EU2019.FI

The New Information Architecture as a Driver for Efficiency and Effectiveness in Internal Security

16 October 2019
Tallinn, Estonia

ANNUAL CONFERENCE REPORT

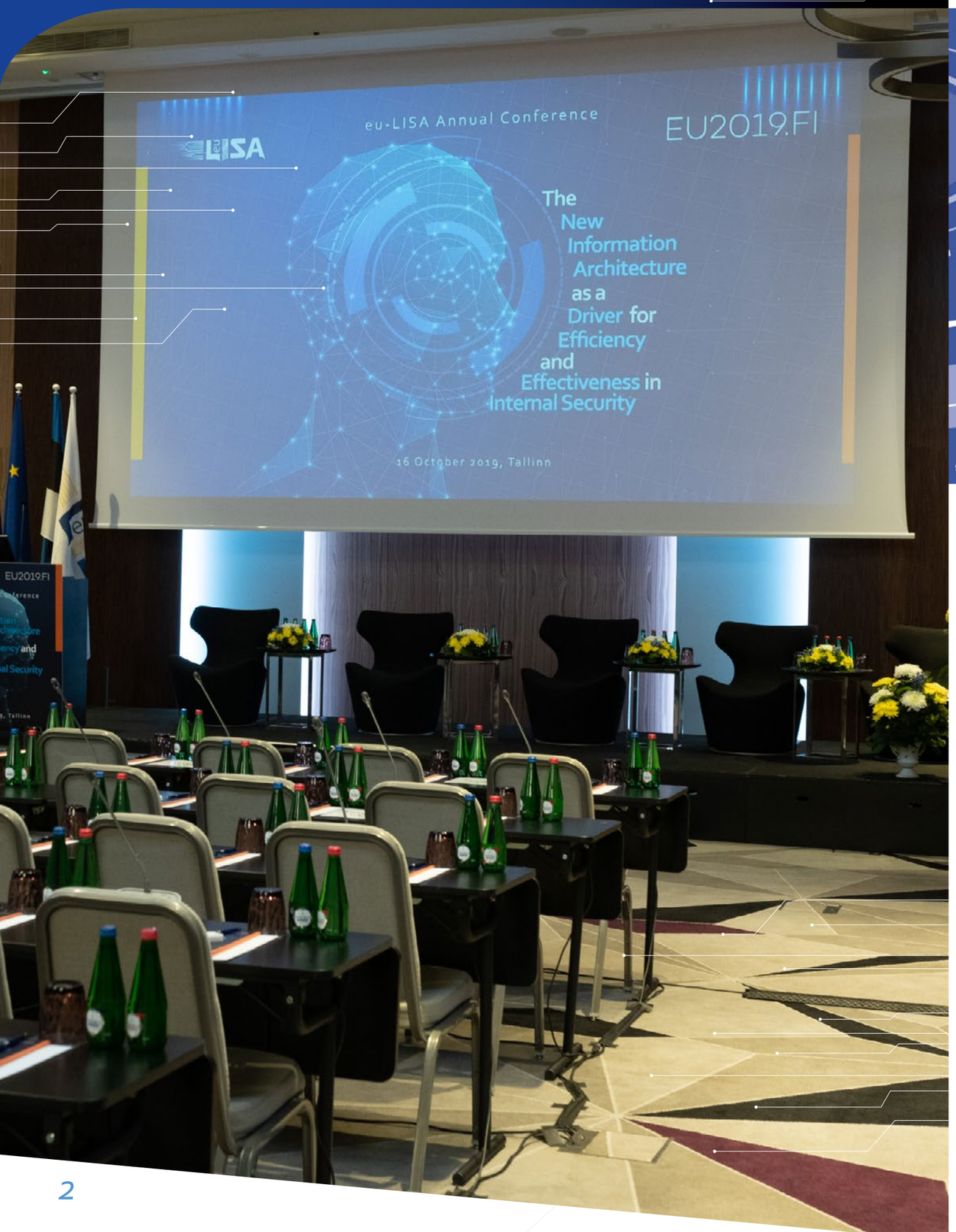
eulisaconference.eu
eulisa.europa.eu
eu2019.fi

Content

Printed in Estonia

This report is based on audio/video recordings and notes taken during the Conference. It does not purport to reproduce in extenso all debates and intervention. The opinions expressed are those of the speaker(s) only and should not be considered as representative of eu-LISA's official position.

ISBN 978-92-95217-57-7
doi:10.2857/477811
Catalogue number: EL-01-19-835-EN-N



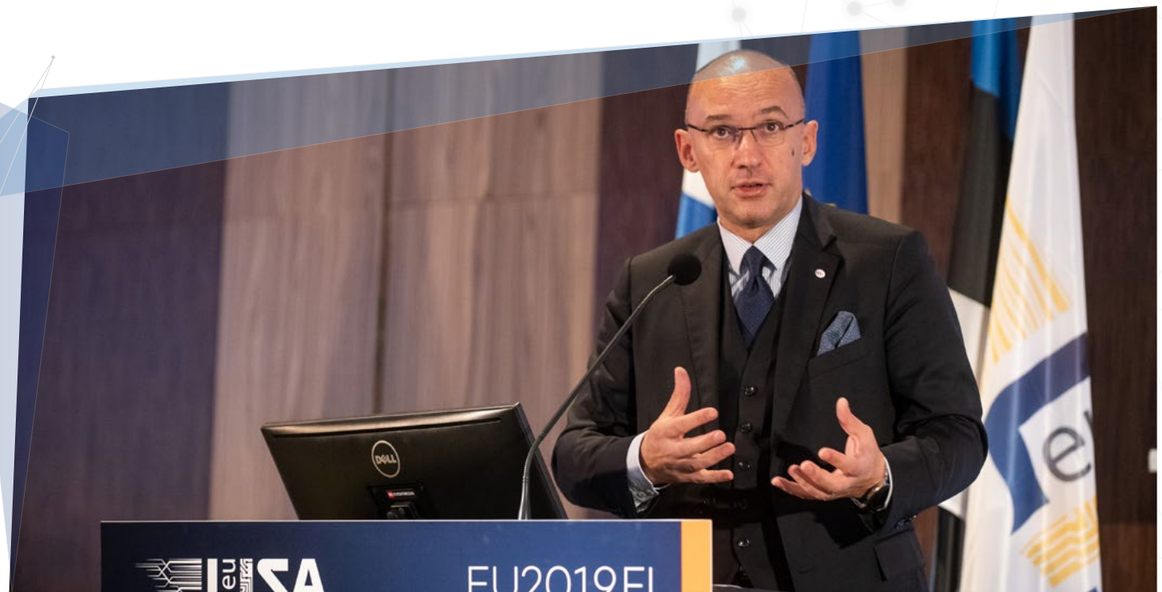
Keynote Addresses: Future of Internal Security Management in the Age of Digitalisation

EU2019.FI

Krum Garkov
Executive Director of eu-LISA

In his opening address, Mr Garkov welcomed the attendees in Tallinn as well as those participating online. He said that the conference was organised under the auspices of Finland's Presidency of the Council of the European Union. Seven years ago, eu-LISA was a relatively unknown but ambitious European public sector start-up. Since then, it has become a reliable partner with a solid structure and highly qualified staff. In recent years, eu-LISA has been a fundamental part of the Schengen architecture. However, the current environment poses additional challenges, such as terrorism and cross-border crime. eu-LISA needs to increase its contribution to the EU, but it must learn how to do more with limited resources. The answer to these challenges is to work harder and smarter, and therefore this year's conference is about changing mindsets to move towards smarter and more efficient operational work.

> ***"eu-LISA is a fundamental part of the Schengen architecture. Without the large-scale IT systems managed by eu-LISA the Schengen Area could not operate. The Agency is a reliable partner for Member States and the EU Institutions with a solid structure and highly qualified staff.***
>
> Krum Garkov,
> *eu-LISA*



Recent terrorist attacks and migration crises demonstrate a need to improve significantly information management and exchange in the EU, Mr Garkov said. Internal security, border management, and migration management are increasingly about data analysis, information exchange and risk assessment. Everything possible must be done to align the capabilities of IT systems and technologies with the needs of practitioners to prepare for future challenges. Mr Garkov identified four specific points. First, interoperability is a political commitment to ensure that services work together and complement each other to address concerns about internal security, migration, and border management. It is therefore time to bring down the silos and change the ways of cooperation. Second, there is a need for new information architecture. It is not so much about the quantity of data, but the quality of data analysis and deliverable insights. Third, there should be more cooperation concerning technical solutions, which must comply with standards and best practices. As a result, more has to be done in R&D to increase the strategic independence of the EU in internal security.

Interoperability is also a question of mindset. In addition to technical developments, close attention should be paid to capacity building and business practices. eu-LISA will remain a key partner in all those processes and stands ready for new challenges. In the future, the eu-LISA will continue to grow and develop in line with its new, extended mandate. Implementing interoperability is a collective exercise that requires the coordinated effort of eu-LISA, Member States, the EU, academia, and industry. Furthermore, it requires learning from the mistakes of the past. Mr Garkov concluded by affirming that there is a genuine opportunity to make Europe safer and stronger. He wished everyone a successful conference.

EU2019.FI

Ilkka Salmi

Permanent Secretary, Ministry of the Interior, Finland

Mr Salmi said it was his honour to represent Finland's Presidency of the Council of the European Union at the conference. He noted that Europe's security functions require interoperable information systems. Ensuring interoperability for internal security, criminal records, border management, and migration management has been a priority of the EU legislative programme in recent years. In May, the Council and European Parliament reached an agreement on establishing a framework for interoperability between EU information systems. The regulations entered into force in June, marking the start of a new critical phase in progress towards a Security Union. This new framework will contribute to border management and internal security in Europe.

> ***"To maintain internal security, Member States must have access to EU-wide information. The interoperability of systems will change the way data is provided to national authorities, which in turn requires close cooperation at EU level in information management.***
>
> Ilkka Salmi,
> *Ministry of the Interior, Finland*

To maintain internal security, Member States must have access to EU-wide information. The interoperability of systems will change the way data are provided to authorities, which in turn requires cooperation in information management. At the core of the EU's work on internal security is a common model for the use of all information. This information should be communicated to all stakeholders in the EU. He noted that interoperability enables smooth information exchange between law enforcement and border authorities, as well as supporting EU Agencies. Without uniform data, the EU will not be able to make full use of existing data or fully enjoy the benefits of biometrics.

Finland has a strong tradition of operational expertise in security. The country's aim is to put in place proactively high-quality border check systems and to serve as a model for inter-authority collaboration that should be integrated into the EU's model. While people are working to facilitate future digitalisation and the deployment of artificial intelligence (AI) across the EU, data interoperability regulations can only have an impact if they are implemented in an effective way. This calls for action by EU Member States, the European Commission and Agencies, such as eu-LISA. Implementation must be monitored at political and technical levels.

He suggested that extending interoperability and automation to data stored currently at national levels only should be explored. The financial framework poses a challenge, he noted. He concluded by stating that the future Entry-Exit System (EES) and the European Travel Information and Authorisation System (ETIAS) will put a strain on the Directorate-General for Migration and Home Affairs (DG HOME) and Member States. eu-LISA should be supported by all means necessary, Mr Salmi maintained. Therefore, the community needs to act in a coherent way, drawing from excellent levels of cooperation.

