07 October 2020

"The State of Biometrics"

Update from the European Data Protection Supervisor

Wojciech Wiewiórowski

I. INTRODUCTION

Ladies and gentlemen,

As Isabelle already referred to in her introduction, the number of devices **processing biometric data is increasing at an amazing speed**. Many smart phones use face images and fingerprints to authenticate its users. Virtual voice assistants process voice data to answer users' requests. Video surveillance and digital signage systems process face and full body images to identify or classify individuals. Smart watches and fitness bands process our heart beat rates and our sleeping habits.

COVID-19 brought us many new obligations for our daily lives. During this ongoing pandemic, some support using face recognition and artificial intelligence to monitor social distancing or the correct use of facemasks. In the same vein, others support the use of temperature-sensitive cameras and face recognition to identify those potentially infected with the Corona virus.

Public administrations are not an exception to this trend, and the **EU institutions, offices, bodies and agencies** are increasingly processing biometric data.

The **establishment and operation of large scale IT systems** form an intrinsic part of the EU legal and policy framework on external borders, migration and asylum. The EU has set up three large-scale IT systems in the areas of asylum and migration, which are currently operational and process biometric data: the Visa Information System (VIS), the Schengen Information System (SIS II) and EURODAC, the system processing asylum seeker data.

On top of these three systems, the European Union is developing **three additional new large-scale IT systems,** two of which will process biometric data: the Entry-Exit System (EES) and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN). Although the EU developed all these large-scale information systems independently, the law now prescribes four interoperability components enabling interaction with one another. Among them, a shared **Biometric Matching Service (BMS)** will enable the querying and comparison of biometric data (both fingerprints and facial images) across systems.

Just in August the European Commission launched a review on the 2008 framework for **automated data exchange** allowing a member state to query DNA, dactyloscopic and vehicle registration data in one or several other member states' national databases ("Prüm").

II. PERCEPTION, TRUST AND THE EDPS

But not all is well.

Along with its growing popularity, some **misconceptions** about the technologies involved have become widespread. I believe we need to raise awareness about some of those misunderstandings about biometric technologies, and we need to motivate everyone to check assertions about the technology, rather than accepting them without verification. That is why I published a Joint paper with the Spanish data protection authority on "14 misunderstandings with regard to biometric identification and authentication" destined for the general public.

In addition, we see clear abuses of the new technologies: **Clearview AI scraped** 3 billion images gathered from millions of websites, including Facebook, Twitter and YouTube, and now sells its services to law enforcement authorities. The **Polish platform PimEyes** did and still does the same. Any user can upload a photo of a person on their website and have it displayed wherever that face can already be found on the internet. So it is de facto possible to have every person you meet on the street, and of whom you might even take a snapshot unnoticed, checked by the database. [After the public attention it received, this company now claims that it is "a multi-purpose tool allowing you to track down your face on the Internet, reclaim image rights, and monitor your online presence".]

The increased use of the biometric data along with the impossibility to change our physiological traits, has also greatly increased our concern on **biometric data security**. If biometric system designers do not implement appropriate safeguards, the consequences of a personal data breach would be very serious. It is for this reason that we very much welcome the development of international standards such as ISO/IEC 24745 and the advances in biometric template protection mechanisms (BTP). European projects such as TURBINE, FIDELITY and SWAN helped develop some of these BTP mechanisms that aim at guaranteeing the irreversibility, unlinkability, and renewability of biometric references. But, despite ISO/IEC 24745 being nine years old, I am still uncertain of the extent to which the biometric system designers' and developers currently follow it. In 2019, security researchers found out that there was a database with 28 million records unprotected and mostly unencrypted. The database pertained to Biostar 2, a system developed by the security company Suprema. Among other data, the unprotected database included fingerprint data, facial recognition data, photos of users' faces, unencrypted usernames and passwords.

The **sensitive nature of biometric data**, recognised both within the EU legal framework, as well as in the framework of the Council of Europe's Modernised Convention 108+, makes it subject to special protection: **the processing of biometric data is prohibited in principle** and there are only a limited number of conditions under which such processing is lawful.

That's why as part of its **supervision and enforcement tasks,** the EDPS conducts regular audits on the EU's large scale IT systems already in operation and we will conduct regular audits on the new ones when they become operational.

The EDPS also provides **advice** on the lawfulness of processing biometric data by EU institutions in other contexts. By way of example: the EDPS accepted the use of biometric systems for security purposes in a limited number of cases. Conversely, the EDPS did not consider proportionate the use of biometric systems for monitoring staff members' working time and leave. We considered the processing of biometric data was not necessary in relation to the purpose because such purpose could be achieved with less intrusive means as by signing in, using attendance sheets, or using clocking in systems via magnetic badges.

