Interparliamentary committee meeting European Parliament – National Parliaments
Smart Borders Package: European Challenges, National Experiences, the way ahead
23-24 February 2015

Smart Borders and Law Enforcement Access: Legitimacy, Effectiveness, and Proportionality

Evelien Brouwer (associate-professor VU University Amsterdam, e.r.brouwer@vu.nl)

1 Introduction - Trust

I am honored to be invited as legal expert in this meeting of members of national and European parliaments and to be able to share my views in the discussion on the added value of smart borders and the question on access to law enforcement authorities. I follow this topic which great interest not only as legal researcher, but also as a member of the Meijers Committee, a Dutch NGO in which we commented on the 2013 draft on smart borders before. In this contribution, I will emphasize on three criteria which in my view should be central in the forthcoming discussions and decision making: legitimacy, effectiveness, and proportionality. Criteria which also take into account the strict conditions as formulated by the European Courts when dealing with fundamental rights, and more recently by the Court of Justice on the Data Retention Directive in 2014.

Before I go into these issues, I hope you allow me to refer to two examples from practice which came up in my mind when thinking about border controls and databases. First, a memory I recall from my earlier research on the establishment of Schengen Information System or SIS. Before SIS became operational, I met police officers expressing their doubts at the development of such a large scale database. They told they preferred bilateral cooperation and exchange of data with police officers from other states they already knew, based on earlier cooperation and mutual knowledge, rather than setting up a European database, giving them the feeling they would lose control over their files. Even if, almost twenty years later, SIS may

be considered as successful tool, because of the specific goals and criteria of reporting data, it always reminds me how important trust is as an underlying basis for sharing information with other authorities. My second example concerns a news item of last week, mentioning that a quarter of Dutch police officers engaged with criminal investigation and asked to submit their DNA in so-called 'elimination files' refused to do so. The goal of these elimination files is clear and is not contested by the police: it prevents mismatches or contamination of DNA traces found at the crime scene. However the reluctance to submit their DNA was explained by the general distrust of police officers to store such 'sensitive' data in central databases, because of their experience these systems can easily be hacked and data misused. I focus on these meanings of trust, because I think it is a condition of every measure or new tool developed by the European legislator.

2 What do we want, what do we have, what do we need (more)?

Dealing with the criterion of effectiveness we should first ask ourselves what do we want and what do we need to control our borders? A clear definition of borders is of course not easy to give, but when considering the function of Europe's external borders, one generally agrees on the following purposes: preventing irregular migration and preventing asylum shopping, facilitate legal migration and free movement, fight against terrorism and serious crimes and, partly, as this also concerns cooperation across the borders, judicial and police cooperation.

Dealing with migration control, three large scale databases are operational: SIS for the purpose of refusal of entrance to ' unwanted migrants', the Visa Information System (VIS) for the exchange of data on every visa application, and Eurodac including fingerprints of all asylum seekers in Europe for the determination of the responsible state for asylum applications. Both SIS and VIS are already accessible to law enforcement authorities, VIS even explicitly for the purpose of prevention of threat to internal security of any of the Member States. As from 20 July 2015, Eurodac will be accessible for law enforcement purposes as well.

Please note that the three systems all concern third-country nationals and that their registration into VIS and Eurodac, and partly in SIS, is unrelated to any criminal investigation or suspicion. Also note, that aside from the use of SIS for the European Arrest Warrant, or the API

Directive obliging air carriers to submit the data of their passengers to the border authorities of the EU, we do not have any large scale system with personal data on EU citizens. Dealing with the EU Regulation on the biometric passport, the centralised storage of biometrics of EU passport holders was explicitly rejected at the EU and national level. This rejection was based on security and privacy reasons.

What do we need (more)? Since the murderous attacks in different cities in Europe and most recently in Paris and Copenhagen, there is a legitimate call for effective measures to prevent these events and to trace people who are a threat to our security. The fact that politicians put both smart borders, but also the EU PNR system again high on the agenda seems not unrelated to those events. But when discussing these measures, we should be honest and ask ourselves whether data in the EES or a PNR system are really going to help us to prevent these security threats. Considering that the actors of these events in most cases were known to and followed by police or internal security agencies, should we not focus on what really caused the fact or circumstances that these attacks could not be stopped? And considering that many of these actors were EU citizens, some of them even never left their country, what is then the added value of access to EES for law enforcement purposes?

