilja

2.8.1 att man kan dra nytta av de ytterligare möjligheter som det skulle innebära att få tillgång till databaserna vid Europol och Interpol, som redan samarbetar med de europeiska tillsynsmyndigheterna,

2.8.2 att man ”synkroniserar” informationssökningarna för att minska svarstiden när det gäller migranters ärenden och för att vid behov påskynda säkerhetsinsatser. Därför föreslår kommissionen att inrätta nya enheter som skulle göra det möjligt att få de befintliga baserna att samverka.

2.9 **Syftet är att i så stor utsträckning som möjligt avhjälpa bristerna i olika system, förbättra** förvaltningen av Schengenområdets yttre gränser, bidra till EU:s inre säkerhet, hantera identitetsbedrägerier, utreda fall med multipla identiteter, spåra misstänkta eller redan dömda personer och kontrollera deras identitet inom Schengenområdet.

2.10 För att återknyta till liknelsen med en smart telefon skulle den behöriga myndigheten inte bara få tillgång till ett flertal appar utan den skulle även samtidigt genom en enda sökning med hjälp av tillträdeskoder kunna samla in uppgifter som finns lagrade i alla stödstrukturer, PC, bärbar dator, telefon, pekplatta, lättare bärbar dator (notebook) osv.

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

3. **Systemets funktion**

3.1 Kommissionen har genomfört samråd och inrättat en högnivåexpertgrupp på området informationssystem och interoperabilitet ([6]), med medlemmar som har utsetts av medlemsstaterna, de länder som ingår i Schengengruppen, europeiska byråer såsom eu-LISA ([7]) och FRA ([8]) under samordning av GD Migration och inrikes frågor.

Metod: sammankoppling eller interoperabilitet?

3.1.1 **Sammankoppling** av informationssystemen avser möjligheten att koppla ihop dem med varandra så att man genom en sökning i ett av systemen automatiskt kan få tillgång till uppgifter i ett annat system.

3.1.2 **Interoperabilitet** ([9]) avser de olika systemens förmåga att kommunicera sinsemellan, att utbyta uppgifter och att använda den information som har överförts, i enlighet med varje systems åtkomsträtt.

3.2 *Att välja interoperabilitet*

3.2.1 Kommissionen anser att detta alternativ inte medför några stora förändringar av de nuvarande strukturerna eller behörigheterna och att uppgifterna fortfarande kommer att hållas åtskilda från varandra. Trots den stärkta kommunikationsförmågan skulle detta innebära en säkerhetsfördel för systemen och uppgifterna, som självklart inte skulle vara tillgängliga via internet. De texter om vilka kommissionen har begärt att kommittén ska yttra sig har stora inbördes likheter:

— Den ena, COM(2017) 793, avser interoperabilitet mellan informationssystem för gränser och viseringar,

— medan den andra, COM(2017) 794, avser polissamarbete och rättsligt samarbete, asyl och migration.

3.3 *De nya verktygen*

3.3.1 För att interoperabiliteten ska fungera behöver de sex grundläggande verktygen kompletteras med en ny struktur med fyra verktyg för att man ska kunna arbeta snabbt och inte starta fler än en sökning i systemet, och alltid se till att det är en behörig person som står bakom sökningen.

3.4 *En europeisk sökportal*

3.4.1 Den behöriga tillsynsmyndigheten (slutanvändaren) bör ha en enda åtkomstpunkt för hela systemet. I stället för att starta sex olika sökningar kan man via en gemensam åtkomstpunkt söka efter de begärda uppgifterna i flera databaser (polis, tull osv.) samtidigt, utan att lagra några uppgifter. Om uppgifterna finns kommer systemet att hitta dem. Om det finns misstanke om brott eller terroristverksamhet kan den första träffen kan vara neutral för den kontrollerade personen (”no-hit”), men om uppgiften stämmer överens med en ytterligare träff (”hit”) i databaser såsom SIS, EES eller Etias, skulle detta kunna leda till fördjupade sökningar och en utredning.

3.5 *Den gemensamma biometriska matchningstjänsten (shared biometric matching service)*

3.5.1 Den gemensamma biometriska matchningstjänsten (shared biometric matching service) Med hjälp av denna delade matchningsplattform kan man samtidigt söka och jämföra matematiska och biometriska data, digitala fingeravtryck och passfoton från olika databaser, såsom SIS, Eurodac, VIS, *in- och utresesystemet* ([10]) och *Ecris*, men inte *Etias*.

3.5.2 Uppgifterna i dessa databaser måste alltså vara kompatibla. De matematiska uppgifterna lagras inte i sin ursprungliga form.

