Briefing
June 2017

European Parliament

Interoperability of European information systems for border management and security

SUMMARY

The collection, processing and sharing of data using new technologies are becoming central to the European Union (EU)'s border management and internal security. In the EU, there are a number of information systems, or databases, that support border management and internal security policies by providing border guards, migration and asylum officials, and law enforcement authorities with information on various categories of people, such as people crossing EU's external borders, staying in the EU or applying for asylum in an EU Member State.

In 2016, the European Commission launched a reflection process on how to improve and develop EU information systems for border management and security. One key dimension of this process is to make the various information systems more interoperable, so as to allow the simultaneous consultation and automatic interconnection of data. While the need to ensure appropriate and effective collection and exchange of information is widely recognised, disagreements remain about the ways and extent to which data should be collected and used, the authorities that can access the data, and the implications for the fundamental rights of individuals, such as the right to privacy and the protection of personal data.

In this briefing:

EPRS | European Parliamentary Research Service
Author: Costica Dumbrava
Members' Research Service
PE 607.256

EN

Glossary

Interoperability: the ability of information technology (IT) systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge.

Single search interface: a technical solution enabling several information systems to be queried simultaneously and the combined results to be visualised on a single screen.

Interconnectivity of information systems: possibility of linking information systems so that data from one system could be consulted automatically by another system.

Shared biometric matching service: a service that enables single searches with biometric data across several information systems.

Common repository of data: a system containing common alphanumerical identity data that is connected with data modules stored in specific information systems.

Background

The European Commission highlighted the interoperability of information systems as a priority challenge in its 2015 communication on the European agenda on security. In 2016, the Commission launched a reflection process on how to make the management and use of information systems in the area of border management and security more effective and efficient. One key dimension of this process is to explore ways in which different European information systems could become interoperable. This reflection was bolstered by the creation, in May 2016, of the high-level expert group on information systems and interoperability (HLEG). The HLEG brings together high-level representatives of the Commission, Member States, associated members of the Schengen area, relevant EU agencies, the European Counter Terrorism Centre (ECTC), and the European Data Protection Supervisor (EDPS), and also representatives of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and of the general secretariat of the Council as observers. HLEG presented recommendations on strengthening and developing the EU's information systems and interoperability first in its interim report of December 2016, and later in its final report of May 2017. In its fourth progress report towards an effective and genuine security union, the European Commission stated that there was a 'clear need for existing and future EU information systems to be searchable simultaneously using biometric identifiers to close off this avenue for terrorists and criminals'.

European information systems for border management and security

Major EU databases in the area of justice and home affairs

The *Schengen Information System* (SIS) is the largest centralised European information system. It supports external border management and law enforcement cooperation in the Schengen area by enabling border and law enforcement authorities to create and check alerts on certain people and objects. Access to SIS data is given to national authorities responsible for border control, police, customs, visa and vehicle registration and, by extension, to national judicial authorities when this is necessary for the performance of their tasks, as well as to Europol.

The *Visa Information System* (VIS) supports the implementation of the common EU visa policy by collecting data on people applying for short-stay visas to enter the Schengen area. The database contains personal data from visa applications, including fingerprints and facial images. Access to the VIS is given to national visa authorities when examining

Schengen visa applications, border authorities upon entry into the Schengen area, and to migration and asylum authorities within the Schengen area in charge with verifying the identity of visa holders. National law enforcement authorities and Europol can access the VIS for the purpose of preventing, detecting and investigating terrorist offences and other serious crimes.

The *European dactyloscopy database* (Eurodac) facilitates the application of the Dublin Regulation by helping to determine the country responsible for the assessment of asylum claims by establishing the point of entry into the EU. Member State authorities responsible for asylum applications have access to Eurodac. As of July 2015, Eurodac is also accessible to designated national authorities responsible for the prevention, detection or investigation of terrorist offences or other serious crimes.

The *Europol Information System* (EIS) is Europol's central criminal information and intelligence database. It contains information on serious international crimes, suspects and people with a criminal record, criminal structures and offences and the means used to commit them. Access to the EIS is given to Europol officials, Member States' liaison officers, seconded national experts stationed at Europol's headquarters, and staff working in the Europol National Units and in national authorities.

Other European databases and systems for information exchange[1] include: Interpol's stolen and lost documents database (SLTD); the Prüm framework; the European Information Exchange Model (EIXM); the EU Passenger Name Record system (EU PNR); the European Criminal Records Information System (ECRIS); and Eurojust's case management system (CMS).