EU2019.FI

Matthias Oel

Director for Borders, Interoperability and Innovation, DG HOME, European Commission

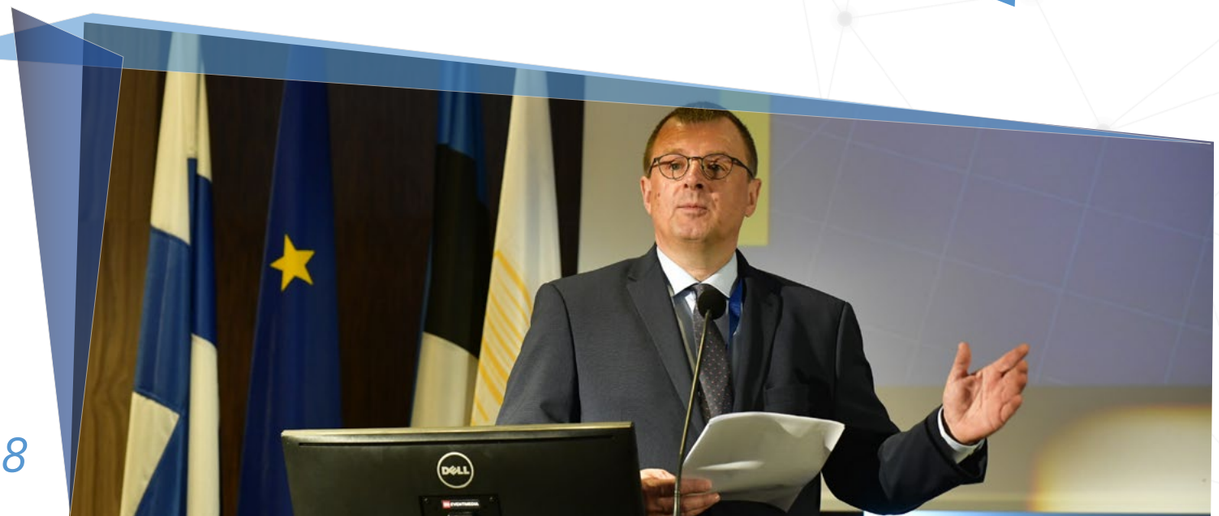
Mr Oel thanked eu-LISA for organising the conference and emphasised that it was important that the conference integrated the topics of information architecture and internal security with efficiency and effectiveness. The latter two are not always in the centre of the conversation, he said. He noted that the past few years have been difficult for the EU and the Schengen Area, citing the migration crisis as challenging for the cohesion of societies, internal security, but also for the stability of the Schengen Area and free movement of citizens. Efficient and effective border management is therefore key for the protection of the Schengen Area. eu-LISA is an intrinsic part of the Schengen architecture.

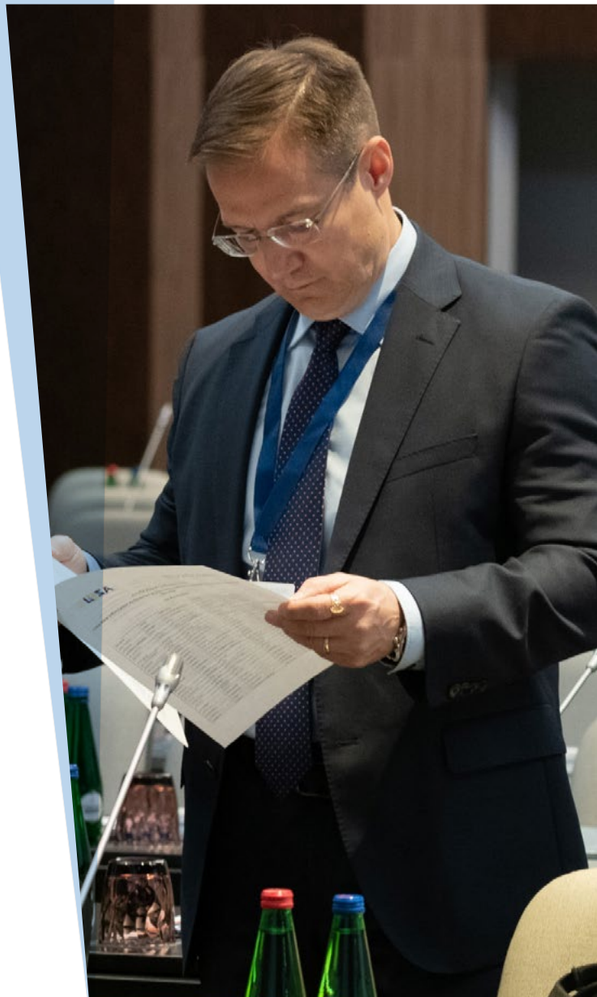
According to Mr Oel, the migration crisis calls for new solutions, as the number of third country nationals coming in and out continues to increase, at a time when the EU remains the issuer of the highest number of visas in the world. This puts stress on border controls and must be handled in a way that allows those who represent a threat to be identified. The EU is popular for settling for study, work, and family, so-called long-term regular migration. In addition, two-thirds of visitors are EU citizens leaving and entering the Schengen Area. The volume is a challenge for the authorities. People want the best of both worlds: fast border controls, yet increased security so that threats are kept out. The response, in his opinion, is to be smart, which means using information at hand to focus on relevant cases. There is a need to design and streamline processes and use technology to do this.

> *"Interoperability will ensure that end users have fast, controlled access to information, and that multiple identities linked to the same biometric data may be detected.*
>
> Matthias Oel,
> *European Commission*

While much has been accomplished to date, new systems and processes will change the concepts of managing borders and internal security in the next few years. There will be a major assembly of new complex IT systems, such as the EES, the enhancement of the Schengen Information System (SIS), and possibly Eurodac, as well as the interoperability infrastructure. Interoperability will ensure that end users have fast, controlled access to information, and that multiple identities linked to the same biometric data may be detected. It will also enable identity checks of third-country nationals by police authorities.

However, interoperability creates challenges for its implementation. We have entered an interoperability era where all stakeholders need to be aware of all systems, components, and processes. This puts stress on resources, requiring more support to complete the journey towards interoperability. The European Commission will on 15 November 2019 organise the 2nd Interoperability Forum to discuss the issue of implementation with Member States and Schengen-associated countries. This should raise awareness with regard to the financial needs and staff needed to support the implementation of the new information infrastructure. The Commission is fully aware of the challenges facing the community. Mr Oel concluded that now is the time to organise, explain projects to stakeholders, create steering committees, draft common plans, as well as contract resources from industry. Finally, in acknowledging the challenges ahead, he suggested that the future is promising.





EU2019.FI

Mart Helme

Minister of the Interior, Republic of Estonia

Minister Helme began his remarks by stating that the topics covered in the conference are of primary importance at the meetings of Ministers of Internal Affairs of the EU. The use of computers and information systems has brought along more changes than expected, he said. In Estonia and other countries, paper has become obsolete. Digitalisation has accelerated processes, but the government is faced with an enormous amount of data, fragmented and incomplete databases, that are often not connected. The migration crisis and terrorist attacks in Berlin and Paris required a large number of searches in databases and several inquiries to generate a complete picture, the Minister noted.

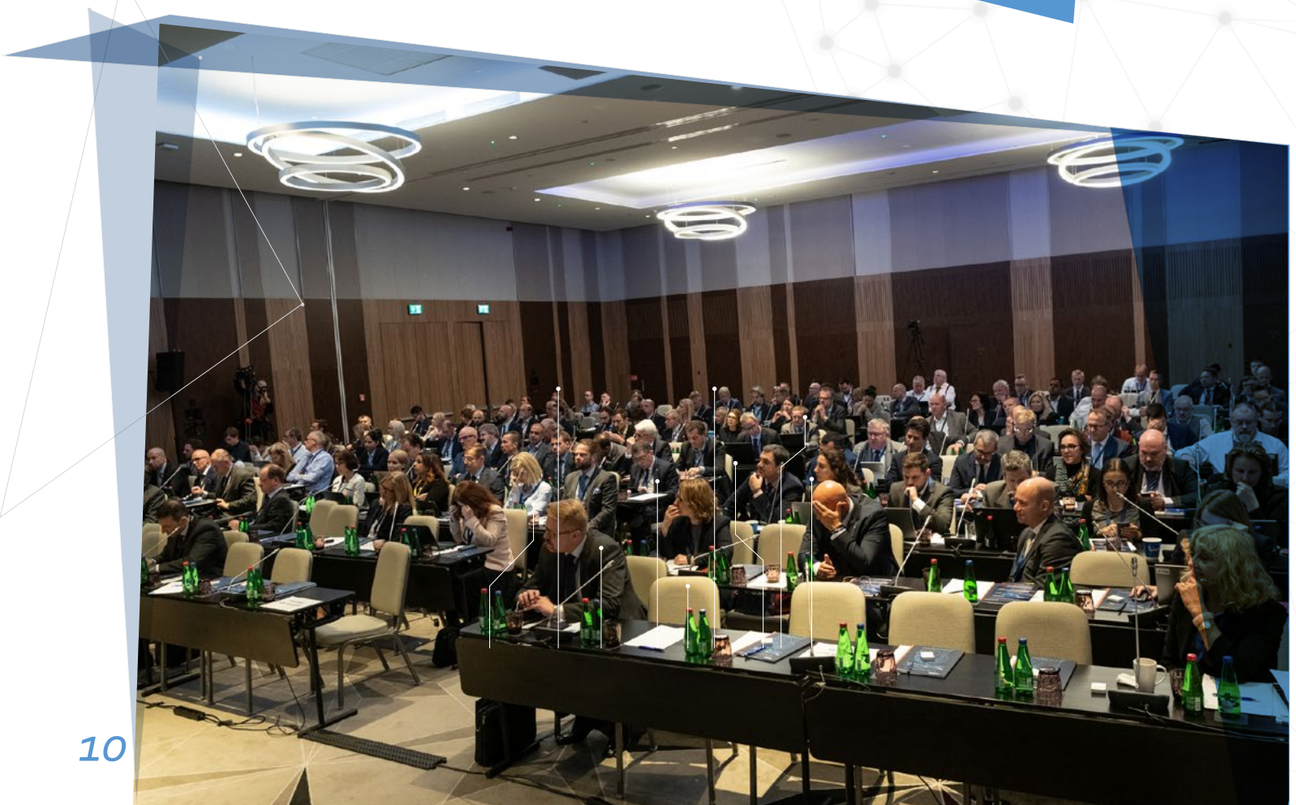
> ***"eu-LISA could take on the responsibility for testing and certifying equipment for internal security in the future.***
>
> Mart Helme,
> *Minister of the Interior, Republic of Estonia*

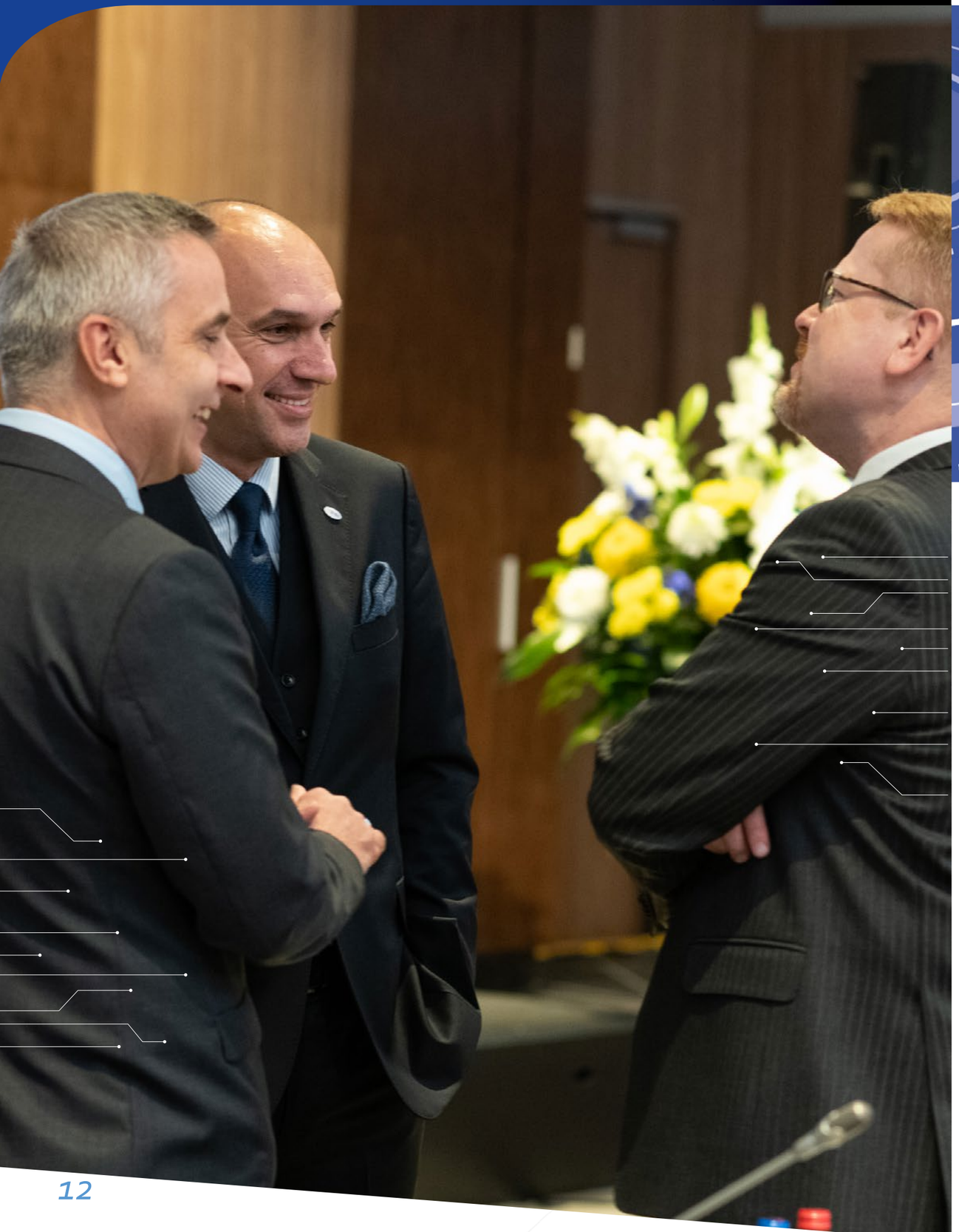
This also applies to the Schengen Area. At the moment, there is not enough information on people who enter the Schengen Area but never leave. The EU, in his opinion, needs joint solutions to tackle these problems. In recent years, significant steps have been taken although today's preparation is mostly IT-based, and focused on establishing information systems and mutual communication. Not only do eu-LISA and the Commission bear the responsibility for carrying out these changes, but this also falls to EU Member States, the Minister added. In addition, the implementation of new systems creates challenges.