3.6 *Den gemensamma databasen för identitetsuppgifter (CIR)*

3.6.1 En gemensam databas för identitetsuppgifter kommer att sammanföra biografiska och biometriska uppgifter om kontrollerade tredjelandsmedborgare, oavsett om de befinner sig vid gränsen eller i Schengenområdets medlemsstater. En flaggfunktion vid träff i de olika databaserna kommer att göra sökningarna snabbare. Under eu-LISA:s överinseende och med hjälp av byråns säkerhetsresurser kommer uppgifterna att lagras på ett sådant sätt att ingen kan få tillgång till mer än en alfanumerisk rad åt gången. CIR skulle bygga på in- och utresesystemet och Etias och skulle inte leda till att några uppgifter dubbleras. Lagret får också användas för civila sökningar.

([6]) GD Migration och inrikes frågor, enhet B/3, kommissionens beslut C(2016) 3780 av den 17 juni 2016 http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=SV.
([7]) Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa.
([8]) FRA: EU:s byrå för grundläggande rättigheter
([9]) Kommissionen, COM(2016) 205 final, meddelande, ”Starkare och smartare informationssystem för gränser och säkerhet”.
([10]) Kursiveringen indikerar att texterna avseende dessa organ ännu inte har antagits.

3.7 *Detektorn för multipla identiteter (MID)*

3.7.1 Detektorns uppgift skulle vara att kontrollera att personer med ärligt uppsåt har lämnat riktiga uppgifter om sin identitet och att bekämpa identitetsbedrägerier genom en sökning i alla databaser samtidigt. Ingen förvaltning har ännu använt sig av ett verktyg av denna typ, som bör göra det möjligt att undvika identitetsstöld.

3.8 *Byrån eu-LISA:s roll* ([11])

3.8.1 Byrån, som inrättades 2011, ska stödja EU:s politik på områdena rättvisa, säkerhet och frihet. Byrån har sitt säte i Tallinn i Estland och handhar redan samarbetet och informationsutbytet mellan olika brottsbekämpande myndigheter i medlemsstaterna och de stora it-systemens obehindrade funktion samt den fria rörligheten för personer inom Schengenområdet.

3.8.2 Byrån medverkar i projektet ”Smarta gränser” och dess roll i den nya strukturen för informationsutbyte kommer att bestå i att lagra de komponenter som är kopplade till personer, till exempel med avseende på myndigheter, utredningar och utredare. Den kommer att kontrollera att de som begär uppgifter har åtkomsträtt och ansvara för datasäkerheten, t.ex. i händelse av säkerhetsincidenter (artikel 44, förslagen (2017) 793 och 794).

3.8.3 **Det universella meddelandeformatet** (UMF) som ännu inte har skapats skulle underlätta arbetet med de nya systemen, som kommer att vara obligatoriska, vilket kräver inrättandet av gränssnitt i de medlemsstater som ännu inte har sådana och ett system för tillfällig översättning från ett språk till ett annat.

3.9 *Skydd av personuppgifter* (artiklarna 7 och 8 i stadgan):

3.9.1 I förslaget till förordning erkänns att säkerhetsincidenter kan inträffa. Medlemsstaterna och deras informationssystem måste vara de första som respekterar de principer för uppgiftsskydd som fastställs i texterna, fördraget, EU-stadgan om de grundläggande rättigheterna och den allmänna dataskyddsförordningen ([12]), som träder i kraft den 25 maj 2018.

4. **Diskussion**

4.1 *Mervärdet av interoperabilitet i en demokrati*

4.1.1 EU behöver ett regelverk och utredningskapacitet som skyddar mot brott. Interoperabilitet mellan informationssystemen innebär en möjlighet att hävda rättsstatsprincipen och skyddet av de mänskliga rättigheterna.

4.1.2 *In- och utresesystemet och Etias* kommer, i kombination med den gemensamma biometriska matchningstjänsten och CIR, att göra det möjligt att kontrollera gränspassager för misstänkta personer och att lagra uppgifter om dem. Möjligheten för de brottsbekämpande myndigheterna att via den gemensamma biometriska matchningstjänsten få tillgång till ”informationssystem som inte är utformade för brottsbekämpning på EU-nivå” (artikel 17 i förslaget till förordning om CIR (2017) 794 och 793)), kan dock inte vara förenlig med de ändamål som anges som grunderna för de aktuella förslagen. Kommittén måste i detta sammanhang hänvisa till proportionalitetsprincipen (artikel 300.4 i EUF-fördraget) och uppmanar kommissionen att undvika varje scenario av typen ”storebror ser dig” ([13]) samt att undvika att skapa hinder för EU-medborgarnas fria rörlighet (artikel 3 i EU-fördraget).

