Something Wicked This Way Comes

Pika Šarf 2022-04-08T10:17:44

Writing in the aftermath of 9/11 terrorist attacks, Steven R. Salbu noted: "*Since EU and U.S. political interests are largely aligned in the war against terrorism, it is possible that the EU will move closer to the U.S. as a result of the attacks, rather than the U.S. moving away from the EU. To the extent that Europeans feel vulnerable as a result of terrorism, they may shift their emphasis away from data privacy and toward protective anti-terrorist surveillance programs*". In the early days of the 2000s, his dystopian prediction could not have felt more ill-fated, as data protection was gaining its momentum with the adoption of Directive 95/46. Today, it is no longer so far away from the truth, at least from the perspective of third country nationals ("TCNs").

One crisis after another was offered as a justification for the establishment of a comprehensive surveillance apparatus, while TCNs were gradually stripped of their rights to privacy and data protection, transforming the movement of innocent individuals into suspicious, potentially terrorist activities. Among the most significant changes in information management in the area of freedom, security and justice (AFSJ), interoperability – the ability of information systems to exchange data – will have the most profound effects on the right to data protection and as such marks the "point of no return". This contribution will seek to answer the question, how did we get to this point, and more importantly, where do we go from here?

Knowledge is power

On 6 June 2013, Snowden's revelations exposed a mass surveillance programme conducted by the U.S. National Security Agency, which for decades had been secretly gathering intelligence on the entire foreign population, including their political leaders, international organisations, and businesses. While the United States vigorously defended the legality of its intelligence gathering programmes, predominantly by leaning on the argument of their indispensability in the fight against terrorism, the international community was unanimous in condemning bulk and systematic blanket collection of (personal) data. The European Parliament was among the most vocal critics of both the surveillance practices as well as the flawed rationale behind it. In its Resolution, adopted on 12 March 2014, it stated that "*the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes;* […] *such programmes are incompatible with the principles of necessity and proportionality in a democratic society*".

What is more intriguing to look at is what the European Parliament stayed silent on, in particular, what it failed to say about the EU's own data gathering practices in the fight against terrorism and serious crime. At that time, all of the EU information systems in the AFSJ that are in use today, namely the second-generation Schengen Information System (SIS II), the Visa Information System (VIS) and the European

Asylum Dactyloscopy Database (Eurodac), were already fully operational. Two of them (SIS II and Eurodac) had just undergone a major transformation from purpose-specific centralised databases with narrowly defined access rights, to more general, security-oriented investigative tools. Additionally, the EU had been contemplating the idea of establishing two additional databases, the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS), and making all of the AFSJ information systems interconnected in order to enhance the level of security while facilitating travel for *bona fide* TCNs. None of the initially proposed measures were adopted at the time. However, that does not mean that they were off the EU's agenda, but rather that they were hibernating, waiting for the right moment to be brought back to the table.

Crises in the EU as the catalyst of enhanced surveillance

The terrorist attacks that occurred in Paris in January and November 2015, and at the beginning of 2016 in Brussels, coupled with the peak of the migrant crisis, fuelled the security agenda of the Juncker Commission. The EU institutions stood united in condemning the tragic events that shocked the old continent and immediately announced new counter-terrorism measures to be adopted. Following the trend of blurring the lines between immigration management, border control, law enforcement and broader (internal and external) security prevention, strengthening control of the external borders of the Union became one of the top priorities in the EU's fight against terrorism, and "*stronger and smarter information systems*" were at its core. While in the European Agenda on Security, which was adopted at the beginning of 2015, a shift towards more generalised surveillance of third-country nationals was already perceptible the Agenda does not urge for introduction of new measures, but rather calls for the reform of the existing tools and their use to the fullest extent possible. However, the documents adopted in 2016 show a noticeably different picture – a picture of Europe striving to "*regain control over the external borders*" by pushing for numerous previously withdrawn legislative proposals and introducing a plethora of new ones with the aim of ensuring a high level of internal security. In the following three years, the legal basis for the establishment of three additional centralised databases was adopted (EES, ETIAS, ECRIS-TCN), information exchange was intensified by the revision of two of the existing information systems (SIS II and VIS), while the proposal to reform Eurodac is still being negotiated as a part of wider transformation of migration and asylum policy in the EU.