Although the Commission underlines that no decision has been taken yet about the necessity of access to law enforcement authorities, this option was included in the 2013 proposal, also making clear that this future use should be taken into account in the technical architecture. This might include the extension for data retention to five years, because law enforcement authorities consider longer time periods more useful for their work. In my view, it is clear that a decision on giving access to law enforcement authorities and the provision of technical tools, can only be taken <u>after</u> agreement on the necessity and proportionality of the EES/RTP for migration control as primary purpose. Therefore this needs careful analysis first. This not only safeguards the effectiveness of the measure, but also secures the legitimacy of the proposal.

3 Proportionality - fundamental rights

Now I come to the principle of proportionality, in view of the protection of the fundamental rights of data protection and privacy and also taking into account the case-law of the European

Courts. In the famous *Digital Rights Ireland Ltd.* judgment of 8 April 2014 (C-293/12), the CJEU found the Data Retention Directive was invalid because of the indiscriminate large scale collection of personal data, allowing data processing on persons without any link to criminal investigation, in the words of the CJEU 'practically the entire European population', without offering sufficient guarantees against misuse or unlawful use, and also because of a lack of prior independent or judicial control. On the relevance or meaning of this Court's decision for other legislative measures of the EU can be no doubt: before deciding and adopting the smart border proposal or EU PNR scheme, the criteria as set out by the Court should be taken into account, if we do not want that these measures to be annulled as well. Time is too limited to provide you with a general overview of DRI judgment or other case-law of the CJEU and the European Court for Human Rights, but let me stress that based on these judgments, other fundamental rights than data protection and privacy must be carefully considered as well, such as the protection of free movement of EU citizens and their third country national family members and the right to non discrimination.

4 Conclusions

I end with three concluding remarks:

First, effectiveness implies that before adopting new measures, the following questions need to be answered: for which goal do we need which tool: this questions also concerns the scope of the tool we are considering: if we know that aforementioned data systems or new proposals are only limited to non-EU citizens, but, in fact we are looking for persons with an EU nationality, or possibly even persons who never left their home country, how effective can new tools used at the borders be in order to detect and find persons who are a security threat?

Second, the principles of effectiveness and proportionality, imply that decision making should be based on **evidence based policy making**. This entails the evaluation of existing datasystems such as SIS, VIS and other mechanisms of data exchange. If we know that Eurodac will be evaluated in 2018, why not await this outcome first? And why do we seem to accept that Europol does not work, without analyzing how systems as the Europol Information System work and what can be improved? Before deciding on and investing in new measures, I would urge

national and European parliamentarians to investigate current gaps in cooperation and exchange of information first. This includes gaps at the European, but also at the national level.

Thirdly, when drafting new rules, it must be provided that not only the storage of personal data is limited to what is strictly necessary, but also the authorities who gain access. From the case-law of the CJEU we know that legislation leading to general surveillance systems are simply invalid, being disproportional. Sufficient safeguards must be incorporated to ensure accuracy, reliability, and the security of data processing. This means amongst others the choice for appropriate but no endless time limits and for secure and non-discriminatory use of biometrics. It also implies prior judicial control when necessary to safeguard the proportionality of access.

It is only by such a balanced and informed decision making that we can make the right choices and ensure the trust I mentioned before. Trust amongst national law enforcement authorities: that when exchanging their data, they know this information will not get lost or be misused. Trust between policy makers and law enforcement authorities: where the latter may trust they get useful, efficient, and reliable tools. Trust between policy makers and parliaments: where the latter can trust that technical tools are not developed before the necessity is actually proven and agreed upon during a democratic process. Finally, and most importantly, trust between law makers and citizens: where both EU and non EU citizens may trust that only those measures are adopted which are necessary and effective to protect their security without undermining their fundamental rights.