The future EES will change the work of border guards. Hundreds of border guard officers and police will need training. With the cooperation of eu-LISA, training sessions are already being planned. Another challenge is the provisional integration of databases that are divided into silos. There is still a lack of overview of false data in different information systems. For instance, the Berlin attacker possessed 14 identities in the system. The Minister said authorities should not be surprised by similar cases in the future. With regard to the implementation of the EES, several Member States are conducting tenders for biometric capture and check.

The Minister expressed concern over the equipment's compliance with legal requirements and suggested establishing European standards in the field of internal security. He closed with the suggestion that eu-LISA could take on the responsibility for testing and certifying equipment for internal security in the future.

He wished eu-LISA much strength in its implementation of new solutions and new technology in the field of internal security.





Session 1

Impact of the New Information Architecture on Internal Security: Efficiency Gains and Challenges

Moderator:
***Anssi Kangas**, Chief Superintendent, Finnish National Police Board*

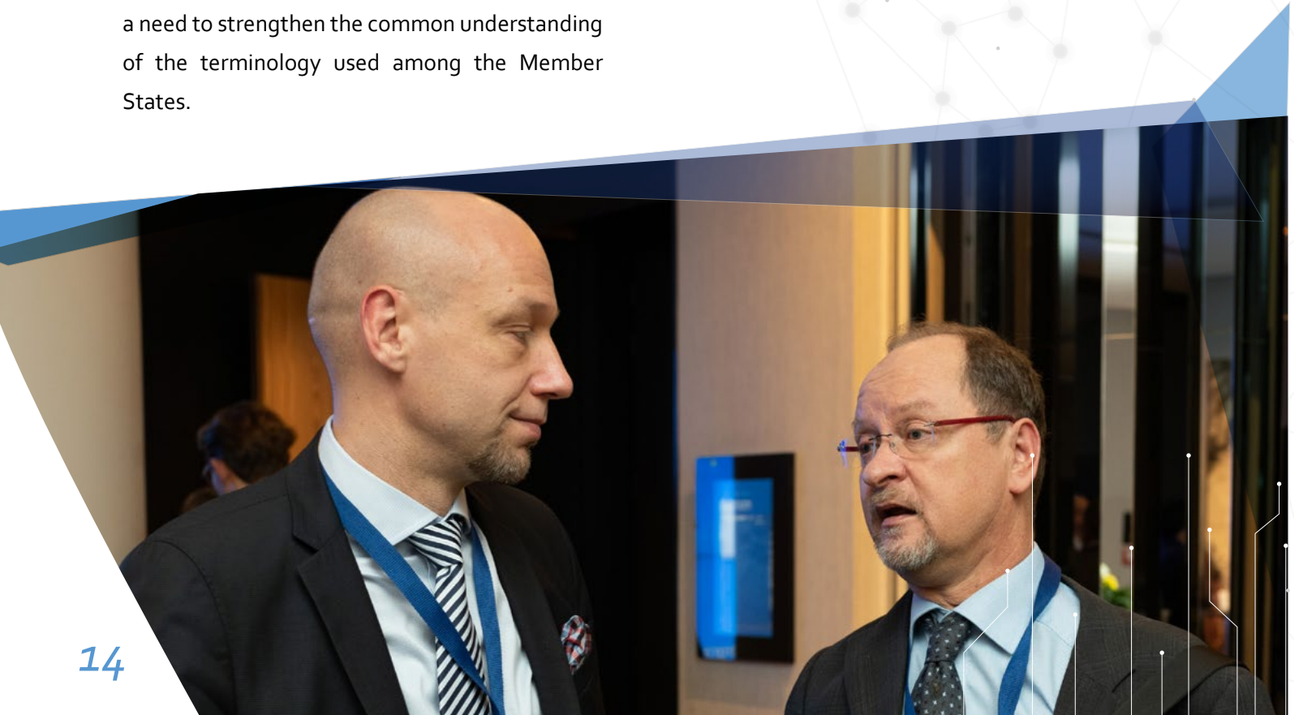
Panellists:
***Richard Rinkens**, Policy Analyst, Coordinator for Biometrics and Identity Management, Directorate-General for Migration and Home Affairs, European Commission*
***Ana Maria Ruginis Andrei**, Head of Architecture Sector, eu-LISA*
***Holger Farnung**, Deputy Special Representative of INTERPOL to the European Union*

Mr Kangas opened the session on the ongoing implementation of interoperability architecture as described in EU regulations. He introduced the panel and started the discussion with a future point of view, covering what was presented in Council meetings during Finland's Presidency of the Council of the European Union. In terms of automation and interoperability, he said there is a need to strengthen the common understanding of the terminology used among the Member States.

> ***"With the interoperability of the EU systems at hand, the next step may be the renewal of the Prüm regime.***
>
> Anssi Kangas,
> *Finnish National Police Board*

The guiding concept in Finland is the point of view of the law enforcement end user, for whom processes should be kept as simple as possible. This means that the end user should not need to make multiple queries on the same search attributes. During its Presidency, Finland has sought to define information exchange and information management – both operational and strategic. Decentralised large-scale information systems are being made interoperable.

For the discussion, he defined automation as a management concept, an approach by which procedures are performed with minimal human interference. With the interoperability of the EU systems at hand, the next step may be the renewal of the Prüm regime, he believed. This would be a step towards the automation of decentralised national data. One could therefore envisage the possibility of making simultaneous queries of fingerprints to large-scale databases and databases of Member States in the future. Despite some pilot projects however, a significant part of law enforcement data is far removed from automation at the moment, and is only available to law enforcement by the traditional query-response method.



Five countries are piloting a project on developing and testing the capability to make automated queries to each other's databases. There is a similar situation with the Passenger Name Record (PNR) data, and an analogous technical solution is envisaged where one could search other databases on a hit- or no-hit basis. Mr Kangas concluded by stating that automated information exchange between Member States involves resolving certain legal issues and making political decisions. Therefore, although the implementation of an interoperability regime is underway, future needs require further discussion.

Mr Rinkens thanked Mr Kangas and eu-LISA. He launched his presentation with the subtitle, "How to find your socks" and discussed the idea of being disorganised at home. He raised the example of Marie Kondo, a Japanese organising consultant, whose key concept is to put items that have the same or similar purpose together. Over the years, Mr Rinkens said we have put our things all over the place. Yet, now we have empowered eu-LISA to put our fingerprints and facial images in one place. If they are there, we will be 100 percent certain of where we can find them. A Common Identity Repository (CIR) will harmonise that.

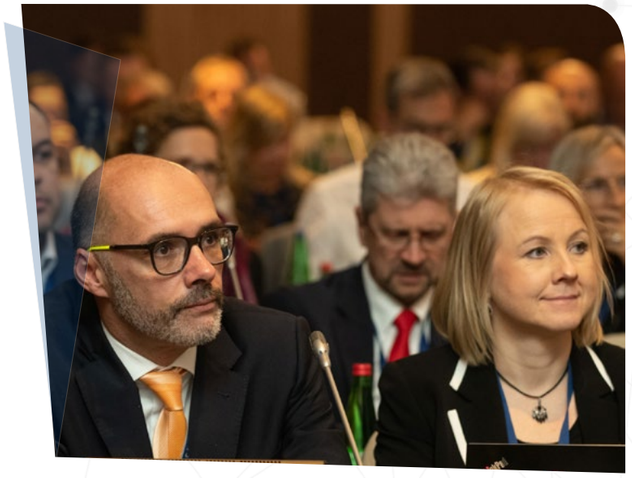
Unfortunately, there are some "adolescents who are not playing the game" in this tidy new house. There are lots of metaphorical "glasses and keys" in Europol, INTERPOL, and especially in SIS, which is why the common European Search Portal (ESP) was created, to be able to search within all these systems. Mr Rinkens discussed some of the new features. A new Multiple Identity Detector (MID) will look at information from multiple sources and tell you if the person in question is who he or she claims to be. This will be a game-changer in

EU2019.FI

Europe if it is implemented correctly, although it brings inevitable challenges too.

Information in SIS has to be made available to a wide range of authorities in the Member States, e.g. law enforcement, judicial, consular, border guards, immigration and asylum authorities. All of those entities have until recently been working in silos and they all speak different languages, creating complex situations. Therefore, changes are needed not only in IT, but also in management and in communications. At the end of his presentation, Mr Rinkens showed a map of border control posts where the EES will be implemented and active, which, with police stations in Europe, courts, and consulates across the world, should support the creation of what he called an amazing network.

> *"We have empowered eu-LISA to put the fingerprints and facial images collected according to the relevant EU regulations in one place. If they are there, we will be 100 percent certain of where we can find them.*
>
> Richard Rinkens,
> *European Commission*



Ms Ruginis Andrei began by asking why do we need an interoperability architecture. While for some it is a clear solution when thinking about filling in the existing gaps, the fact is that access to meaningful identity and decision-making information is still scarce and tedious. She added that authorities have made progress since the terrorist attacks in Paris, Brussels and Berlin in recent years. In deciding to overcome their reluctance to work together, EU countries have improved their tracking of non-national terrorist fighters, she said. The authorities have been gradually moving towards a more positive era, an era of change and an era of data synchronisation. For Justice and Home Affairs (JHA), the key words have been availability and sharing. This includes the sharing of data among police, border guards, as well as visa, asylum and judicial authorities. All these will enable more effective screening of travel documents, more success in fighting identity fraud and in identifying terrorist offenders.

In this respect, eu-LISA is committed to working towards building trust and awareness via events and training. Together with the Commission, Member States, EU agencies, and industry, the Agency is striving to give meaningful terms to the new updated rules for data access in order for this to become today's reality. Every piece of the interoperability architecture is being carefully thought out, discussed, and assembled in order to forge the perfect engine to successfully fight against the threats to internal security, to effectively control migration and to overcome blind spots regarding identity management. This is being accomplished by deploying components in a controlled, gradual way, by introducing new and reusing existing technology, by strengthening and streamlining the data security and data protection conditions that govern the respective systems, while at the same time improving and harmonising their data quality requirements. This has started with the EES, the first interoperable system linked to VIS that by its Biometric Matching System (BMS) lays the first stone in the building of the future shared Biometric Matching Service (sBMS). There is also continued work on boosting the interoperability of ETIAS, paving the way for fast, seamless and controlled simultaneous queries to multiple systems, by introducing the European Search Portal (ESP).