4.1.3 Den modell som föreslås för insamling och användning av de personuppgifter som erhålls vid gränserna och på EU:s territorium vid kontroller av resvägar och innehavda dokument presenteras som vattentät och endast öppen för behöriga personer och för säkerhets- och hanteringssyften, och den kommer att göra förfarandena smidigare.

4.1.4 Kommittén ifrågasätter denna vattentäthet: det finns fortfarande brister, uppbyggnaden av systemet ska ske över en tidsperiod på nio år och bygger på ”grunder” som ännu inte finns, såsom databaserna för in- och utresesystemet och Etias, eller nationella gränssnitt. Den tekniska kontexten förändras ständigt, projektet grundar sig med nödvändighet på tekniken och det finns inga budgetanslag för att hantera den föråldring som uppstår inom vissa digitala sektorer.

([11]) Europaparlamentets och rådets förordning (EU) nr 1077/2011 av den 25 oktober 2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa

([12]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). EESK:s yttrande: EUT C 229, 31.7.2012, s. 90 och EUT C 345, 13.10.2017, s. 138.

([13]) I *1984* av George Orwell.

4.1.5 Den snabbt ökande användningen av algoritmer, eller artificiell intelligens (AI), skulle ha kunnat beaktas i förslaget, både som ett verktyg för kontroll av systemen och som en säkerhetsnyckel som de beslutsfattande myndigheterna kan använda sig av för att säkerställa en demokratisk användning av strukturen.

4.1.6 I förslaget presenteras ett system för laglydiga aktörer med ärligt uppsåt. Det faktum att människor ska ha kontrollen är betryggande, men detta faktum kan även utgöra en svag länk. Kommittén föreslår att man lägger till en artikel om att införa en mekanism för att avbryta systemet i händelse av politisk kris och/eller ”förvaltningsproblem”, eftersom alla problem i en databas kan innebära en risk för hela strukturen ([14]). Generaliseringen av det universella meddelandeformatet skulle kunna leda till en internationell användning, vilket är mycket positivt men mycket riskfyllt för skyddet av personuppgifter. De behöriga myndigheterna bär ett stort ansvar. Dessa aspekter tas inte upp i de aktuella texterna. Skydd av de grundläggande rättigheterna

4.2 *De grundläggande rättigheterna är absoluta*

4.2.1 Begränsningar får endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen, och om de är förenliga med det väsentliga innehållet i de grundläggande rättigheterna (artiklarna 8 och 52.1 i stadgan om de grundläggande rättigheterna). Kommittén ställer sig frågan hur man kan bedöma kontrollåtgärdernas proportionalitet när det gäller migranter som flyr förföljelse och söker asyl i EU. (COM(2017) 794 final, Motivering – Grundläggande rättigheter). Sökandet efter misstänkta i syfte att förebygga kriminella handlingar, särskilt terrorism, **får inte medföra att våra demokratier går mot en utveckling där man kan straffas för brott som man ännu inte begått**. Det måste fortsatt finnas en skillnad mellan ”verksamhet” som stör den allmänna ordningen och ”åsikter”.

4.2.2 Om alla människor respekterar de rättigheter som fastställs i stadgan bör detta garantera den balans mellan säkerhet och frihet som krävs för att demokratin ska överleva. Kommittén anser att en sådan balans är av avgörande betydelse och bör vara ett permanent mål för samtliga myndigheter, inklusive tillsynsmyndigheter, såväl på nationell som europeisk nivå.

4.2.3 Information om vilka myndigheter som deltar i en sökning och tillhörande metadata kommer att lagras i systemet. De grundläggande rättigheter som dessa behöriga myndigheter besitter bör också respekteras i fråga om de uppgifter som genereras, i synnerhet med avseende på säkerhet, integritet, samt vid fall av skadliga intrång i strukturen och missbruk av uppgifter från och med tidpunkten för insamlingen av uppgifterna till dess att de raderas.

4.3 *Dataskydd*

4.3.1 I förslaget erkänns principen om inbyggt persondataskydd och persondataskydd som standard, även om man i motiveringen påminner om att det enligt Europeiska unionens domstol inte rör sig om en absolut rättighet. Kommittén erkänner fördelarna med förebyggande åtgärder för att garantera säkerhet, kampen mot falska identiteter och säkerställandet av rätten till asyl. Men vi vill understryka gränserna för kvantifiering och anonymisering av uppgifter: de berörda personerna kan till exempel behöva sina uppgifter i ett senare skede.

