EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

MEMO / 28 March 2018

'Under watchful eyes – biometrics, EU IT-systems and fundamental rights'
Q&A

1. Why was this study needed?

In 2015, over 50 million non-EU nationals visited the EU. There were over 200 million border crossings over the external Schengen border. Given the number of crossings, border management increasingly relies heavily on technology which is rapidly changing to make decisions about the people crossing.

However, the impact of the ever growing number large-scale EU migration and security IT-systems on fundamental rights remains largely unexplored, apart from some analysis on data protection issues. This report intends to partly fill this gap.

2. How was the study conducted?

The Agency's multidisciplinary network of researchers carried out desk research for FRA. In 2015, they mapped practices and procedures related to the use of databases in all EU Member States.

FRA also contracted field researchers to carry out in-depth interviews with practitioners (public officials, including immigration lawyers and NGOs), experts (fundamental rights, biometrics and IT experts) and asylum seekers and migrants. It also did three small-scale surveys with border guards, staff processing visa applications at embassies and their external service providers and with visa applicants.

3. What does this report cover?

It analyses the positive and negative fundamental rights implications of processing biometric and other data in EU IT-systems in the field of visa, borders and asylum.

IT systems increasingly build on biometrics as the unique identifier. They connect the person to an increasing amount of information stored digitally.

It examines the importance of the right to information and the obligation to respect human dignity when biometric data are collected - data related to the physical characteristics of a person such as their fingerprints or how their face looks. It analyses how the right to asylum and the rights of the child are affected. It looks at how access to and use of data could be optimised, while also acknowledging the obvious risks involved in unlawful access to data. The report examines the reliability of data collected and stored and the consequences for individuals if such data is blindly trusted. The report also examines the possibilities for people to effectively exercise their right of access, correction and deletion of data.

4. How does the EU use IT systems?

They are used in various migration-related processes: for checking asylum and visa applications, during border checks, when issuing residence permits, when apprehending irregular migrants, in return procedures and for issuing entry bans. In addition, they are used for police checks and in the fight against serious crimes and terrorism.

Currently the EU has created three large-scale asylum and migration IT systems:

1. SIS II – the Schengen Information System to aid police and border checks;
2. Eurodac – for identifying asylum applicants;

3. VIS – the Visa Information System for visa processing.

There are also plans exist to set up three new systems:

1. EES – the Entry-Exit System for registering travel in and out of the EU;
2. ETIAS – the European Travel Information and Authorisation System for pre-border checks for visa free travellers;
3. ECRIS-TCN – the European Criminal Records Information System for non-EU nationals.

At the end of 2017, the European Commission proposed making these systems 'interoperable' by creating a common search portal. Biometrics would be used to match core biographic data, stored in a common repository, of the people whose data are stored in the different IT systems would be accessed.

5. What data do the systems collect?

The IT systems referred to in this report often store, or are expected to store, biometric data. This is addition to biographical data such as name, date of birth and nationality, for example. The preferred EU biometric identifiers are fingerprints and/or facial images. This report focuses on these and not on, for instance, iris recognition, which is also sometimes used nationally.

6. What are the main benefits of using IT systems?

With large numbers of people on the move, IT systems are more efficient and allow quicker and more reliable data processing, if fed with accurate information and are correctly used. They also offer more robust and timely protection – for example, for missing children, and victims and witnesses of crime – and can help prevent identity fraud and identity theft.

7. What are the main drawbacks of using IT systems?

There are many fundamental rights challenges that result from collecting, storing and processing data in large-scale IT systems. They range from disrespectful treatment when taking fingerprints, difficulties to disprove a wrong assumption and in correcting or deleting inaccurate data, to the risk of unlawful use and sharing of personal data with third parties.

8. Are the data reliable?

About 50% of European border and visa officials interviewed by FRA spoke of data entry mistakes in their IT systems. This can result from spellings errors including mistakes when converting names to Latin alphabets, difficulties in interpretation, incomplete or incorrect data provided, confusion over first and last names, uncertainty over the exact date of birth or fingerprints being assigned to the wrong person.

National authorities and experts attach a high degree of credibility to biometric data. This makes it difficult to rebut errors in IT systems and prove that the biometric match is wrong.

In addition, as children age their fingerprint and face change, undermining the reliability when making comparisons with records taken many years earlier.