EU in crises meets technical feasibility: Interoperability of information systems in the AFSJ

Finally, in May 2019, all of the previously separated AFSJ databases became interoperable – or at least are on the path towards becoming interconnected once the proposed measures become operational – with the adoption of two Interoperability Regulations (Regulation 2019/817, Regulation 2019/818). Interoperability as "*the ability of information systems to exchange data and to enable* *the sharing of information*" will consist of four components: the European Search Portal, the Shared Biometric Matching Service, the Multiple Identity Repository and the Multiple Identity Detector (detailed description of the components is available here). They will enable separate information systems to start *talking to each other* in order to fill the blind spots created by the compartmentalised approach to AFSJ information systems. EU documents and proposals continuously endorse the position that reduces the concept to a purely technical matter, explicitly stripping it of any political or legal connotation by stating that "*interoperability is a technical rather than legal or political concept*". By endorsing the position of interoperability being a technical choice, the debate surrounding the adoption of the Interoperability Regulations mainly revolved around the question whether the proposed measures were technically feasible, rather than compatible with the human rights regime in the EU, especially with the right to data protection. This position was met with fierce opposition from the institutions entrusted with the protection of human rights (e.g. EDPS, WP29, FRA). They recalled with a single voice that interoperability will profoundly change the information sharing apparatus in the EU, thus the choice to implement it should be made upon thorough consideration of all relevant factors, not merely technical feasibility. Confusing legal with technical repercussions precludes having a proper debate from the human rights perspective. Yet, by reducing interoperability to a purely technical concept and then allowing the technical feasibility to dictate political choices without clearly specified aims of the measure, the risk is that interoperability becomes an end in itself.

Where to next?

When assessing surveillance measures at this critical moment in time, when the world is faced with the Covid-19 pandemic, it is perhaps more than ever important to look into the past to better understand what may lie ahead for us. Once again, we are faced with an unprecedented threat, similar to the situation in 2001, when the 9/11 terrorist attacks forever changed the intelligence-gathering practices of the global community. With the global spread of Covid-19, a highly contagious disease with a large percentage of asymptomatic cases, the adversary today is more intangible than ever. As a consequence, countries may feel the urge to extend the scope of their surveillance practices a step further, by subjecting their own citizens to constant monitoring.

The idea is nothing new; quite the contrary. Already during the discussions regarding the Smart Borders Package there arose an idea to monitor the border crossings of all travellers, not just TCNs, either in the Entry/Exit System or in a separate large-scale database. If (or better, when) border controls are no longer a measure of immigration control and internal security, but rather a measure to contain the spread of the deadly virus, which does not differentiate between EU citizens and third-country nationals, it becomes much easier to justify the surveillance of the entire population. In fact, this would not be the first privacy-invading measure imposed in the fight against Covid-19. Numerous countries introduced contact-tracing applications, while others were even subjecting infected individuals to mandatory geolocation tracking enabled by wearable technology. Although the majority of the solutions being developed in the EU attempt to preserve privacy and are in line with the established data protection regime, it is undeniable that they have the potential to reveal certain aspects of our private lives. The arguments put forward by governments worldwide in favour of the new wave of highly sophisticated digital surveillance tools are strikingly similar to the post 9/11 rhetoric: each and every one of us will have to give up a bit of our privacy in order to survive as a community.

Since it is becoming ever clearer that fundamental rights may very well be the biggest victim of the coronavirus pandemic, it is high time for the EU to re-evaluate whether it still values privacy and data protection enough to be willing to fight for it. And if it does, it should start by protecting the rights of third-country nationals, as their rights are at the moment endangered the most – tomorrow it could be us.