> *"Every piece of the interoperability architecture is being carefully thought out, discussed, and assembled in order to forge the perfect engine to successfully fight against the threats to internal security, to effectively control migration and to overcome blind spots regarding identity management.*
>
> Ana Maria Ruginis Andrei,
> *eu-LISA*

EU2019.FI

Ms Ruginis Andrei said that the Agency is also working on establishing automated data quality control mechanisms and common data quality indicators for use with the Central Repository for Reporting and Statistics (CRRS). This will generate cross-system anonymised statistical data and analytical reporting for policy, operational and data quality purposes in accordance with the applicable legal instruments. A Multiple Identity Detector (MID) will also be developed with the aim of checking whether the queried identity data exist in more than one of the systems connected to it, enabling the detection of multiple identities linked to the same set of biometric data, and ensuring the correct identification or detection of fraud. In parallel, SIS has been enhanced with some new functionalities. Ms Ruginis Andrei explained that gradually the rest of the systems will be connected to the European Search Portal and data will be migrated to sBMS and CIR. The fulfilment of all of these objectives and building the systems with effective technological solutions is only feasible with the constructive collaboration of all relevant stakeholders.

> ***"There is a need to work on an Interpol-EU agreement to enable data exchange between Interpol and the EU in the framework of the interoperability and ETIAS regulations.***
>
> Holger Farnung,
> *INTERPOL*

Mr Farnung began by addressing the added value for Member States from the SLTD (Stolen and Lost Travel Documents) and TDAWN (the Interpol Travel Documents Associated with Notices database) databases. INTERPOL currently maintains 18 databases and has 194 member countries, 172 of which have already extended their NCB I-24/7 system, which is interoperable with the MIDAS and PISCES systems, he said. INTERPOL has 87 million records in its databases, 4.5 billion SLTD searches are carried out every year and close to one billion searches are carried out in TDAWN. Altogether, there are about 1.4 million hits on both databases worldwide. Mr Farnung mentioned the new EU legislation that includes the 2014 Council Conclusions on strengthening the use of SLTD in operations, a new Schengen Borders Code on checks against SLTD and SIS in place since 2017, and a Council Decision on API/PNR from 2015.

However, security gaps and challenges still exist with these new regulations as those focus only on silent hits. This poses a problem for INTERPOL as rules are based on reciprocity, creating a need to check hits with data owners. Therefore, there is a need to work on an INTERPOL-EU agreement, because there cannot be data exchange data without such an agreement. Both INTERPOL's General Assembly and the European Commission should enter into negotiations. However, to resolve the silent-hit basis will also require rules

and processes within INTERPOL to change, which is not simple, as any changes to rules and processes require a two-thirds majority of the General Assembly. Another possibility that can be considered is for INTERPOL to interpret its rules in a different way. It is also possible to use opt-out systems, Mr Farnung suggested. He concluded by stating that, from INTERPOL's perspective, it would be a huge gap for the ETIAS system not to be able to use its systems.

Following the panel discussion, ***Mr Kangas*** opened the floor for questions and comments from the audience.

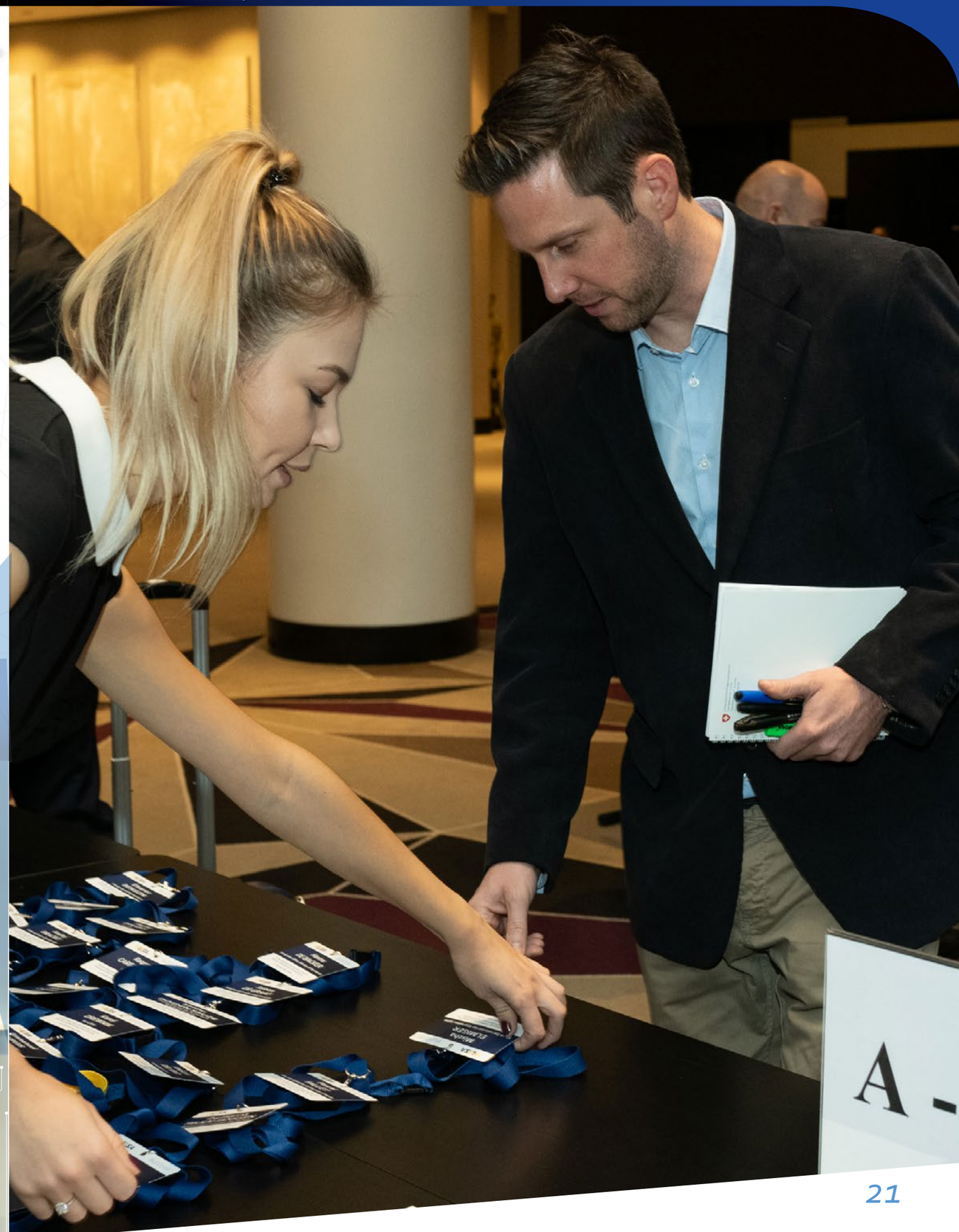
Several questions were raised. First, there was a question about opening up the SLTD database for commercial entities processing passport information, such as airlines or visa service providers. ***Mr Farnung*** responded that access to SLTD has been provided to certain entities, such as cruise ship companies under special agreements. A follow-up question, about other potential use cases for such data and the possibility for citizens to access it, was then addressed to the panel. ***Mr Rinkens*** responded that where identity management is concerned, the involvement of other entities not directly related to identity management is not foreseen any time soon. However, Mr Rinkens suggested that ETIAS will be the first system to allow citizens to check their own data and explore some of the information in the future. Discussion with the audience continued with a question regarding the future of biographic data in the new architecture. In response to the query, Mr Rinkens noted that Eurodac will only be part of CIR if it carries biographical details. Discussions on this are currently ongoing, however, Mr Rinkens stated that biographical data will be there. He further suggested that the capturing and matching of fingerprints and facial images should be fixed to a certain biographic identity, which will then be used in connection with biometric data.

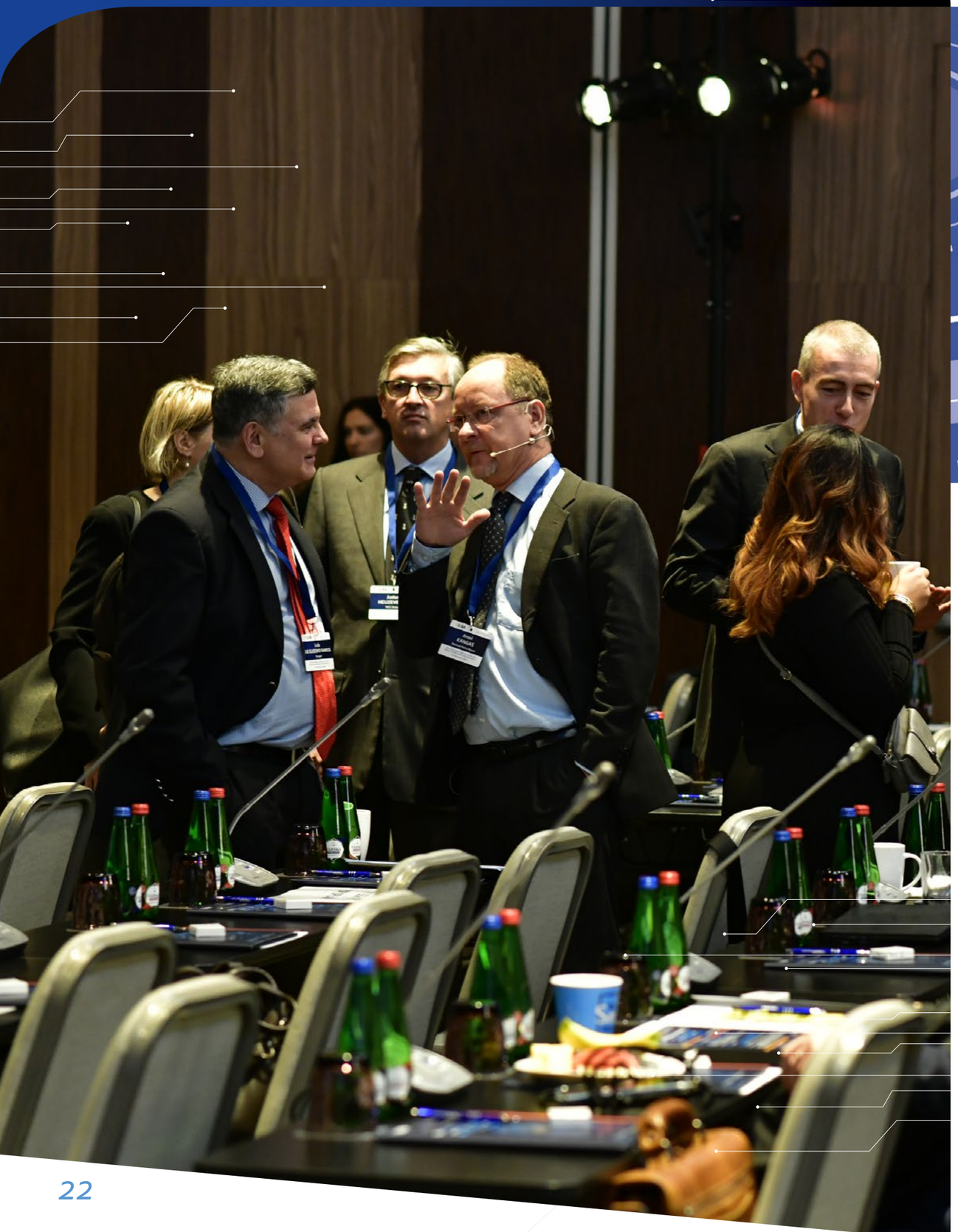
Ms Felkai Janssen emphasised the importance of putting a strict identity management system in place to ensure consistency in the process.

In particular, she stressed the importance of identifying the entity in charge of system management. There was a question on decentralised identity access management and consent-based controls during the discussion. ***Ms Ruginis Andrei*** responded that this type of access is not foreseen in the current legislation but could be further elaborated and discussed if in the future it is legally possible. Although eu-LISA is currently not exploring decentralised identity management, it monitors technological developments and is open to technological solutions that are mature and ready for implementation at scale.

One participant expressed his concern regarding the ability of eu-LISA to achieve interoperability in the short term.

Mr Rinkens responded by stating that although it is challenging and will require significant effort in change management, it is possible, but can take longer than currently projected. The final question addressed to the panel from the audience, concerned storage of the same data across different databases and whether the European Commission envisages any changes in the architecture to address this issue. Two points were offered in response to this query by ***Mr Rinkens***. First, although it is indeed a good objective to aim for, some of the data could be difficult to import into the system e.g. INTERPOL data. Hence, centralisation is perhaps not the best approach to follow, rather searching across decentralised systems would be the best approach. Mr Farnung added that INTERPOL already contributes to the European databases, in particular with data on foreign fighters. There are 50 000 foreign fighters from the US who are in the database, he said.