Main shortcomings and proposed changes

In its communication on stronger and smarter information systems, presented in April 2016, the European Commission identified a series of key shortcomings in the existing information systems in the area of border management and security:

- partial utilisation of the existing information systems;
- suboptimal functionalities and technical limitations;
- gaps in the EU's informational architecture;
- a complex legal and policy landscape;
- overall fragmentation of EU data management architecture and limited interoperability between information systems.

The way the EU's information systems are used has generally improved recently, although their full potential has not yet been reached. According to reports by the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA), the total number of alerts inserted in the SIS increased from 50 million in 2013 to almost 71 million in 2016. The number of visa applications registered in the VIS increased from 5.5 million in 2014, to 6.5 million in 2015 and the number of data subjects (sets of fingerprints) in Eurodac increased from 0.4 million in 2012 to 1.6 million in 2016. According to Europol, between 2006 and 2012, the number of objects in the EIS increased from under 50 000 to more than 150 000. The number of searches in the databases have also generally increased. For example, the number of searches in the SIS increased from 1.2 billion to 3.9 billion between April 2013 and December 2016. However, the contributions of Member States to various databases remain uneven. For example, alerts on foreign terrorist fighters (FTF) are still not systematically inserted and checked in the SIS. According to a note presented by the ECTC, not all Member States

systematically insert data on FTF into the SIS and, when they do, the information recorded is often incomplete. As reported by the ECTC, although all the perpetrators of the Paris and Brussels attacks were subjects of SIS alerts, the information inserted was insufficient and, in the absence of biometric identifiers, the attackers were able to travel under false identities and thus avoid being stopped at the external border.

Despite expanding the access of law enforcement authorities to the VIS and Eurodac, the role played by these databases in the area of internal security remains limited. As reported by the eu-LISA, between September 2013 and September 2015, only 11 Member States granted access to the VIS to law enforcement authorities, which resulted in about 9 400 searches. Similarly, between July and December 2015, only five Member States used Eurodac for the purpose of preventing, detecting and investigating terrorist offences and other serious crimes (Germany, France, the Netherlands, Austria and Finland), performing 95 searches in total. Although Europol has gained extensive access to the VIS and Eurodac, it has not yet established connections to these databases.

Currently, identity checks in the SIS are based on alphanumeric searches (name and date of birth), while fingerprints can be used only in order to verify and confirm the identity of a person who has already been identified by name. The SIS legal framework allows the use of facial image and fingerprints in order to verify identity, provided that the necessary technology is available. The European Commission and the eu-LISA are testing an automatic fingerprint identification system (AFIS) for the SIS. In March 2016, the ECTC reported problems related to the absence of common standards for inserting alerts, and interpreting and reporting information in the SIS. For example, Member States continued to apply different definitions and standards with regard to identified foreign terrorist fighters. The European Commission has made several legal and technical improvements to the SIS to enable real-time communication between the ground and the competent services in other Member States and to improve information exchange on terrorist suspects. In 2015, the Commission revised the Schengen handbook and finalised a set of common risk indicators to be used during border checks in order to detect foreign terrorist fighters. The proposal for a directive on combating terrorism obliges Member States to enter alerts on suspected or convicted terrorist offenders systematically in the SIS.

In order to close information gaps related to people who might pose security risks but are not covered by the existing database, the Commission has adopted proposals to expand the scope of several existing databases and to establish two new information systems. In January 2016, the Commission adopted a proposal to upgrade ECRIS by establishing an index system enabling national authorities to determine which Member State holds criminal records of a third-country national. The proposal introduces the obligation to store criminal record information, including fingerprints, on convicted third-country nationals and to exchange such information for the purpose of criminal proceedings. In May 2016, the Commission put forward a proposal for a recast Eurodac Regulation that will introduce the obligation to collect data on third-country nationals or stateless people who have been apprehended crossing EU borders irregularly or staying illegally on EU territory. The proposal expands the range of data collected (fingerprints and facial images) and lowers the age of people subject to fingerprint checks.

