Biometric passports

Biometric passports have progressively become the global standard since the 9/11 terrorist attacks, but questions continue to be raised as to how secure they really are. Weaknesses have been observed on the technological side and in the procedures for issuing passports, as well as in the reliability of the basic documents and data required to obtain a passport.

International context after 9/11

Following the September 2001 terrorist attacks and the adoption of the Enhanced Border Security and Visa Entry Reform Act (2002), the United States decided to strengthen the reliability of passports and visas. They have also required third countries to make them machine readable, including electronic chips storing biometric identifiers as recommended by the International Civil Aviation Organisation - ICAO (see the Machine Readable Travel Document (MRTD) Programme outlined in ICAO Doc 9303 and its supplements, with reference to passports, visas and ID cards). The biometric identifiers chosen by the US are digital versions of the facial image and fingerprints (which, contrary to the iris, may also be valuable from a forensic perspective). Moreover it has been recommended that even minors should have their own passport (under the ICAO principle 'one person, one passport'). The US has led the way, progressively making all these requirements mandatory for third-country nationals wishing to travel to the US even under the visa-waiver programme.

The EU framework

The EU has followed a similar path: Council Regulation (EC) No 2252/2004 sets out standards for security features and biometrics in passports and travel documents issued by Member States (MS). This regulation was amended in 2009, at which time a number of issues were raised by the EP. During a January 2009 parliamentary debate, several MEPs expressed reservations about the mandatory collection of children's fingerprints. The Rapporteur Carlos Coelho (EPP, Portugal) stressed the improved security linked to the use of biometrics. However he made clear that the same level of security should be followed for each link of the "security chain" leading to the issue of a passport. Thus, security needs to apply to the administrative procedures, to the public officials involved and to the "breeder documents", on the basis of which a passport is delivered. This requirement arises from a 2009 joint statement of the EP and Council, stressing that "breeder documents" may have fewer security features than the passport itself, thus weakening the whole security chain which could be subject to forgery or counterfeiting.

The impact of the use of biometric technologies not only concerns issues of privacy. There are also problems linked with the interoperability of different systems (e.g. use of different security systems may lead to passport-holder's data being compromised). On the general issue of biometrics, even national constitutional courts have taken a strong interest as shown by the French Conseil Constitutionnel's Decision on 22 March 2012 abrogating part of the new French Law on Identity Protection.

Open issues on enhancing security

In compliance with Article 5(a) of Regulation 444/2009 and Article 2 of the Regulation amending the Common Consular Instructions, the European Commission must publish, not later than 26 June 2012, an independent study on the treatment of breeder documents by the MS (see also the EP position of 14 January 2009). The EP's concerns have been echoed by a political source, which claims that in France more than 10% of biometric passports in circulation were fraudulently obtained. Similar concerns on the security of the passport-issuance chain have also been raised by a US Government Accountability Office (GAO) report denouncing the weaknesses in the State Department's passport-issuing processes. The subject of breeder documents is due to be discussed at ICAO level from 17 to 19 April 2012 in a regional seminar on Biometrics and Border Security.