Session 2

Effects of Digitalisation on the Collection and Processing of Data for Law Enforcement Purposes

Moderator:
***Guido Brockmann**, Head of Product Management Sector, eu-LISA*

Panellists:
***Patrick Padding**, Core Group leader of ENLETS, The National Police of the Netherlands*
***Luis de Eusebio Ramos**, Deputy Executive Director of Europol*
***Ave Poom**, Senior Policy Officer, Executive Support and Stakeholder Relations Unit, eu-LISA*
***Georg Biekötter**, Political Administrator, General Secretariat of the Council of the European Union*

The moderator, ***Mr Brockmann,*** introduced the panel and posed the question: What is digitalisation? He defined it as the act of getting the right information at the right time to the right person with the goal of furthering the agency's mission. Technology enables different law enforcement agencies to communicate in real time, which is especially important given the lack of internal borders in Europe, he suggested. Criminal cases easily cross jurisdictions, hence digitalisation can have transformative effects. The law enforcement community has traditionally relied on the availability of accurate information, more and more of which has come from large-scale IT systems. Yet all these systems have been developed for specific purposes, he said, and we cannot think in terms of silos anymore. Mr Brockmann advocated for secure collaboration, driving the need for better communication between departments and agencies, and effectively bridging the silos. Collaboration tools for judicial processes are also needed. He noted that the MID, part of the interoperability architecture in the JHA domain, is a good example of this. In the law enforcement domain, Mr Brockmann noted, the right information is needed at the right time and place, and sometimes a person's life can depend on it. He said that law enforcement is still dependent on "old school methods" and often relies on a second-line support at the station as well as manual intelligence and paper-based files. This is not efficient. Police authorities have started digitalisation at individual levels and most use smartphones to take photos from crime sites and send messages. However, the equipment being used is mostly private, raising concerns about the security of the data being exchanged.

> ***"Technology enables different law enforcement agencies to communicate in real time, which is especially important given the lifting of internal borders in Europe.***
>
> Guido Brockmann,
> *eu-LISA*

Law enforcement authorities are becoming more technologically adept, but this requires new processes, procedures and information systems. There is also an abundance of data that needs to be managed. Concluding his remarks, Mr Brockmann noted that eu-LISA can support law enforcement authorities in tackling these challenges by developing standards, such as the Universal Message Format (UMF) for data exchange between systems and agencies.

Mr Padding introduced himself and the European Network of Law Enforcement Technology Services (ENLETS). He pointed out that ENLETS connects 29 Member States that share best practices, including laws, tools, education and culture. When looking at the next stage of technology, ENLETS engages in co-creation processes with research and technology organisations, universities, and SMEs, in particular focusing on identifying the opportunities for improving its work. Mr Padding presented two use cases in his talk. The first was an organised gang killing. In this case, 45 people were arrested, and significant amounts of data were collected from eavesdropping, GPS, IP and Wi-Fi data. This raises questions about how to manage data effectively and automate the processes. Currently, such data will be given to a digital forensics expert, who will extract the data and return it as a paper report to an analyst and a case investigator. Most investigations are still paper-based, although some digital tools, such as Microsoft Excel, are often used to facilitate investigations. However, ENLETS is evaluating options for automating some processes. Within the new expanded mandate of eu-LISA, more must be done to strengthen capacity and make data interoperable. The second case concerned terrorist attacks. Mr Padding referred to the attacker at the Berlin Christmas market who was pursued and killed in Italy. In that case, crime scene images, such as a car fleeing the scene, needed to be distributed and shared quickly. Direct European mobile access is needed, to have data in place at any time in any place. Data collected from a crime scene has to be disseminated via an operational centre. Currently, however, there is no direct data exchange at European level, which needs to be changed. Concluding his presentation, Mr Padding mentioned that ENLETS is working on

> ***"ENLETS connects 29 Member States that share best practices in the fields of legislation, technical tools, education and culture.***
>
> Patrick Padding,
> *ENLETS*

EU2019.FI

a project called Quick Response for Operational Centres with the aim of addressing some of the challenges described above.

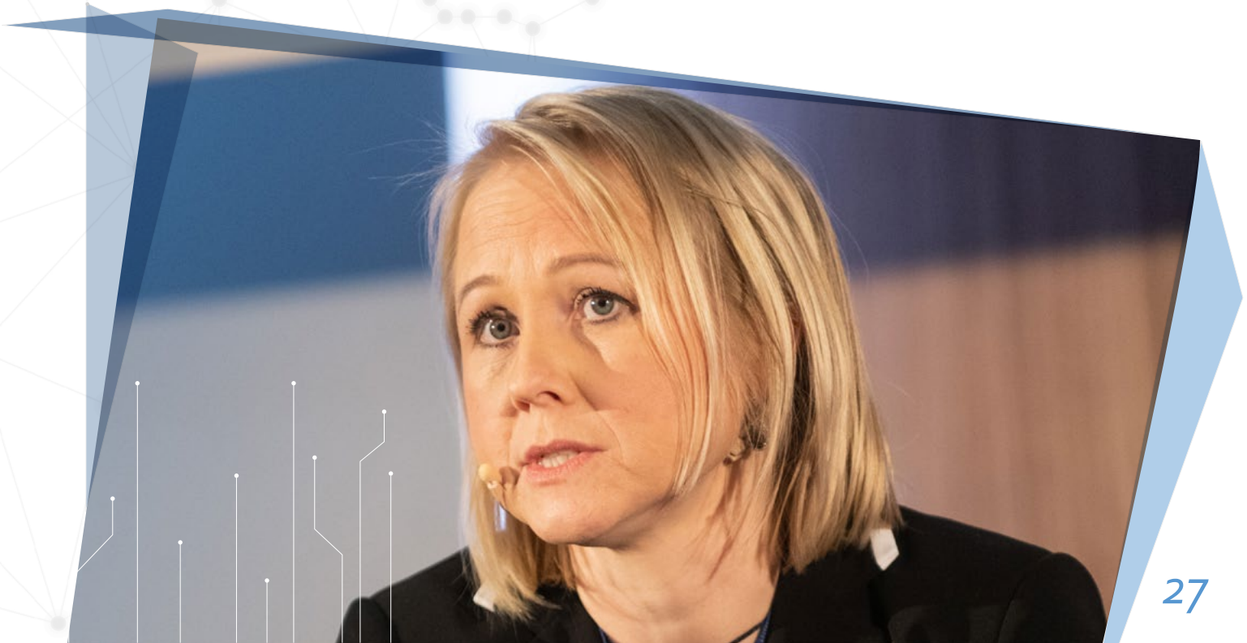
Mr Brockmann introduced the next panellist, Mr de Eusebio Ramos, noting that Mr de Eusebio Ramos had played an important role in the digital transformation of the Spanish police force.

Mr de Eusebio Ramos began his presentation by outlining the main aim of Europol, which is to act as Europe's information hub for law enforcement authorities. Europol seeks to transform data into information and generate intelligence and knowledge based on this data. He continued by stating that Europol is under pressure due to increasing amounts of data – text, audio, and images. It is a challenge for Europol to handle this information and to provide intelligence in a timely manner. In 2016, Europol put forth a new plan to manage its data by using artificial intelligence. A pilot project was proposed based on facial recognition. The pilot was successful, and paves a path for further implementation in the agency. Forensic tools have since been developed, such as

> ***"Europol seeks to transform data into information and to generate intelligence and knowledge based on this data.***
>
> Luis de Eusebio Ramos, *Europol*

a tool for removing links from the internet linked to terrorism. Europol has also started a project with the Joint Research Centre of the Commission that will commence in 2020. This project aims to develop a secure way of communication between law enforcement officers. Mr de Eusebio Ramos noted that Europol has developed the QUEST interface to facilitate the access of different law enforcement parties to all of its databases. He concluded with three takeaways. First, there needs to be a mindset focused on change. Second, he noted that more non-IT specialists are using IT tools than ever before. Last but certainly not least, there needs to be an openness to change in IT.

Ms Poom in her presentation focused on eu-LISA's perspective on law enforcement digitalisation, touching on its own projects, spillover into other domains, and the challenges of digitalisation. Digitalisation, she added, generally improves data collection, exchange, data quality, and analytics. It increases cost-effectiveness, scalability, and can support automation. eu-LISA works on a regular basis with the European Commission and the Joint Research Centre, several JHA agencies, and vendors in the IT sector. It has also started to enhance cooperation with academia, think tanks, as well as with ENLETS. In terms of projects, the finalisation of the SIS Automated Fingerprint Identification System (AFIS) should happen by the end of 2021. SIS AFIS as a new digital tool will include fingerprints, latent prints, and palm prints, making those available for search by Member States. Access to SIS will be extended, providing for the first time access to SIS to the European Border and Coast Guard Agency (Frontex), as well as extending access to SIS articles for Europol and Eurojust. She referred to eu-LISA's work on developing the EES and ETIAS, which through digital means will enhance the fight against crime and terrorism and help reduce the misuse of identities. The largest digital project that is currently being carried out by eu-LISA is interoperability. When implemented, interoperability will benefit national authorities with different components: the European Search Portal, the Common Identity Repository, the Multiple Identity Detector, and the shared Biometric Matching Service. An additional benefit, Ms Poom suggested, is the Central Repository for Reporting and Statistics (CRRS), which will help to analyse data in the system. For the first time, eu-LISA will also offer transversal services to Member States instead of a silo approach. The Agency is also working with the European Commission and the Member States, to analyse the Prüm information exchange mechanism, and to see how this can be potentially made more interoperable. With the successful completion of these initiatives, there can be positive spillover effects into other domains, such as the ICT sector and European societies and economies overall. Ms Poom added that there are human and financial resource challenges to engaging in digitalisation processes. In conclusion, Ms Poom noted that at every step, both the Member States and the Commission and other EU bodies need to ask what is the main goal of digitalisation and whether the investment pays off compared to



benefits received. This needs to be cooperatively analysed and decided on a case-by-case basis.

> *"The ongoing digitalisation initiatives in the Justice and Home Affairs domain can bring positive spillover effects into other domains, such as the ICT sector, the academia, and European societies and economies overall.*
>
> Ave Poom,
> *eu-LISA*

Mr Biekötter began by discussing his work on digitalisation at the General Secretariat of the Council of the EU. Data protection creates highly ideological debates in Europe. Data protection works in liberal democracies, where there is a separation of powers, rule of law, an independent judiciary, and political freedoms. Liberal constitutions tend to limit the authority of government. The General Secretariat has had discussions on interoperability since 2010. He provided an overview of the information landscape, focusing on police officers who need to solve cases. When working on cases, they first query national databases; then they search European databases, such as SIS, the Prüm data exchange on biometrics, as well as other channels. The idea of the Commission, however, has been to make single-click search across databases possible. The technical feasibility of this proposal is a challenge to be addressed by eu-LISA. When processing data, law enforcement must take into account the protection of natural persons. These requirements were a part of best practices until Directive (EU) 2016/680, the Police Directive, which set out principles for assessing personal data. Data quality is also important. According to Mr Biekötter, individuals have the right not to be subjected to decisions when based on automated processing under the directive, and this has an adverse legal effect. Automated decision-making is always ambiguous, he noted, and in the end, a human always makes the decision, not the machine. Some people, he noted, have argued that what is gained in automated data processing is lost when one has to comply with the relevant data protection requirements. Police officers have complained that accountability measures cost too much in terms of resources. Still, he believes that the EU will export its models for automated data exchange and interoperability worldwide. He added that when algorithms are developed, one should take note of data protection by design and by default. As a final point, he noted that automated profiling is highly dependent on clean and high quality data and reliant on a human in the end, in line with the applicable regulations.

Mr Brockmann followed up with a question to the panellists about new technologies and policy, the collection of digital data in an investigation, the automation of change and processes, and how that would translate into a challenge for cross-border law enforcement information exchange.