In December 2016, the Commission adopted three proposals aimed at revising the SIS. First, the proposal for the revision of SIS in the field of police cooperation and judicial cooperation in criminal matters introduces new alerts and checks, extends the use of

biometrics and expands access to the SIS for law enforcement authorities. It also makes it mandatory for the Member States to issue alerts on people connected with terrorist offences. Second, the proposal for a regulation on the establishment, operation and use of the SIS in the field of border checks introduces the obligation for Member States to enter into the system entry bans issued to illegally staying third-country nationals. Third, the proposal for a regulation on the use of the SIS for the return of illegally staying third-country nationals introduces the obligation for Member States to enter all return decisions in the system with a view to enhancing their enforcement and contributing to reducing incentives to irregular migration. In April 2016, the Commission adopted a proposal for establishing an Entry/Exit System (EES) that will record entry and exit data from all third-country nationals, including from visa-exempt third countries, crossing the Schengen borders. In November 2016, the Commission presented a proposal to establish the European Travel Information and Authorisation System (ETIAS) that will collect pre-arrival information about non-EU citizens travelling to the EU, including family members of EU citizens and for third-country nationals enjoying the right to free movement but who do not hold a residence card issued by a Member State.

Towards interoperability of information systems

Commission communication on enhanced interoperability (2005)

In its November 2005 communication on improved effectiveness, enhanced inter-operability and synergies among European databases in the area of justice and home affairs, the European Commission identified the shortcomings of the structure and use of European information systems, and mapped possible developments. The Commission envisaged the development of a service-oriented informational architecture to allow functions to be shared 'in a flexible and cost-efficient way without merging existing systems'. The Commission emphasised that 'when putting forward possible future proposals, the Commission will proceed … to a specific impact assessment on the respect of fundamental rights'. The Commission's definition of interoperability as 'a technical rather than a legal or political concept' was criticised because it ignored the complex legal and political issues raised by interoperability: according to De Hert and Gutwirth,[2] 'interoperability is much more than interconnecting ICT-systems. It obviously has technical, semantic, social, cultural, economic, organisational and legal dimensions'.

The Hague programme (2014)

In the Hague Programme, adopted in November 2014, the European Council called on the Council to examine ways to maximise the effectiveness and interoperability of EU information systems in tackling illegal immigration and improving border controls. The programme stated that 'the methods of exchange of information should make full use of new technology and must be adapted to each type of information, where appropriate, through reciprocal access to or interoperability of national databases, or direct (on-line) access, including for Europol, to existing central EU databases, such as the SIS'. It also maintained that 'new centralised European databases should be created only on the basis of studies that have shown their added value'.

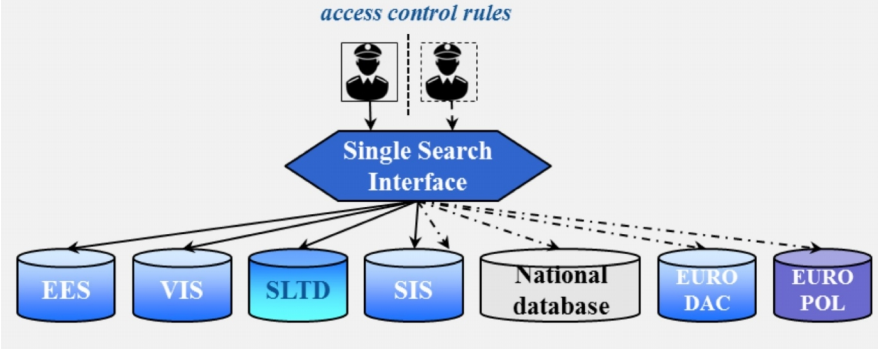
Commission communication on stronger and smarter information systems (2015)

The Commission communication on stronger and smarter information systems for borders and security, of April 2015, distinguished four dimensions of interoperability, each raising specific technical, operational and legal issues. The four interoperability options identified were:

1. establishing a single search interface for accessing different information systems simultaneously;
2. interconnecting information systems to allow data registered in one system to be automatically consulted by another system;
3. creating a shared biometric matching service that will support various information systems;
4. establishing a common repository of data for different information systems.

Single search interface

Figure 1 – Single search interface for European information systems



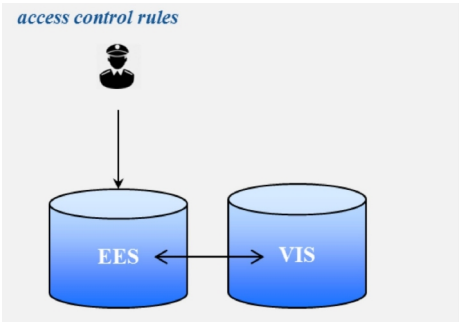
Source: European Commission.