4.3.2 Vi understryker också att den typ av uppgifter som lagras (biometriska och biologiska) är av särskilt intresse för vissa företag och för kriminella. It-säkerheten är i detta sammanhang lika viktig som den fysiska säkerheten, men återspeglas i alltför liten utsträckning i förslagen. Uppgifterna lagras på en enda fysisk plats – även med de allra striktaste säkerhetsarrangemang kan den utsättas för risker.

4.3.3 EESK påminner om att när det gäller dataskydd och rätten till radering (rätten att bli bortglömd) omfattas EU:s organ av förordning (EG) nr 45/2001, som ger ett mindre skydd än den allmänna dataskyddsförordningen ([15]) från 2016 (som träder i kraft i maj 2018), som medlemsstaterna omfattas av. EESK betonar att tillämpningen av denna rättighet är komplex, och betvivlar att resenärer, migranter och asylsökande framgångsrikt kommer att kunna kräva att den efterlevs.

1) Skyddet av personuppgifter måste valideras för samtliga befintliga databaser – nationella och europeiska – för att alla uppgifter ska vara skyddade.

2) Detta skydd är av avgörande betydelse för att medborgarna ska acceptera att underkastas detta vidsträckta övervakningsnätverk.

4.3.4 Lagringstiden för uppgifter som samlats in av behöriga myndigheter specificeras inte i förslagen. I texterna nämns förfarandet för rätt till korrigering och/eller radering, som bollas mellan den medlemsstat till vilken begäran har ställts och den stat som är ansvarig för prövningen, men inte lagringstiden för uppgifterna (artikel 47 i förslagen). Kommittén rekommenderar att lagringstiden fastställs och att den ska vara kortare för minderåriga (artikel 24 i stadgan), utom när det gäller terrorism, så att de få möjlighet till integrering.

([14]) Europeiska datatillsynsmannen, Expertgruppens slutrapport, bilaga, maj 2017.
([15]) Den allmänna dataskyddsförordningen (förordning (EU) 2016/679).

4.4 *Förvaltning och redovisningsskyldighet*

4.4.1 Internationella databaser omfattas inte av samma regler som europeiska datoriserade system. Inrättandet av ett internationellt format för åtkomst, som skulle kunna bli internationellt, skulle endast vara en teknisk komponent som inte gör bestämmelserna enhetliga, även om Interpol självfallet måste efterleva artikel 17 i FN:s konvention ([16]). För övrigt faller åtkomsträtten även fortsättningsvis under medlemsstaterna. EESK anser att denna fråga bör behandlas i förslagen.

4.4.2 En enda sökning ska räcka för att få den samlade informationen från de europeiska databaserna. EESK understryker att den byråkrati som skapas gott och väl kommer att uppvägas av den tid man vinner. Kommissionen kommer tillsammans med medlemsstaterna att ansvara för förvaltningen inom ramen för ett kontrollförfarande. Centralpunkten kommer att vara byrån eu-LISA, som bland annat ska säkerställa att det finns förfaranden för insamling av uppgifter om interoperabilitetskomponenternas funktion. Byrån ska samla in uppgifter från medlemsstaterna och Europol och vart fjärde år lämna in en teknisk utvärderingsrapport till rådet, Europaparlamentet och kommissionen. Kommissionen utarbetar i sin tur en övergripande rapport ett år efter varje utvärderingsrapport (artikel 68 i förslagen). Kommittén anser att dessa tidsperspektiv är alltför långa. Bedömningen av säkerheten i interoperabilitetskomponenterna (artikel 68.5 d) bör äga rum åtminstone varje år och bedömningen av inverkan på de grundläggande rättigheterna åtminstone vartannat år (artikel 68.5 b).

4.4.3 Kommittén beklagar att så grundläggande frågor som de som tas upp i de aktuella förslagen ska hanteras av europeiska byråer, vars rekryteringsförfaranden och funktion är oklara för många medborgare. Vi anser att det är nödvändigt att utbyta bästa praxis och att samråda med alla oberoende tillsynsmyndigheter avseende användningen av uppgifter (Europeiska datatillsynsmannen) och andra byråer, såsom Europeiska unionens byrå för grundläggande rättigheter (FRA) och Europeiska unionens byrå för nät- och informationssäkerhet (Enisa).