In response to this question, ***Mr Padding*** said that if consistent data exchange across borders exists, and data are collected legally, in a transparent chain of custody, the data will end up in the database, where there are data protection rules on data exchange. At the moment, though, direct cross-border data exchange, such as is necessary in the case of a terrorist attack, can be difficult, he added. Once there is a relevant photograph or name, investigators will want to transfer it across borders. This might be a violation of data protection requirements. It would be good to hand data over to other Member States, but there should be assurance that the data will be removed after the incident and the investigation has been closed, he said. ***Mr Biekötter*** responded to the question by saying that if agencies comply with data protection law, then data exchange is not a real problem. Requirements for data protection should be complied with at all times, he said. ***Mr Padding*** suggested that there could be a standard approach for handling such

> *"Automated decision-making is always ambiguous, and in the end, a human always needs to make the decision, not the machine.*
>
> Georg Biekötter,
> *General Secretariat of the Council of the European Union*

situations, with boundary conditions in place, taking into consideration the legal specifics of the Member States. ***Mr Biekötter*** added that another relevant aspect is data quality. In PNR, there is a lot of data, however, the data are not as clean as law enforcement data, he noted. If you start investigations based on unclear data, it is a risk. eu-LISA is working on data quality, he added.

Addressing Mr de Eusebio Ramos, ***Mr Brockmann*** asked how the law enforcement agency looks when it has been through the process of digitalisation. Mr de Eusebio Ramos suggested that the best example of the positive effects of digital transformation is the ability of the agency to provide to relevant stakeholders the right information at the right time, in the right place and to the right person. Simply put, the idea is to allow all police officers and investigators to have access to the information that they need for investigating cases. This also allows internal operational processes to be transformed into data-driven processes.

Mr Brockmann continued the panel discussion by asking ***Ms Poom*** to provide more examples of the

spillover effects mentioned in her presentation. Ms Poom replied by stating that based on her studies of European integration, spillover is a trigger from one domain to another. First, there are clear economic benefits from the expenditure of millions of euros in the development of new IT systems. In addition to the economic spillovers, there are technical spillover effects, such as the harmonisation of information exchange standards and biometric standards, for example, which may lead to greater efficiency and effectiveness, she concluded.

Mr Brockmann opened the floor to questions from the audience.

The discussion with the audience started with a question on the management of latent fingerprint data, namely whether it will be managed centrally or on the MS level? In response to this question, ***Ms Poom*** suggested that eu-LISA does not own the data that is stored in the systems and fully relies on the MS in this regard. ***Mr Brockmann*** added that in the future it will be possible to store latent fingerprint data and alerts on unknown subjects in SIS. The discussion continued with a question on how industry can collect personal data without being exposed to the provisions of the General Data Protection Regulation (GDPR). In response to the query, ***Mr Biekötter*** said that eu-LISA is dealing with the issue and it is addressed in the terms of contract with the respective entity. ***Mr Brockmann*** added that only Agency staff has access to production data, whereas contractors do not. The final question from the audience focused on the position of the Europol QUEST system in the new architecture, in particular in relation to the new systems developed by eu-LISA and the European Search Portal. ***Mr de Eusebio Ramos*** responded that QUEST is an interface which enables users to query information from multiple databases at Europol, and therefore enables interoperability.

Session 3

How Will the New Information Architecture Support Border and Migration Management?

Moderator:
Theofanis Syrigos, *Chairperson of the EES-ETIAS AG, Head of Business Relations Management Sector, eu-LISA*

Panellists:
Nina Gregori, *Executive Director of EASO*
Dirk Vande Ryse, *Director of the Situational Awareness and Monitoring Division, Frontex*
James E. McLaughlin IV, *Executive Director, Targeting and Analysis Systems Program Directorate, U.S. Customs and Border Protection*
Jesse Seppälä, *Senior Policy Officer, Border and Coast Guard Department, Finnish Ministry of the Interior*

EU2019.FI

Mr Syrigos introduced the panel, stating that the new EU information architecture will redesign the whole concept of border and migration management. These new systems will make a difference by providing a modern approach to different business areas, borders, immigration, law enforcement, and consulates, he maintained. This raises questions about point-of-migration management and requires input from asylum authorities on the subject. Other pertinent questions to be addressed concern the CRRS, how to analyse risks and vulnerabilities, and how to benefit from the different challenges faced. Another important question is how to best understand information from both EU and non-EU entities?

What is the impact on the national level, and what do Member States and involved agencies have to do? Mr Syrigos concluded his introductory remarks by asking whether government coordination is still an issue and what do we have to focus on in this respect?

Ms Gregori began her intervention by discussing the activities of the European Asylum Support Office (EASO). Its mandate is to support Member States in the implementation of a Common European Asylum System. The implementation is based on four pillars: training; asylum support and practical implementation of the European asylum system; operational support with frontline states including Italy, Greece, Cyprus, and Malta; and information analysis and knowledge development. EASO has developed a common country-of-origin information guidance, information, and communication system, as well as a data hub, and provides strategic analysis,

research, and forecasting. She continued by stating that based on its data, the number of asylum applications is exceeding the number of irregular border crossings in recent years. Pending asylum cases in the meantime have hardly reduced since the migration crisis of 2015-16. The focus of discussion has often been on border management or security aspects, Ms Gregori noted, however, that there has not been much room for a discussion of asylum and the importance of interoperability in this context. According to Ms Gregori, EASO believes that large-scale IT systems and interoperability should lead to improvements in efficiency as well as effectiveness of the relevant processes. In terms of IT systems in the JHA domain, improved VIS and Eurodac systems will provide authorities with more and better information. These developments may eventually lead to better-informed decisions, and could be used by the Member States in processing asylum applications. There are also important advantages in bridging the asylum and the new EES. However, this cannot replace the examination of individual asylum requests. Concluding her remarks, Ms Gregori noted that asylum authorities could also benefit from the CRRS and linking data from different IT systems, such as VIS, Eurodac, and the EES. This would enable the linking of depersonalised data and personalised statistics that could help with forecasting events and the movements of people.

> ***"Large-scale IT systems and interoperability should lead to improvements in efficiency as well as effectiveness of the relevant processes.***
>
> Nina Gregori, *EASO*

Mr McLaughlin began his talk by referring to the importance of the September 11 (2001) attacks in forcing a range of legislative and regulatory changes around processing and storing of data in the US. He introduced the activities of US Customs and Border Protection (US CBP) including border patrols, and air and marine operations. Since 2001, US CBP has been under the Department of Homeland Security. US CBP is an integrated border management agency that does passenger, immigration, as well as cargo processing. Over time, it has introduced a range of methods for automated analysis. On a daily basis, its program processes every person coming in and out of the US, and every piece of cargo. The accumulation

of data has allowed it to utilise sophisticated analytical techniques. Mr McLaughlin praised European efforts and said they are achievable and worthwhile goals. By keeping aggregate composites of data, he suggested, there is a better chance to look at data, identify and resolve any possible inconsistencies. On a daily basis, US CBP deals with about a million visitors entering and exiting the country. Over time, it has determined that geography is important, as is selector data like phone numbers and email addresses, as they assist resolving and identifying good from bad. Since 2004, the US has been collecting biometric data through the US Visa Program. First-time arrivals to the US undergo facial capture, a ten-print, and a document swipe. That information goes into its systems, and US CBP can utilise it in its facial recognition programme. The US has been using biometrics as facilitation and entity-resolution mechanism. He noted that they have seen many imposters, people travelling on other people's documents. Compared to border guards, the camera never gets tired and always has the same fidelity. In conclusion, Mr McLaughlin again emphasised the importance of storing and aggregating data.

> *"Compared to border guards, the camera never gets tired and always has the same fidelity.*
>
> James E. McLaughlin, *US CBP*

Mr Vande Ryse introduced Frontex, indicating that a new regulation will soon be adopted to provide for additional responsibilities related to the recruitment of a standing corps. The standing corps will be managed and coordinated in cooperation with the Member States. Frontex is an intelligence-led agency, where the automation of information processing is crucial. One of the objectives of Frontex is to get more involved in forecasting, rather than reacting to situations, thus, thinking in terms of scenarios becomes important. Scenario-building requires collecting more information from EU borders, including from non-EU countries, the pre-frontier area, and the external borders. Mr Vande Ryse specifically underlined one of the key benefits of interoperability, namely the easy access to all relevant data. In his opinion, however, this remains a huge challenge, and the reality in the Member States is that there is not always sufficient staff at external borders. Not all border guard communities are sufficiently staffed or properly trained. Biometrics in the meantime are not always available, nor are certain systems,

> *"For border guards, having one system to access all relevant information is a dream come true.*
>
> Dirk Vande Rise, *Frontex*

like SIS. Looking into the future, Frontex sees the need to recruit a standing corps to manage the thousands of people arriving to the EU in coming years. Once recruited, they will also require training. To conclude, Mr Vande Ryse showed an image of small vessels coming to Greece from Turkey, in the migration crisis of 2015, and explained that people often remained unchecked. He expressed the hope that in the future Frontex and its Member State partners will be better prepared.

Mr Seppälä focused his remarks on the ongoing work of the EU Council related to external border control. He suggested that the Member States have reached a compromise on the revised regulation of Frontex, which is expected to be signed and adopted in the coming weeks. Frontex will play an important role in the future of the EU and Schengen border management, and in the provision of relevant services. He emphasised that ongoing work on some of the legislative files might not be accomplished during Finland's Presidency and therefore will continue under the forthcoming Croatian Presidency. He stressed that delays in adopting legislative files will have an impact on the procurement of systems, writing of handbooks, as well as the preparation of implementing and delegated acts. The signing of legislative acts is only the beginning of the process. Finland's Presidency has been concerned with the readiness of the Member States to start implementing the new legislative acts once adopted. Policy discussions have focused on a number of related issues, such as governance, on making the decision-making process clear, and on building the integrated border management policy cycle. In conclusion, Mr Seppälä discussed budgetary issues related to the implementation of the new legislation, emphasising that national

investments are needed to implement changes in operations and external border control. We cannot wait for funds to emerge from Brussels, he said.

Mr Syrigos addressed the first question to Ms Gregori, asking her to reflect on the topics discussed by the panel. ***Ms Gregori*** said the panel showed how much we have achieved in recent years. Questions however remain about how Europe can react quickly in a crisis and what tools are at its disposal.

Mr Syrigos asked ***Mr McLaughlin*** about the added value of technology-driven borders. Mr McLaughlin replied that the US has spent a lot of money on border security and it has made its processes more efficient. It continues to build better workflows to enable admission and enforcement.

Mr Syrigos then asked ***Mr Vande Ryse*** about the benefits of the new information architecture from the perspective of Frontex. Mr Vande Ryse responded by stating that having the ability to look at the whole process, including what is going wrong, is a benefit. For border guards, having one screen, one system will be a dream come true and will benefit efficiency and effectiveness. He added that Frontex is working together with eu-LISA on the issue of establishing access to SIS, in order to move closer to their objectives.

Mr Syrigos then asked Mr Seppälä about other

elements related to the preparation of the Member States. ***Mr Seppälä*** suggested that there is a need for further legislative changes in the future, including cooperation with carriers and guidance on how to train personnel in future.

Mr Syrigos then opened the floor for questions.

Discussion

The first question from the discussion was addressed to ***Mr McLaughlin*** on the assessment of first-time travellers using the ESTA (Electronic System for Travel Authorization) system. Mr McLaughlin responded that the US looks at a number of different pieces of data prior to a travel event, which is done within 72 hours prior to travel. The follow-up question to Mr McLaughlin focused on the ability to implement biometric solutions at land borders in the US. In response to this query, Mr McLaughlin suggested that the US is working towards that end at three ports of entry in Southern Arizona, but does not foresee the implementation of biometrics at scale at land borders. He provided an example of a border crossing in San Ysidro, California, where there are 62 lanes for crossing the border. Making facial recognition work optimally in such scenarios is a challenge, he explained.

The next question focused on the possibility to prioritise some user groups, such as border guards in relation to visa and immigration, instead of trying to spread efforts across all fronts. ***Mr Syrigos*** responded to this by suggesting that the EES is currently the top priority and scheduled to go live in February 2022, where preparation work in collaboration with the MS and other Agencies is ongoing. ***Ms Felkai Janssen*** emphasised the importance of developing comprehensive statistical reports alongside the new EES, in particular for policy-making. ***Mr Syrigos*** explained that there is a legal basis for this, therefore cooperation with the MS, with the aim of developing such reports, will also be established. Furthermore, at eu-LISA level, activities have commenced in the form of a working group for CRRS that will work closely to analyse and design interoperability tools.