The single search interface would enable competent authorities to query several information systems simultaneously and to visualise the combined results on a single screen, with full respect for their access rights and in line with the specific purposes of the databases searched (see Figure 1).

Interconnectivity of information systems

The interconnectivity of information systems refers to the possibility of linking information systems so that data from one system could be consulted by another system automatically at a central level (see Figure 2). This solution requires technical compatibility between the systems, as well as 'appropriate data protection safeguards and strict access control rules'. A number of recent legislative proposals make reference to interconnectivity between the VIS and other information systems. Under the proposal for establishing the EES, the fingerprints of visa holders already stored in the VIS will not be stored once more in the EES, but instead the EES will re-use fingerprints from the VIS for the purposes of the EES. The proposal for establishing the ETIAS also provides for the interoperability of the new system and the VIS.

Figure 2 – Interconnectivity of systems (EES-VIS)



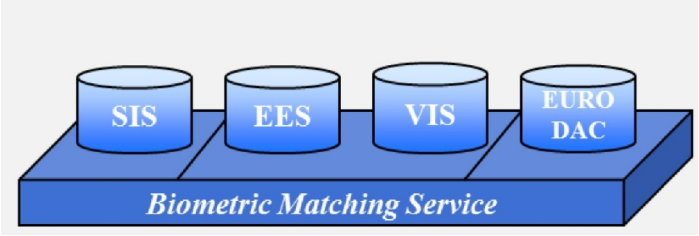
Source: European Commission.

Shared biometric matching service

The use of a shared biometric matching service will enable single searches with biometric data across several information systems (see Figure 3). According to the Commission, this solution will require special attention in view of 'respecting personal data protection rules

by compartmentalising the data, with separate access control rules for each category of data'.

Figure 3 – Shared biometric matching service

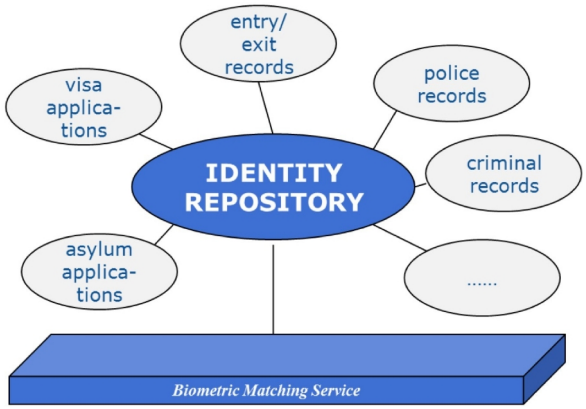


Source: European Commission.

Common repository of data

The common repository of data would consist of a core module containing alphanumeric and biometric data that would be connected with other specific modules containing data elements from different information systems (see Figure 4). This solution would imply the relocation of all alphanumerical identity data from existing information systems into a common repository. Given that this solution 'raises important questions of definition of purpose, necessity, technical feasibility and proportionality of the data processing involved', the Commission considered it only as a long-term objective.

Figure 4 – Common repository of data



Source: European Commission.

Council roadmap to enhance information exchange and management

In June 2016, the Dutch Presidency of the Council put forward a roadmap to enhance information exchange and information management including interoperability solutions in the area of justice and home affairs. The roadmap set out the framework for a more integrated EU information architecture and specific, practical short- and medium-term actions as well as long-term orientations to enhance information management and information exchange. One of the horizontal guidelines outlined by the Presidency was to 'pursue interoperability solutions, including but not necessarily ending with implementation of a single search interface following the development of (a) technical solution(s)'. Two implementation reports on the roadmap have been presented, the first in November 2016 and the second in May 2017.

High-level expert group on information systems and interoperability

In its interim report, the HLEG stated that ensuring respect for fundamental rights and data protection rules is central to its work. HLEG identified several priority options to be considered in promoting the interoperability of information systems. It recommended

that the Commission start working on establishing a single search interface and expressed reservations with regard to interconnecting information systems, beyond the proposed interconnection of the VIS and the future EES. According to HLEG, sharing a biometric matching service would offer financial, maintenance and operational benefits and would enable single searches with biometric data, and a common identity repository would help to avoid data duplication and overlaps.