Therefore, we should **first ask ourselves about their necessity and proportionality**. We should not use a perfect system that we do not need or that is processing biometric data in a disproportionate way. Although often accuracy, necessity and proportionality are discussed altogether, they are different topics that should not be merged.

The necessity is hard to establish in some cases. Some months ago one of the biggest supermarket chains in Spain installed facial recognition systems in 40 of its supermarkets. The system processes the faces of **all customers** in the supermarkets to detect the **few individuals** banned by court orders. The first question that comes to mind should not be if the system is accurate enough, but if it is necessary and proportionate to achieve its goal. In July 2020, the Spanish data protection authority started an investigation on this system and I am looking forward to learn about their findings.

All **other relevant data protection principles** laid down in the GDPR such as purpose limitation, and data minimisation, need to be adhered to.

Processing of biometric data should strictly adhere to the **purpose limitation principle**: personal data must be collected for specified, explicit and legitimate purposes and it cannot be further processed in a manner which is incompatible with those purposes. Purpose limitation is especially relevant in this context because many biometric data types allow inferring about other personal data. The same facial images allowing users to authenticate themselves can also be used to infer some health conditions. Voice data processed by smart assistants to answer users' commands allow inferring about their emotions. It is possible to use keystrokes patterns to tell apart humans and computers in online exams, but it is also possible to use this data to uniquely identify individuals. Not to speak of the amount of inferences that DNA allows.

It is also for this reason that biometric data processing needs to fully apply **data minimisation**. When assessing which biometric technologies to use, it is necessary to limit the biometric data processed to what is necessary to accomplish a specific task. For instance, in the EDPS opinion on the Proposal for a Regulation strengthening the security of identity cards[1] we explained that while storing fingerprint **images** enhances interoperability, at the same time, it increases the amount of biometric data processed and the risk of impersonation in case of a personal data breach. Therefore, the EDPS recommended limiting the fingerprint data stored on the documents chip to the biometric template.

[1] European Data Protection Supervisor, Opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents

While multimodal biometric systems could be more secure and accurate than regular biometric systems, processing more biometric data involves higher risks for the fundamental rights of individuals. When considering the processing of more than one type of biometric data, it is once again necessary to assess their necessity and proportionality, balancing the expected benefits against the risks.

As with any other technologies, the shine of the new possibilities blinds or distracts us from asking ourselves the fundamental questions: Are these biometric applications something we really need or are they just convenient? Is processing the biometric data of all individuals proportional to their aims? Is it the right thing to do?

I believe if you want the biometric data processing to thrive, it is vital to invest in public trust. To gain the trust of our society in biometric systems, it is necessary to be honest, clear and direct in communicating the strengths and limitations of each biometric technology, its possibilities and its risks. This **public perception of those risks** is why millions of users voluntarily decide to use biometric data to authenticate when using their smartphones, while there is a growing opposition on the use of biometric identification and categorisation in public spaces.

The European Union is currently preparing **new legislation for data, artificial intelligence and digital services** provided in the EU. This will have a clear impact on biometrics and the lawful use of biometric data.

In that context, the European Parliament's IMCO Committee calls for digital service providers to store biometric data only on the device itself, unless central storage is allowed by law, to always give users of digital services an alternative for using biometric data set by default for the functioning of a service, and the obligation to clearly inform the customers on the risks of using biometric data".

Biometric identification in public spaces, even for public good purposes, would have a much stronger effect on fundamental rights. Furthermore, the frictionless nature of facial recognition would have the same chilling effect regardless of whether its use in public spaces would be ubiquitous or not. The fear of surveillance is enough to affect our behaviour.

The EDPS shares citizens' concerns on the risks brought about by some processing of biometric data in public spaces such as live facial recognition. The fact that these systems are easily hidden and frictionless increases the risk of turning them into a ubiquitous and pervasive surveillance complex.

I fear we in our societies still lack the full picture of the individual and societal impact of automated recognition in public spaces of human features, not only of faces but also of gait, voice, and other biometric or behavioural signals. **I therefore support the idea of a moratorium on their deployment, in the EU, so that an informed and democratic debate can take place.**[2]

III. Concluding remarks

My staff and I at the EDPS are closely following the advances in biometrics and we will liaise more with experts in the field.

[2] EDPS strategy 2020-2024, https://edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future_en

This brings me to the necessary work done by the Biometrics Institute. With the publication of the "Good Practice Framework" and the "Three laws of biometrics" you clearly do your part on the path to promote the responsible and ethical use of Biometrics and Biometric Analytics.

I very much welcome these efforts.

But we can't stop there. This is not only for the experts. These seeming technicalities affect everyone. We need to have **informed and democratic debates.**

I cannot underline therefore how important it is to deploy biometric data in full knowledge and not only respect the existing legal frameworks, but also of the possible implications on society.

We need to protect individuals, not just data.

I wish you a very fruitful discussion in the coming days.

* * *