Session 4

Effects of Digitalisation on Data Analytics and the Use of Artificial Intelligence in the JHA Domain

Moderator:
***Maria Bouligaraki**, Head of Test Transition Unit, eu-LISA*

Panellists:
***Zsuzsanna Felkai Janssen**, Head of Sector for Migration, Directorate-General for Migration and Home Affairs, European Commission*
***Ann-Charlotte Nygard**, Head of the Technical Assistance and Capacity Building Unit, FRA*
***Bernd Zenker**, Lead Senior Experts – Big Data Analysis, Central Office for Information Technology in the Security Sector (ZITiS), Germany*
***Ott Velsberg**, Government Chief Data Officer, Estonian Ministry of Economic Affairs*

Ms Bouligaraki began by defining artificial intelligence as a set of advanced technologies using statistics, computer science techniques, neuroscience and cognitive psychology, that is capable of producing knowledge and making autonomous decisions, similar to human beings, using reasoning, autonomy and creativity. She further elaborated on one of the key approaches to artificial intelligence, namely machine learning.

> *"AI should be human-centric as well as trustworthy.*
>
> Zsuzsanna Felkai Janssen, *European Commission*

Machine-learning applies statistical methods to the analysis of training data in order to develop machine-learning models, which can then be used for different purposes, such as classification or prediction. Specific types of machine-learning systems mimic the way the human brain functions and deep-learning systems are based on the same technology as neural networks. Ms Bouligarki added that these systems have been essential for the development of modern AI systems.

There has recently been a huge improvement in the performance of AI systems for specific tasks, she continued. Different methods can be used, including supervised and unsupervised learning. However, whenever training of machine-learning models is concerned, it is important to take into consideration the size of the training dataset as well as the quality of data contained within it. The quality outputs produced by AI models will depend on the quality of training data used for training machine-learning models. AI systems are now used in everyday life. AI is also becoming relevant in the JHA domain as a means to integrate large, unconnected silos of data. She pointed out that progress in the development of AI has been accompanied by ethical dilemmas. In her concluding remarks, Ms Bouligaraki noted that despite all the challenges, interest in AI on the European level has been on the rise during recent years. The new Digital Europe Programme for 2021-2027, for instance, names AI as one of its main priorities, in addition to cybersecurity and supercomputing.

Ms Felkai Janssen began her presentation by introducing the ongoing activities focused on AI of DG HOME. She noted that in law enforcement, authorities are currently facing bigger threats because of emerging new disruptive technologies. These emerging technologies present a moving target for law enforcement authorities, both in terms of potential benefits as well as threats. Ms Felkai Janssen referred to two reports published by Europol recently, namely "Do Criminals Dream of Electric Sheep?" and "Common Challenges in Combating Cybercrime". According to Ms Felkai Janssen, the traceability of criminals is becoming increasingly difficult due to the use of encryption, the loss of localisation, and large data volumes. AI can help address these threats and counter them. In the law enforcement context, we need to demystify AI, she explained. So far, there have

not been many criminal attacks that use AI, but that does not mean that it will not happen. She outlined some of the criminal activities facilitated by AI, such as drones threatening airline security, large-scale cyber attacks, manipulation of autonomous systems, as well as tampering with digital evidence and the manipulation of voice and images, which all pose additional challenges for law enforcement.

Ms Felkai Janssen said that the European Commission launched a strategy on AI in 2018. The outstanding question is how individual Member States and individual authorities can face these challenges. There is a general understanding within DG HOME that AI will change how law enforcement works. In particular, AI poses considerable challenges concerning technology, available manpower and expertise. However, AI also offers a range of opportunities, some of those yet to be discovered, which will require engaging third parties, such as researchers. Law enforcement must have the capacity to work with the same technologies, as those used by the criminal organisations. All the Member States should develop a similar way of working in this field. If any state is weaker, criminals can exploit these weaknesses.

Furthermore, the European Commission has also been working on defining the principles of AI for law enforcement. AI should be human-centric as well as trustworthy. Ms Felkai Janssen provided an overview of the key principles of ethical AI, such as human agency and oversight, technical robustness and safety, privacy and data governance, transparency, non-discrimination and accountability. These principles will be continuously implemented and evaluated throughout the life cycle of all AI systems.

She presented the approach of DG HOME to AI, which includes a number of activities, such as a

EU2019.FI

pilot research project under the Horizon 2020 framework, building the underlying infrastructure with the support of the Digital Europe Programme, developing a pool of training data, establishing the Innovation Lab within Europol, as well as a study on AI in the field of large-scale IT systems. To conclude, she noted that the complex legal landscape in the EU is a particular challenge. For instance, the diverging transposition of the Police Data Protection Directive may result in some countries advancing much faster, while others lag behind in terms of the implementation of AI. Another challenge is to foster ongoing dialogue among the Member States, she noted.

Ms Bouligaraki asked whether the GDPR will be fit for purpose in the future to remove some constraints related to these developments.

Ms Felkai Janssen said that there needs to be serious discussion with data protection authorities about purpose-limitation principles in the context of law enforcement and operational data. Operational data could be used to train models. If you want good models, you need to use real data but for the time being that is not possible, she explained.

> ***"Algorithms may not be representative of the population and therefore lead to indirect discrimination.***
>
> Ann-Charlotte Nygard, *FRA*

Ms Nygard began her presentation from the perspective of the Fundamental Rights Agency (FRA) on how individuals are affected by new technologies and developments, including AI. FRA's mandate is to provide evidence and advise Member States based on data and evidence collected. Ms Nygard provided an overview of two recent FRA papers related to AI, big data, and facial recognition technology and discussed new fieldwork in Estonia, Finland, France, The Netherlands and Spain with people who are developing AI tools for the private and public sectors. These results will be available in 2020.

The work of FRA is focussed not only on risks but also on opportunities. It seeks to assess the compliance of algorithms and whether they are fairly developed and balanced. Referencing the metaphor of the misplaced shoes and socks introduced by Mr Rinkens earlier, Ms Nygard added that FRA keeps an eye out for data owners who may or may not be responsible for the "mess" in the system.

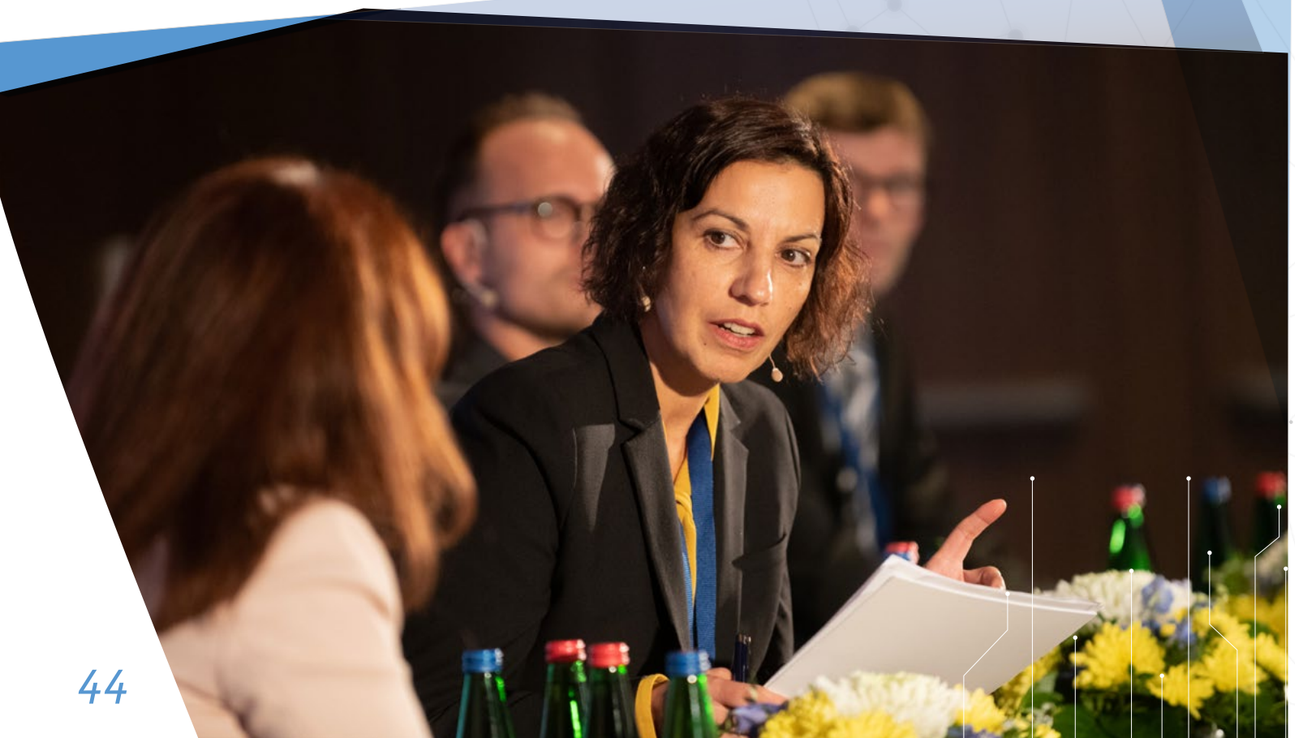
Ms Nygard discussed the right to non-discrimination in the European Charter of Fundamental Rights, which covers discrimination based on sex, race, colour, ethnic origin, genetic features, language, religion, birth, disability, sexual orientation, and other factors. While not intentional, she noted that some algorithms have been shown to be biased against a particular group, and this enables the algorithm to discriminate and reinforce discrimination. Algorithms may not be representative of the population for which they are used, and facial recognition may be biased based on gender or ethnicity. Algorithms can therefore lead to indirect discrimination. The quality of the algorithm can also have implications if built on data that are of poor quality, indirect, or outdated. This would also impact screening rules in the context of ETIAS to determine whether a person is considered a risk for entering Europe. Ms Nygard cited two specific risks concerning ETIAS: first, the use of data that could lead to the unintentional discrimination of certain groups, for instance if an applicant is from a particular ethnic group with a high in-migration risk; the second relates to a security risk assessed

on the basis of past convictions in the country of origin. Some such earlier convictions could be considered unreasonable by Europeans, such as LGBT convictions in certain countries. To avoid this, she concluded, algorithms need to be audited to ensure that they do not discriminate and this kind of auditing would involve experts from interdisciplinary areas.

Following on Ms Nygard's presentation, ***Ms Bouligaraki*** noted that bias in algorithms at times reproduces human bias. She said that people need to be rational and analytical with regard to AI. She called this an "emotional area". The community needs to tackle fears about AI. She asked Ms Nygard whether those fears are real. ***Ms Nygard*** responded that many aspects of AI are hidden from plain view and can be difficult to understand. As such, opinions are based on anecdotal evidence. The field must rely on concrete case studies, facts, and data to represent itself better. In terms of bias, Ms Nygard suggested four steps: an impact assessment to detect bias in the application and outputs of algorithms; data quality checks to avoid faulty algorithm training; transparency about how the algorithm is built; and expert oversight of the developed systems.

Mr Zenker began his presentation with an overview of the four areas to be covered in his talk: artificial intelligence, data and analytics, opportunities, and conflicts. Mr Zenker defined AI as automated decision-making by computers, and differentiated between so-called weak and strong AI. Weak AI supports humans in their decision-making, whereas strong AI performs equally well or better than humans. Another important classification is how the algorithm works. There are rule-based systems, where the developer has programmed the output. More advanced systems use machine-learning methods. In the case of machine learning, the model is developed by observing and analysing the relationships between the data. Digitalisation is a process that concerns the entire community, not just law enforcement. The same discussions are going on in healthcare and commerce. Some possible side effects of digitalisation may include a review of the whole decision-making pipeline, and increased awareness of what can go wrong in analytics. The opportunities arising from AI include the freeing-up of resources, harmonisation of processes, and knowledge acquisition from other communities. The results are less influenced by the bias of analysts. Conflicts present themselves as a trade-off between technical possibilities versus data protection regulations. The community needs to find a sweet spot to push development, he concluded.