In its final report, the HLEG restated that a proper exchange of information between Member States can serve not only to identify irregular migrants and criminals but also to protect vulnerable people, such as victims of trafficking and abducted children. It maintained that 'this positive effect of information systems on the fundamental rights of persons is often ignored, and deserves more attention and emphasis'. Nevertheless, given their impact on the right to privacy and the protection of personal data, HLEG argued that 'information systems for border management, migration and security should be designed and implemented in compliance with all relevant data protection principles', including data protection by design and by default, and 'the requirements of necessity, proportionality, purpose limitation and quality of data'.

HLEG emphasised the need to ensure data quality, as wrong or incomplete data could greatly affect the 'fundamental rights of innocent people'. In this respect, it recommended setting up a central data control mechanism, implementing the data quality roadmap proposed by the eu-LISA, and establishing a data warehouse containing anonymised data extracted from information systems. With a view to establishing a comprehensive framework for law enforcement access to various databases, HLEG recommended drawing a clear distinction between access for identification purposes and access for investigative purposes. Whereas access for identification purpose 'should not require prior authorisation or be subject to complicated procedures', requests for investigations 'should continue to require, except in emergency situations and under clearly defined conditions, *ex ante* verification and authorisation'.

HLEG recommended the creation of a centralised single-search interface, or European search portal, capable of searching in parallel all relevant EU systems and possibly Interpol's databases. It reaffirmed that the interconnecting information systems option 'should only be considered on a case-by-case basis, while evaluating if certain data from one system needs to be systematically and automatically reused to be entered into another system'. HLEG recommended the establishment of a shared biometric matching service that would enable single searches with biometric data. A preferred system of 'hit/non-hit flags' – indicating the presence of data in other systems – should be designed to ensure compliance with the original data access rules for different information systems and with data protection principles. Lastly, HLEG recommended the creation of a common repository of alphanumeric identity data for different information systems, which would enable identity records in the common repository to be linked to specific data from the different systems. The repository would help to avoid the duplication of data and 'overcome the current fragmentation in the EU's architecture of data management for border control and security and the related risk of blind spots'.

In a follow-up discussion paper on interoperability in the light of the recommendations by HLEG, the Council invited the Commission to make legislative proposals by the beginning of 2018 in order to implement interoperability solutions.

Position of the European Parliament

The European Parliament has consistently advocated for more effective cooperation between Member States' law enforcement authorities and for increased use of European information systems, provided that appropriate safeguards on data protection and privacy are maintained.

In June 2012, the European Parliament blocked five files in the area of justice and home affairs in a dispute about the reform of the Schengen governance rules. Parliament demanded stricter security measures for data inserted in the SIS and an assessment on the collection of biometric data from children.[3] In its resolution of 12 September 2013, Parliament stressed that new IT systems in the area of migration and border management should be analysed carefully, in the light of the principles of necessity and proportionality. In its report of December 2012, LIBE agreed on extending access to Eurodac to law enforcement authorities and Europol but insisted on imposing strict data protection safeguards. In its resolution of 17 December 2014 Parliament called on the Member States to make a better use of valuable existing instruments, including through 'more expeditious and efficient sharing of relevant data and information'. In its resolution of 11 February 2015 on anti-terrorism measures, Parliament restated its call on the Member States to make optimal use of existing databases and reiterated that 'all data collection and sharing, including by EU agencies such as Europol, should be compliant with EU and national law and based on a coherent data protection framework offering legally binding personal data protection standards at an EU level'. In its resolution of 9 July 2015, Parliament called for 'greater use of the existing instruments and databases such as SIS and ECRIS' and for 'the integration and further development of all aspects of judicial cooperation in criminal matters'.

Key concepts – *Function creep*

The digital storage, sharing, and processing of data raise the issue of function creep, which refers to the 'continuous repurposing of information initially gathered for other purposes'.[4] On the one hand, function creep is an inevitable outcome of innovation, a function of policy development that may be accepted if properly justified. On the other hand, function creep may violate standards under data protection law, namely the purpose limitation principle and the prohibition on automated decision-making.[5]

In its resolution on the situation in the Mediterranean and the need for a holistic EU approach to migration of 12 April 2016, Parliament stressed that the integrity of the Schengen Area and the abolition of internal border controls were dependent on having effective management of external borders and an effective exchange of information between Member States. In its resolution of 6 July 2016, Parliament called on the European Commission to present proposals to improve and develop existing information systems, to address information gaps and to move towards interoperability, accompanied by necessary data protection safeguards. In February 2017, the LIBE rapporteur presented a draft report on the recast Eurodac proposal, in which she welcomed the reinforced role of Eurodac in tracking unaccompanied minors. In a report on the EES proposal, the LIBE rapporteur agreed to extend access to the EES to law enforcement authorities but pushed for stronger data protection provisions.