4.4.4 Inrättandet av alla dessa nya strukturer och förfaranden kommer att ske med hjälp av delegerade akter och genomförandeakter från kommissionen. Kommittén skulle vilja att målet att respektera de grundläggande rättigheterna och rätten till skydd av personuppgifter ska finnas inskrivet i alla dessa akter permanent, i en ansats till ett bättre mottagande av människor vid gränserna. EESK rekommenderar att EU-medborgarna informeras om etapperna fram till projektets slutförande, och att människorna får pedagogisk information om de kontroller som de är föremål för.

5. **Utbildning som behövs för alla tillsynsmyndigheter i hela unionen**

5.1 Kommittén anser, i motsats till vad kommissionen anger i sin sammanfattade konsekvensanalys (C), att det kommer att krävas mycket utbildning under den första perioden (efter 2021). Kommissionen anger ett belopp på 76 miljoner euro per år. Övergången till nya förfaranden kräver alltid en uppdatering. Det handlar här om EU:s samtliga gränser och de nationella systemen. Vissa medlemsstater har ännu inte system som är kompatibla och måste göra avsevärda insatser för att införa gränssnitt som gör det möjligt för dem att delta. För att interoperabiliteten ska fungera bör skillnaderna mellan medlemsstaterna undanröjas.

5.2 Utbildning i god användning av uppgifter och det universella meddelandeformatet (UMF) kommer att vara av avgörande betydelse. EESK föreslår att Cepol ([17]), Frontex och Europol osv. anordnar gemensam utbildning för behöriga myndigheter, inbegripet eu-LISA vars medlemmar bör få sin behörighet strikt kontrollerad.

5.3 Ett verktyg som detektorn för multipla identiteter finns ingen annanstans. Om verktyget blir framgångsrikt kommer det att bli mycket kraftfullt. Den nya strukturen kommer att kräva att uppgifterna är av högsta kvalitet. För att allt ska motsvara förväntningarna på projektet måste samtliga medlemsstater delta i samma utsträckning, annars kommer bristerna att bli allvarligare än tidigare. Om så blir fallet kommer rätten till asyl och rätten till internationellt skydd att undergrävas (artiklarna 18 och 19 i stadgan).

6. **Finansiering**

6.1 Grunden till hela den struktur som föreslås bygger på vissa antaganden och är beroende av att de beslutsfattande myndigheterna antar *in- och utresesystemet*, *Etias* och *UMF*, att *detektorn för multipla identiteter* fungerar väl och att den *gemensamma databasen för identitetsuppgifter (CIR)* är säker. Har de två organen EDPS och byrån eu-LISA, och eventuellt Enisa, tillräckliga personalresurser och ekonomiska resurser? Kommissionen föreslår samfinansiering mellan EU och medlemsstaterna. Kommittén konstaterar att förvaltningen av den europeiska planeringsterminen fortfarande görs med åtstramade budgetar och att den aktuella användningen av befintliga databaser (SIS, VIS, Prüm och *in- och utresesystemet*) för övrigt bör optimeras ytterligare vad gäller de rättsliga kraven (expertgruppens rapport).

([16]) Den internationella konventionen om medborgerliga och politiska rättigheter – FN, ”Artikel 17: 1. Ingen får utsättas för godtyckligt eller olagligt ingripande med avseende på privatliv, familj, hem eller korrespondens och inte heller för olagliga angrepp på sin heder eller sitt anseende. 2. Var och en har rätt till lagens skydd mot sådana ingripanden och angrepp.”

([17]) Cepol, Europeiska unionens byrå för utbildning av tjänstemän inom brottsbekämpning (Budapest, Ungern).

6.2 EESK undrar över de budgetmässiga konsekvenserna av brexit, även om Förenade kungariket inte är med i Schengensystemet, och mer allmänt över den framtida komplexiteten i hanteringen av interoperabiliteten i de europeiska länder som inte deltar i SIS men som deltar i andra system, t.ex. Eurodac.

6.3 Den fond som man planerar att använda är Fonden för inre säkerhet. Driftsstarten planeras till 2023. Kommittén ställer sig frågande till om fem år räcker för att minska skillnaderna inom EU och för att de förutsättningar som krävs för att projektet ska bli framgångsrikt ska kunna uppnås. Den planerade budgeten uppgår till 424,7 miljoner euro under nio år (2019–2027). EU (Fonden för inre säkerhet) och medlemsstaterna kommer att behöva stå för finansieringen. Medlemsstaterna måste uppnå en situation där de befintliga systemen fungerar väl tillsammans med den nya it-strukturen. Kommittén anser att en förbättrad tillväxt kommer att bidra till förverkligandet av dessa investeringar.

Bryssel den 23 maj 2018.

Luca JAHIER
Europeiska ekonomiska och sociala kommitténs ordförande