Mistakes can have serious consequences. For example, it can lead to arrests by the police or prevent legitimate border crossings. Asylum applicants may also be suspected of having intentionally tried to provide a false identity undermining the credibility of their asylum claim.

9. Can mistakes be easily corrected?

Complicated procedures as well as administrative and language barriers may prevent people from exercising their right of access, correction and deletion of inaccurate or wrong data. In addition, there tends to be a lack of specialised lawyers who can help.

Corrections may become even harder once IT systems become interoperable as people do not know where to go to have the information amended. However, the creation of a 'one-stop-shop procedure' for receiving requests for right of access, correction and deletion of data, could simplify procedures.

10.Who can access the data?

EU IT systems are increasingly being used for purposes other than the ones they were built for. Law enforcement authorities typically access the data to fight serious crime and terrorism, and for immigration control.

Data may also be shared with private companies such as airlines and non-EU countries when it comes to preparing to return a asylum applicant before the process and/or appeal has closed. This can have repurcussions for those who return as they may be persecuted in their countries of origin for having sought asylum.

With interoperability across different IT systems, access could be potentially become wider.

Therefore, the risks for unlawful sharing and further use are very real. Illegal access and hacking are additional threats to the protection of personal data. This is especially true as data on non-EU nationals are attractive to organised crime groups, as well as hackers linked to foreign governments seeking to prevent political opponents from leaving those states. Oppressive governments may also use the data to punish family members as acts of retaliation to force dissidents to return.

11.How are children particularly affected?

Taking fingerprints of young children affects the quality and reliability of a future match. This risk of a wrong match increases when the fingerprints or facial images are compared more than five years later.

Depending on their age and maturity children may also have difficulty understanding what is happening to them. Using force to take fingerprints risks retraumatising children who may have suffered in their home countries or when travelling to the EU. This underlines the need to take fingerprints of children and inform them in a child- and gender-sensitive manner.

Criminal records of children may also be stored in some IT systems. However, sometimes the migration offences were committed when travelling with their parents and relate to irregular entry or stay in a country. In other cases, children may have been forced to commit crimes as a result of being trafficked and exploited. According to international child rights law, children should be protected from the stigma of having previous convictions. Such data should be kept confidential and not shared with third parties. This should allow them the opporunity for rehabilitation in later life.

Many unaccompanied or separated children who enter the EU later go missing. This may lead to abuse and exploitation, including human trafficking. IT systems could help trace missing and abducted children and forge links between police and child protection authorities.

12.What can be done to protect fundamental rights better?

- Provide information in a clear and understandable way so that people know why data are being collected. This will make them more willing to cooperate.
- Treat people with respect when taking fingerprints without resorting to force. This includes taking fingerprints in a child-friendly and child-sensitive manner.
- Making better use of IT systems to trace missing children.
- Ensure that industry uses fundamental rights expertise in the design of new solutions through for example embedding data protection into their products and services.
- Provide strong safeguards to prevent unlawful access to data. This includes the use of strong firewalls to prevent private companies for example seeing information they are not meant to see. Monitoring access through log files should also continue to be reinforced.
- Respect for the right to seek asylum, especially for those people who may be trying to hide their identity because they were being persecuted or have been flagged in international crime databases to be found by oppressive regimes.
- Prohibit the transfer of data to non-EU countries especially in cases where asylum applications are still ongoing.
- Evaluate the fundamental rights impact of law enforcement access to border management IT systems for fighting crime and terrorism. They must first consult databases linked to criminal investigations before being allowed access to other such systems. There also must

only be limited or no access to information about the criminal records of children stored in border management IT systems.

- IT systems are increasinlgy been used for apprehending and returning irregular migrants. Applying apprehension policies for irregular migrants in line with fundamental rights is therefore becoming increasingly important. This means they should not fear reporting a crime or seeking healthcare to avoid having their residence status revealed and being apprehended.
- Improve data quality and accuracy of the records stored in IT systems.
- Allow people to access their personal data and have the data corrected and deleted if inaccurate. This could be helped by simplified procedures, information campaigns on how to exercise this right and dedicated training for lawyers so they can offer relevant help.

For further information, please contact the FRA Media Team.

Email: media@fra.europa.eu / Tel.: +43 1 58030-642