CONTRIBUTION FROM THE UK

Mobility, Security and Privacy

Developing and maintaining the European Union as an area of Freedom, Security and Justice is a fundamental objective of the Union (TEU Art 2) and is at the heart of EU citizens' interests. In order to achieve this objective, one of the key challenges Member States must overcome is the development of a coherent approach to safeguarding and promoting security, mobility and privacy within the EU. The simultaneous promotion of these concepts is often regarded as unachievable; and security, mobility and privacy are instead presented as mutually exclusive or antagonistic pursuits. In fact, the reality is rather more nuanced, and steps taken to improve specifically security, mobility or privacy can often also provide potential to leverage improvements in other areas. The key political question is whether and how the relationship between these concepts is likely to change over the coming years; and how national governments and the EU seek to communicate and explain such change.

Definitions

It is not always easy to define what we mean by security, mobility and privacy. Essentially, mobility here refers to the ease with which individuals can move across national boundaries for legitimate purposes; security means the safeguards in place to protect Member States; people and property; and privacy is defined in Article 8 of the European Convention on Human Rights (ECHR) as the respect for private and family life, home and correspondence.

Different approaches

It is easy to understand why these concepts are often viewed as antagonistic: indeed, some elements appear explicitly to incorporate "trade-offs". For example, Article 8 ECHR acknowledges restrictions to privacy are necessary in the interests (among other things) of national security and public safety, to prevent disorder or crime, or to protect the rights and freedoms of others. Furthermore, a common response to improving security in an increasingly mobile society is to require personal data from travellers in advance of their journeys and to strengthen borders and reduce crossing points, potentially impacting upon both privacy and mobility.

However, the idea that one or more element must be sacrificed in order to strengthen another is only one way to view the interplay between security, mobility and privacy. Instead of regarding these elements as the simple sides of a triangle where the extension of one side (or concept) has the effect of warping the others, it might instead be more accurate to depict the interdependent nature of security, mobility and privacy as a pyramid: the apex or point may lean more towards a particular concept at any given time, but is more properly reflected as the result of all three elements combined. In that context, they are not mutually exclusive. New technologies can assist in ensuring mobility, whilst at the same time promoting security. E-borders, for example, can create a more secure environment for EU citizens to enjoy their mobility.

Of importance in improving security, mobility and privacy, and helping to advance one alongside another, is effective and appropriately targeted data sharing between the relevant competent authorities of MS. Data sharing, which goes hand in hand with data protection, is usually associated with privacy matters but is in fact also intrinsic in promoting security and enhancing swift and efficient travel. The transfer of PNR data is an example of this, as are trusted traveller schemes. We need consciously to consider how the opportunities presented as the result of work in one particular field may be utilised to make progress in another, and data sharing will frequently provide the link between them.

Future JHA programme

The relationship between mobility, security and privacy, and the way data sharing can act as the catalyst for all three, will be critical for the post-2009 JHA programme. Advancements will require an examination of the extent to which new technologies might assist in enhancing security, mobility and privacy. Interoperability and privacy enhancing technologies (PETs) are both significant here. The compatibility of forms of identification from one State with the verification technology in others, for example, biometric passports and machine readers at immigration posts, is vital if Member States are to work together effectively and consultation must take place as early as possible in the design process. The practical ability - and desirability –, subject to necessary safeguards, of effectively linking databases in such a way that one State may easily obtain information in the database of another might also be explored.

PETs are known for the help they can provide in making breaches of data protection rules and violations of privacy technically more difficult. However, this technology also has the potential to undermine the work of law enforcement authorities. For example, PETs may be used by individuals carrying out illegal activities on the Internet to prevent their identity being discovered, and so any developments in this field must be analysed carefully.

It will also be important to agree on an intra-EU approach to mobility in a law enforcement context. We will need to find appropriate ways to ensure the removal of EU nationals involved in criminal activity from a host Member State to their own, while bearing in mind the basic principle of freedom of movement.

Questions around improving security, mobility and privacy are also relevant to the EU's relationship with the wider world – once again, data sharing mechanisms lie at the very heart of this. Key aims for data sharing with third countries must be to share data quickly when it is in the EU's interests to do so and to avoid any detrimental impact on international relations while ensuring the data transferred are protected to an appropriate standard. The EU must decide how it can share data most effectively with third countries, ensuring that the correct frameworks and safeguards are in place. Agreement on high-level principles of data protection might add value with countries unlikely to achieve adequacy overall, but with whom we need to share considerable law enforcement data, for example, the US.