On 23 March 2017, the LIBE Committee held its first Security Dialogue with Commissioner Julian King on the implementation and use of existing information-sharing instruments in the area of security. Among the key issues raised in the debate were the lack of proper impact assessments accompanying Commission's proposals in the area and the push to

expand data collection and to multiply databases despite the fact that existing databases are not used effectively.

Stakeholders' views

European Data Protection Supervisor (EDPS)

The EDPS has consistently stated that the expansion of data collection for border management and security purposes should be appropriately justified in view of the principles of necessity and proportionality and that more stringent safeguards should apply in the case of biometric data. In its comments on the Commission's communication on interoperability, of March 2006, the EDPS argued that 'before creating new databases or new functionalities, investments should be made in ensuring full use of already existing databases'. It pointed out that interoperability is a complex concept that is not limited to technical matters only, as suggested by the Commission. According to the EDPS, the continuous development of databases increases the risk of 'function creep' – when the interlinking of two databases designed for two distinct purposes results in a third one for which they were not built – thus violating the data protection principle of purpose limitation.

In December 2012, the EDPS criticised the proposal to extend access to Eurodac by law enforcement authorities as 'a serious intrusion into the rights of a vulnerable group of people in need of protection'. In his opinion on the reform of Common European asylum System (CEAS), of September 2016, the EDPS stated that 'the extension of the scope of the Eurodac database does not only raise concerns in relation to the purpose limitation principle, but can in relation to the proportionality of the processing: a database, regarded as proportionate when used for one specific purpose, can become inadequate or excessive when the use is expanded to other purposes afterwards'. The EDPS recommended that the Commission make available a full data protection and privacy impact assessment in order to measure the impact on privacy, as required by the new data protection framework. In its opinion on the second EU Smart Borders Package, of September 2016, the EDPS recognised 'the need for coherent and effective information systems for borders and security' but underlined 'the significant and potentially intrusive nature of the proposed processing of personal data under the EES'. The EDPS recommends differentiating clearly between the border management and law enforcement purposes of the EES. While not against interoperability, the EDPS emphasised that interoperability increases 'the risks of infringement of data protection principles, and in particular of the purpose limitation principle'. In his March 2017 opinion on the proposals for establishing the ETIAS, the EDPS stated that, given that various kinds of data in the new database that were collected for administrative purposes will become accessible to a broader range of public authorities, the proposal requires 'an assessment of the impact that the proposal will entail on the right to privacy and the right to data protection'. The EDPS called for 'convincing evidence supporting the necessity of using profiling tools for the purposes of ETIAS'. In his opinion on the new legal basis of the SIS, of May 2017, the EDPS considered that, given that the proposals envisage the collection of new biometric data they 'should be complemented with the impact assessment of the right to privacy and the right to data protection'.

In his statement annexed to the HLEG's final report, the EDPS maintained that it was 'not in a position to endorse all the conclusions referred to by the high-level expert group in its final report on existing systems, new systems and interoperability of systems' because 'full compliance with data protection requirements' could only be assessed having 'a

comprehensive and further detailed picture of the measures and solutions envisaged by the group'. The EDPS endorsed the idea of establishing a central single search interface 'as long as this solution fully complies with purpose limitation and access rights' but warned that 'a common (and centralised) identity repository raises serious issues in terms of data protection'.

EU Fundamental Rights Agency (FRA)

According to Article 8 of the Charter of Fundamental Rights of the European Union, the fundamental right to data protection applies to every individual whose data are processed by a controller in the EU whether or not he/she is an EU citizen, a migrant (irregular or not), an asylum seeker or a presumed innocent. According to Article 52 (1) of the Charter, any interference with or limitation on the exercise of the right to the protection of personal data must be necessary and genuinely meet objectives of general interest or the need to protect the rights and freedoms of others. In a speech delivered on 25 April 2017 before the HLEG, Michael O'Flaherty, Director of FRA, stated that interoperability can contribute to ensure better and timelier protection of people entering the EU, including vulnerable people, such as missing children and trafficked people, and can be a 'crucial security and law enforcement tool'. However, making information systems more interoperable raises important fundamental rights issues. He pointed to seven key risks: attempts to illegally access personal data; unlawful sharing of data with third countries; partial information about a person in one area (e.g. the existence of a record) influencing decision making in another area; cases of wrong matches or inaccurate data; the disproportionate impact on children; serious human rights implications for irregular migrants; and the risk of discriminatory profiling.

