The role of law, ethics and justice in security practices

Gloria González Fuster, Serge Gutwirth and Paul de Hert
Free University Brussels

This position statement aims to identify key subjects for the future of security research relative to the themes of law, ethics and justice, with special attention to the questions of globalisation, technology, risk and norms of conflict. In general terms, we believe that the widespread implementation of identity-based security practices demands responses that include a re-framing of certain key assumptions of the right to privacy and to data protection, but that it cannot be limited to it.

Globalisation
- The globalisation of security practices represents a fundamental challenge for data protection law, notably in regards to its effective implementation. Transborder data flows, combined with the global tendency to support ‘enhanced information sharing’ [especially in the United States (US) and in the European Union (EU)], constitute an extremely difficult challenge for the effectiveness of fair information practices, as well as for liability regarding compliance with data protection law. Coordinated approaches are a key factor to enhance implementation in this context. At the European level, the design of solid rules for onward transfers to third countries of police and judicial data is a prime concern.
- Biometrics and ICT allow for the re-configuration and progressive deterritorialization of international borders. This virtualization of borders can have positive implications for citizens, if accompanied by measures that empower them, i.e. by increasing capacity of reaction against unjust decisions under electronic travel authorisation systems. However, this transformation of the borders does not represent a removal of barriers. ‘Outsourcing’ also conveys borders where they were non-existing or from where they had been removed. This displacement of borders goes hand in hand with the displacement of border controls, which expand accordingly. By following the individual, border control tends to transform itself into (semi)permanent control. Limits to this expansion must be set urgently.

Technology
- The global tendency towards ambient intelligence security enforcement scenarios, relying on the massive collection and processing of (personal and non personal) data in combination with data mining and profiling techniques, highlights the fragility of data protection law as a tool to control surveillance. Lawful collection and processing of personal data does not prevent per se unethical practices deployed in the name of security, or unjust decisions based on them. Arguably, the alleged need ‘to mobilize information to prevent terrorism’ and equivalent instructions frontally


15 For instance, through wide access to entry/exit databases.

contradict fundamental principles of data protection law (such as the minimization principle). A general framework to limit surveillance needs to be designed, in which the enabling force of (transparency-inducing) data protection regulation is complemented with more clearly defined (opacity-ensuring) restrictive principles.

- The importance of the recent judgment of the German Constitutional Court on the constitutionality of secret online searches of computers by government agencies\textsuperscript{17} could be capital, as it establishes a new "basic right to the confidentiality and integrity of information systems" as part of the general personality rights constitutionally protected in Germany. The Court limits exceptions to the right to specific cases where exist "factual indications for a concrete danger" for the life, body and freedom of persons or for the foundations of the state or the existence of human beings, and declares that measures can only be implemented after approval by a judge. Moreover, secret online searches must in any case be constrained by ad-hoc technical measures not to interfere with "the core area of the conduct of private life". This landmark ruling can potentially be as influential as 1983 recognition by the same Court of the "right to informational self-determination".

- Technology plays a crucial role in the implementation of targeted, 'smart' sanctions, which represent a beneficial development for security inasmuch they: a) take full advantage of technology to minimize negative humanitarian impact (are as 'smart' as possible); and b) are legally construed in full accordance with human rights. Targeted sanctions must be strengthened notably through: periodic review, procedural fairness, and judicial review of decisions.

- Use of technology cannot be separated from techniques used to process information. The relation between technology and law has been recurrently explored (i.e. through the notion of 'code'). However, much is still to be said on the relation between statistical analysis techniques and actuarial strategies deployed in the name of pro-active surveillance. Emphasis should be placed on the need to respect the principles of criminal law (i.e. the presumption of innocence), to democratize those practices, increasing the transparency of inferences and openness of procedures.

**Risk**

- The notion of risk has been conceptually stretched to fit different perceptions and uses, becoming increasingly vague and malleable. Instead of a clear-cut shift in focus from ‘risk management’ to ‘risk deterrence’, the process could be envisaged as a dangerous blur, in which other notions are also pressed to contribute to semantic distortion (such as the ‘precaution’ notion exported from the ‘precautionary principle’ to proactive security policies). Exploration of the values underpinning the use of these notions in different specific contexts is necessary.

- Intrinsically linked to risk-analysis, data mining and profiling techniques are becoming widespread and are on the verge of official support at EU level through the European Passenger Name Record (PNR) system.\textsuperscript{18} Profiling practices transform ‘statistic’ or ‘actuarial’ categories into legal notions with specific negative effects for those falling under them (such as ‘risk passengers’)\textsuperscript{19} to be further questioned or refused entry, or potentially worth investigating persons to be further controlled\textsuperscript{20}. At this crucial moment:

\textsuperscript{17} Published on 27 February 2008 (Online-Durchsuchung, 1 BvR 370/07; 1 BvR 595/07).

\textsuperscript{18} See: Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007.


\textsuperscript{20} Other expressions used are ‘persons requiring further examination’ [see Proposal mentioned in note 7, Article 3(3)] and ‘high-risk passengers’ [European Commission (2007), Accompanying document to the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes: Summary of the
a) there is a need to legally and ethically assess the legitimacy of those techniques to determine what is a ‘risk’, which ‘risks’ require further attention and which ones do not, as well as the proportionality of the system considering the major interference with privacy that it represents and the actual value of statistical methods of prediction;

b) justice considerations oblige the legislator to ensure that no discrimination takes place during the process of distinction, classification and categorization inherent to any data mining and profiling practices; and

c) law should grant to those marked as ‘risk passenger’ specific rights equivalent to the ‘rights of the suspect’. The ‘rights of the risk passenger’ must include access to judicial revision of the decision and redress.

This debate cannot in any case be confined to the right to privacy and the protection of personal data, even if the magnitude of the collection and processing of personal data does call for major measures ensuring the security of data and effective fair information practices (limits for the duration of retention, purpose limitation, filtering of sensitive information, exercise of data subjects rights).

**Norms of armed conflict**

- Priority is to be given to better defining the right to have access to justice, including the right to a fair trial and the right to an effective remedy. The undergoing European courts review of *ius cogens* is especially relevant in this sense. The European Court of First Instance case law on ‘terror blacklisting’ (cases of Kadi and Yusuf) and subsequent appeals have fed the discussion on the qualification of certain human rights as norms of *ius cogens*. While the right to privacy was not invoked in those cases, its possible qualification as *ius cogens* should be examined in detail, taking into account that the protection of privacy can either be ensured as a separate right or subsumed under other rights such as the right to dignity or personality rights, as in certain EU Member States.

- Specific technological developments require special attention in the context of armed conflict. It is the case notably of biometrics and bio-data banks. United States military scanning of fingerprints and iris of Iraq population offers a powerful illustration of the delicate problem, as the consequences of function-creep of the collected data could be catastrophic. The debate on biometrics in unstable situations needs however to take account also of its benefits for identification and therefore access to rights.

---

21 Case law such as the European Court of First Instance judgment in José María Sisón vs. Council case (Case T-47/03) is also to be considered, concretely on the rights of the defence and the right to effective judicial protection.