Mr Velsberg gave a presentation about how the Estonian government has used AI to change its operations. Estonia launched its AI task force in August 2018 with three or four AI use cases. As of today, Estonia has 23 live AI projects in daily services. The government has the goal of having 50 AI projects by 2020. Many projects are multipurpose, and can be used in civic cases and potentially for internal security as well. For instance, there is a planning project called Kotkas (meaning "Eagle") whereby the police can detect movement when people are on the move, and the Ministry of Agriculture is interested in applying it to tracking horses and deer. The



EU2019.FI

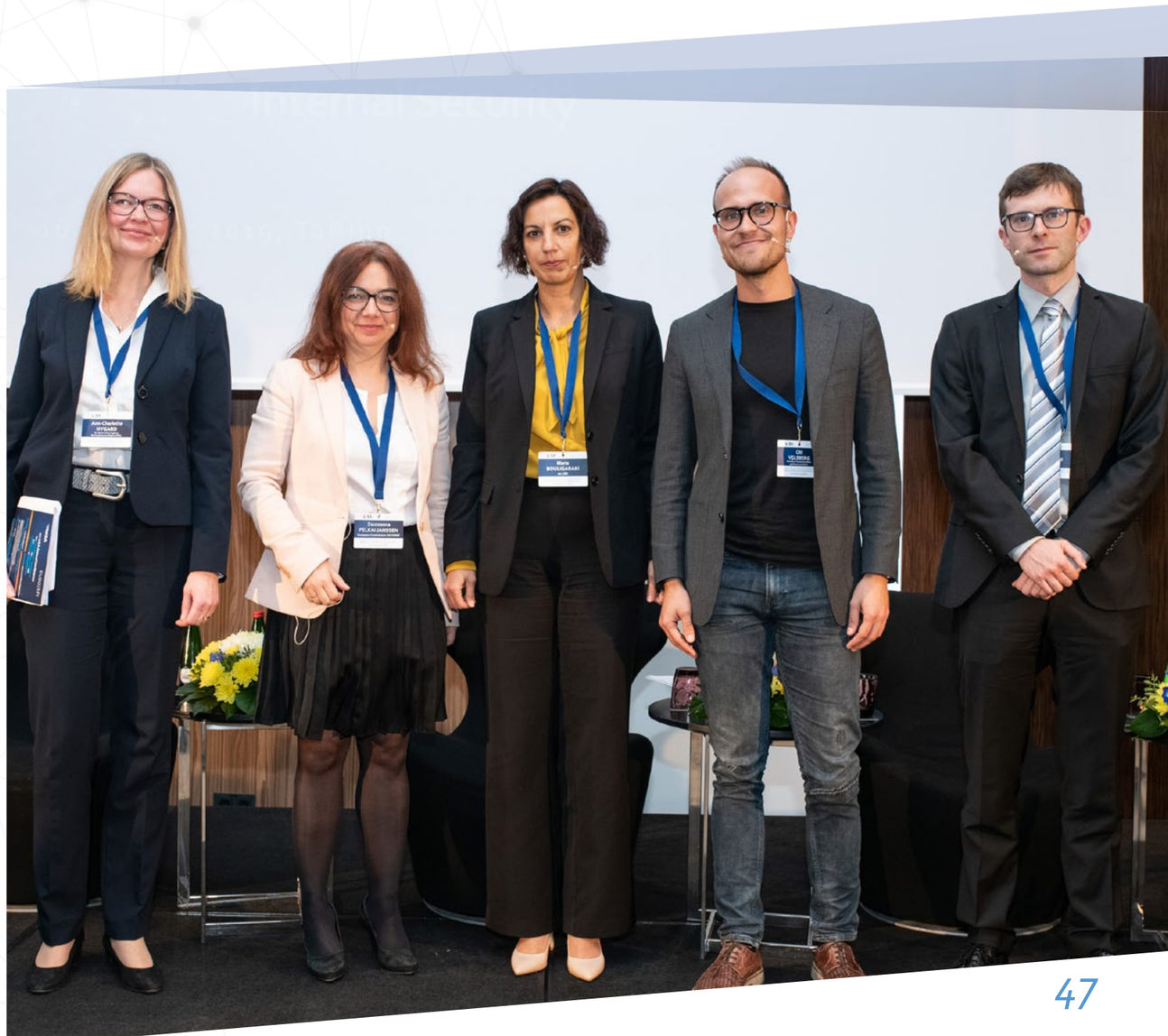
Estonian government is supporting its uptake across different sectors. Mr Velsberg discussed the limitations of automation. If processes cannot be automated fully, he asked, what is the point of automation? In Estonia, the government is trying to automate as much as possible. Scalability continues to be an issue as projects are reliant on cloud services. He said that people need to lower their standards when it comes to questions of transcription, for example, as, inevitably, some data will be missed. There are other challenges related to data protection, data governance, and the procurement of funding, which often depends on testing certain defined hypotheses. In general, Mr Velsberg suggested, people have unrealistic expectations when it comes to AI. They think AI will do everything, but it is really being used in narrow use cases and only a part of what humans do is automated. He indicated that no additional regulation is needed at the moment. Rather, people should learn from experience first and then determine what regulation is necessary. He concluded by saying that authorities should not deploy AI for the sake of it, but that AI projects should always add value.

> *"Authorities should not deploy AI for the sake of it, AI projects should always add value.*
>
> Ott Velsberg,
> *Estonian Ministry of Economic Affairs*

Ms Bouligaraki agreed that there was no need for overregulating AI before exploring the opportunities it can provide. She opened the floor for questions from the audience.

Discussion

The first issue raised by the audience focused on the division between AI training and its deployment. ***Ms Felkai Janssen*** suggested that in the case of law enforcement, deployment is always regulated, and therefore the main issue is the use of personal data during the training phase of development of AI or machine-learning algorithms. Although the GDPR is not applicable to data used for research purposes, there are different regulatory requirements on data processing at the Member States' level, which need to be taken into account. ***Mr Velsberg*** suggested that regulation during deployment should be applied on a case-by-case basis, emphasising that not every use case should be regulated in the same way. The next question focussed on the ETIAS screening rules and the application of AI to that, and in particular whether AI is mature enough for that. In response to this question, ***Mr Velsberg*** said that the technology is mature enough but that there are still areas where it needs further development. One issue facing the Estonian government is in language technologies, in particular in relation to small languages where significant investments are needed by national governments in order to make AI functional. In addition, despite the fact that a number of cloud-based AI services already exist and are ready for deployment at scale, he emphasised that in the case of government-owned data there are a number of restrictions prohibiting such use. Ms Felkai Janssen added that there are several products available on the market that could be used for ETIAS, however they need to be assessed properly before deployment. She further stressed that users need to work with vendors to bring these products in-house and use them based on their specific needs and requirements.



Closing Remarks

Krum Garkov
Executive Director of eu-LISA

Mr Garkov in his concluding remarks declared that the conference had been a success. He thanked the panellists and participants for their discussions on the new information architecture, the effects of digitalisation, and how both influence the collection and use of data and the ways data are turned into useful information. He said the community faces common challenges, including a volatile situation at its external borders, terrorist threats, and organised crime. The only way to address these challenges is with an interoperable mindset, which requires bringing down the silos between the various authorities, including law enforcement, border guards and other authorities. To get this done, not only must the technical issues be resolved but strong political commitment is needed. As internal security is undergoing transformation, the success of these efforts depends not only on the quantity of data but on the quality of data as well as the ability to turn it into meaningful information. New systems must be put in place so that common practices and best standards are followed across the board, and more resources are needed for developing standards. These elements underpin the success of interoperability. According to Mr Garkov, eu-LISA will continue to be an important partner in the future, in supporting both the Member States and the Commission. He said that eu-LISA expects to grow in the coming years and will expand its internal development and capacity building. He emphasised that the time for theoretical discussions is over and that it is now time for practical solutions that can be deployed to support practitioners.

Ilkka Salmi
Permanent Secretary, Ministry of the Interior, Finland

Mr Salmi made five points in his concluding remarks. First, he provided a comprehensive view of the main challenges from a technological standpoint, especially in the areas of law enforcement and home affairs. Second, he emphasised the importance of complying with fundamental rights, data protection and privacy, when a new technology is introduced. Third, he pointed to the importance of handling vast amounts of available data well. Fourth, he emphasised the need for efficient use of available information. Last, he said that European Ministries of the Interior need to drive the future, and not just react to changes. In conclusion, on behalf of the Finland's Presidency, he thanked all of the panellists and moderators and eu-LISA for organising the conference.

AFIS	*Automated Fingerprint Identification System*
AI	*Artificial Intelligence*
API	*Advance Passenger Information*
BMS	*Biometric Matching Service*
CIR	*Common Identity Repository*
CRRS	*Central Repository for Reporting and Statistics*
DG HOME	*European Commission Directorate-General for Migration and Home Affairs*
EASO	*European Asylum Support Office*
EES	*Entry-Exit System*
ENLETS	*European Network of Law Enforcement Technology Services*
ESP	*European Search Portal*
EU	*European Union*
eu-LISA	*European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice*
ESTA	*Electronic System for Travel Authorization*
ETIAS	*European Travel Information and Authorisation System*
EURODAC	*European Asylum Dactyloscopy Database*
FRA	*European Union Agency for Fundamental Rights*
Frontex	*European Border and Coast Guard Agency*
GDPR	*General Data Protection Regulation*
GPS	*Global Positioning System*
ICT	*Information and Communication Technology*
IP	*Internet Protocol*
IT	*Information Technology*
JHA	*Justice and Home Affairs*
LGBT	*Lesbian, Gay, Bisexual and Transgender*
MID	*Multiple-Identity Detector*
MIDAS	*Migration Information and Data Analysis System*
NCB	*National Central Bureau*
PISCES	*Personal Identification Secure Comparison and Evaluation System*
PNR	*Passenger Name Record*
QUEST	*Querying Europol's systems*
R&D	*Research and Development*
SLTD	*Stolen and Lost Travel Documents database*
sBMS	*Shared Biometric Matching Service*
SIS	*Schengen Information System*
SMEs	*Small and Medium Enterprises*
TDAWN	*Interpol Travel Documents Associated with Notices database*
UMF	*Universal Message Format*
US	*The United States of America*
US CBP	*The United States Customs and Border Protection agency*
VIS	*Visa Information System*

EU2019.FI

The sixth eu-LISA annual conference "The New Information Architecture as a Driver for Efficiency and Effectiveness in Internal Security" was organised by eu-LISA under the auspices of Finland's Presidency of the Council of the European Union, in Tallinn, Estonia.

The event was the first to take place since the provision of an extended mandate to the Agency through the approval of the new eu-LISA regulation. The enlarged mandate provides for the development of several new large-scale IT systems – the Entry-Exit System (EES), European Travel Information and Authorisation System (ETIAS) and the European Criminal Records Information System for Third Country Nationals (ECRIS-TCN) – as well as the implementation of interoperability. Together, the new capabilities and the new approach to data organisation and information provision constitute a new information architecture at EU level. As the Agency embarks on the elaboration of this architecture, working closely with Members States, EU Agencies and the wider stakeholder community, the time is right to reflect on how work can be best carried out and to define milestones that best fulfil the stated goals of improving the efficiency and effectiveness of internal security related activities. By convening over 180 delegates and providing a forum for debate and discussion, the conference brought an important contribution to these efforts to define optimal future outcomes.

Discussions focused on the future of internal security and opportunities presented by the new information architecture, the specific future roles of current and new IT systems in the Justice and Home Affairs domain, and the effect of digitalisation and the overall information ecosystem being created on law enforcement and border management activities.

The main conclusion drawn from the conference is that the consolidation of large-scale IT systems will lead to better possibilities to examine data together and take information management to the next level. Furthermore, applying machine learning and artificial intelligence capabilities can help derive better insight from system data in the future. These goals, however, can only be reached in close cooperation and engagement between the EU Agencies, Member States, and all other relevant stakeholders.

eu-LISA looks forward to playing a critical role in the enhancement of EU internal security in the coming years through offering high quality and highly effective technological solutions!

Publications Office

ISBN 978-92-95217-57-7
doi:10.2857/477811
Catalogue number: EL-01-19-835-EN-N

@EULISA_agency
@EU2019FI

/agencyeulisa
/EU2019FI