Key concepts – *Social sorting*

The expansion of databases and the extended access of law enforcement authorities may lead to generic surveillance and thus raise suspicion without prior evidence. This surveillance may generate social sorting[6] – a phenomenon in which the predefined criteria used to survey and classify people contribute to reinforcing long-term social differences, along ethnic, national, racial or religious lines for instance.[7]

In the executive summary of its paper on fundamental rights and interoperability, annexed to the HLEG's final report, FRA stated that 'interoperability should not lead to the processing of more – biometric or alphanumeric – data than necessary for the existing purposes under the individual legal instruments'. Given that data stored in information systems may not always be accurate, there is an important need to uphold the right to effective remedies. Special attention should be paid to the rights of the child as 'interoperability may magnify some pre-existing risks in the case of children, particularly as the child had no say in the parents' decision to migrate'. Enhanced interoperability may help in identifying missing children, detecting identity fraud, and reducing the risk of apprehension, detention or return of people in need of international protection. However, by supporting law enforcement measures, interoperability may have disproportionate impact on certain people, such as irregular migrants, who may avoid accessing public services for fear of being apprehended. Lastly, interoperability may also increase the risk of discriminatory profiling. The new directive on data protection in law enforcement prohibits automated risk assessment or profiling based on algorithms that are primarily or solely determined by personal characteristics that reveal sensitive information such as, race, ethnicity, health, sexual orientation, or religious beliefs.

Main references

Alegre, S., Jeandesboz, J., Vavoula, N., European Travel Information and Authorisation System (ETIAS): Border management, fundamental rights and data protection, European Parliament, Directorate General for Internal Policies, April 2017.

Dumbrava, C., European information systems in the area of justice and home affairs: An overview, EPRS, European Parliament, May 2017.

Dumbrava, C. Revision of the Schengen Information System for law enforcement, EPRS, European Parliament, March 2017.

Gatto, A., Carmona, J., European Border and Coast Guard System, EPRS, European Parliament, October 2016.

Ivanov, D., Reform of the Dublin System, EPRS, European Parliament, March 2017.

Orav, A., Recast Eurodac Regulation, EPRS, European Parliament, March 2017.

Orav, A., D'Alfonso, A., Smart Borders: EU Entry/Exit System, EPRS, European Parliament, June 2017.

Radjenovic, A., European Travel Information and Authorisation System (ETIAS), EPRS, European Parliament, March 2017.

Voronova, S., Combating terrorism, EPRS, European Parliament, July 2016.

Wensink W., et al. The European Union's policies on counter-terrorism – Relevance, coherence and effectiveness, European Parliament, Directorate General for Internal Policies, January 2017.

Endnotes

[1] For a more extensive overview, see C. Dumbrava, European information systems in the area of justice and home affairs: An overview, EPRS, European Parliament, May 2017.

[2] P. De Hert and S. Gutwirth, 'Interoperability of Police Databases within the EU: An Accountable Political Choice?', *International Review of Law Computers and Technology*, 20(1-2), 2006, pp. 21-35.

[3] K. Huber, 'The European Parliament as an actor in EU border policies: its role, relations with other EU institutions, and impact', *European Security*, 24(3), 2014, pp. 420-437.

[4] M. Andrejevic, and K. Gates, 'Big Data Surveillance: Introduction', *Surveillance & Society* 12(2), 2014, pp. 185-196.

[5] E. Brouwer, 'Legal Boundaries and the Use of Migration Technology' in *Migration and the New Technological Borders of Europe*, eds H Dijstelbloem & A Meijer, 2011, pp. 134-169.

[6] D. Lyon *Surveillance as social sorting: Privacy, risk, and digital discrimination*, Routledge, London, 2013.

[7] M. König, 'The borders, they are a-changin'! The emergence of socio-digital borders in the EU'. *Internet Policy Review*, 5(1), March 2016.

Disclaimer and Copyright

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)