Universität für Bodenkultur Wien (BOKU)
University of Natural Resources and Life Sciences, Vienna

Institut für Rechtswissenschaften
Institute of Law

Report

Artificial Intelligence in the Age of Terrorism.
A Tipping Point for Constitutional Law.

Prof. Arianna Vedaschi | Bocconi University

Chiara Graziani | Bocconi University, University of Genoa

13 December 2019

In the post-9/11 era of jihadist terrorism, the security situation has changed dramatically. Terrorism, by its very nature, follows no clear pattern, so predicting future incidents seems almost impossible. In addition, it is difficult, if not impossible, to punish terrorists. Therefore, preventing terrorism altogether becomes all the more important. During their LTS lecture, Prof. Arianna Vedaschi and Chiara Graziani explored the opportunities and legal challenges of using artificial intelligence (AI) to prevent terrorism.

Maintaining a high level of security in the face of terrorist threats has two sides to it, an objective one and a subjective one. Facing terrorism is not only about *making* people *safe*; it is about making them *feel safe* as well.

Mass surveillance (acquiring large amounts of data) and AI (looking for patterns in data) have already been used for both these purposes. Are they compatible with protecting fundamental and human rights, however? As always, tensions arise between security interests and individual liberties. Is the current proportionality test employed by the European Court of Justice (ECJ) able to resolve that tension?

There are several reasons for these concerns. First, like humans, AI can make mistakes and, in doing so, can infringe human rights. Secondly, AI could discriminate against certain groups of people. This could be due to biased input, due to certain patterns being discerned by AI itself, or due to the sheer fact that AI is not equipped to do equally well at recognizing the faces of people in different groups. Thirdly, there seems to be a lack of transparency and responsibility. Who is the agent in charge of an automated decision, and how can we challenge the outcome of an algorithm? Additionally, a shortcoming of AI so far seems to be the context-dependent interpretation of a situation.

Is mass surveillance hence incompatible with human rights? No, or, at least, not per se, says the ECJ. In its decision on Passenger Name Records (PNR) data, the ECJ held that mass surveillance is possible in principle, provided the provisions are specific and precise, and that decisions are reviewed by a human being. In practice, however, AI cannot be used without infringing human rights.[1]

Categories of counter-terrorism measures. There are a variety of ways in which AI and big data (which is not the same but often comes into play in conjunction with AI technology) can be used to counter terrorism.

Meta-data are an important part of big data analysis. They contain information about other data. As such, they are neutral. If combined with other (meta-)data, however, they can be used to profile people with the aim of predicting and preventing events like terror attacks. **Facial recognition technology** creates a biometric template based on a person's facial features. Screening faces in public and comparing them to a database allows for the automated identification of individuals.[2] **Content on the internet** can be screened with the help of AI to look for and prevent dangerous activities. As this is regularly also done by private actors, the question of how to regulate public–private-partnerships in this area is highly topical. Closely related to this are attempts to **anti-radicalize** individuals showing suspicious behaviour online. Strategies like the *redirect method*[3] identify users who are susceptible to radicalization and redirect them to content with a more balanced view on a certain topic. Lastly, AI can be used in the **financial sector** in order to hinder the financing of terrorism. There have been different legislative acts in the EU related to money laundering. However, using AI to conduct these activities has not yet been addressed, leaving the decision on whether and how to use it to financial institutions.

Constitutional law analysis. Making use of modern technology allows for higher standards of safety. For a constitutional lawyer, however, several questions arise that need to be addressed.

Principle of Proportionality. Several provisions of EU law limit restrictions on the enjoyment of individuals' rights and liberties. According to Article 52 CFREU, any limitation on rights and liberties must be enacted by law. It also must target a legitimate aim and be necessary for that aim. Finally, the provision must be proportional, meaning that the severity of the infringement and the gains from the restriction must strike a certain balance. In several decisions, the ECJ has declared that mass surveillance fails the proportionality test. The indiscriminate storage of communications data, for example, has been deemed to be excessive.[4]

---

[1] *PNR,* Opinion 1/15 of the Court (Grand Chamber) of 27 July 2017, ECLI:EU:C:2017:592.
PNR is about automated risk assessments of airline passengers based on information they provide.
[2] The use by the UK police of facial recognition to identify individuals in crowds was deemed to be legal by the Cardiff High Court: EWHC 2341, 4 September 2019.
[3] https://redirectmethod.org/.
[4] *Digital Rights Ireland*, Judgement of the Court (Grand Chamber), 8 April 2014, ECLI:EU:C:2014:238.

N**on-discrimination.** Using face recognition algorithms, AI can be used to differentiate between suspect and non-suspect individuals. As AI is not equally well equipped, for instance, to recognize male as opposed to female faces, it could discriminate against certain groups of people. Also, biased input to self-learning machines leads to biased learning outcomes.

Expanding role of the private sector. The private sector often has more resources and more advanced technology available than the public sector. This could lead to the outsourcing of functions that are considered to be essentially state functions. A quasi-judicial role might be handed over to private parties. There are practical arguments on the side of private actors. On the other hand, a lack of transparency and accountability speak against them. Powerful private parties dealing with these issues would also take over the task of defining terms. Outsourcing of vital functions could also pose a threat to our concept of *state sovereignty*. Lastly, it is doubtful whether private actors who operate on the basis of profit are appropriate to provide for public security.

Lack of traditional sources of law. Besides hard law (e.g. Art 7 of *Directive 2016/681*) and institutional soft law sources (e.g. *Guidelines on Artificial Intelligence and Data Protection* by the Council of Europe), private soft law emerges as the real master of AI and counter-terrorism. The pivotal role of private soft law is especially problematic as it cannot be subject to judicial review.

A very lively discussion following this multifaceted talk proved the importance of this topic. The questions ranged from generally contesting AI's ability to interpret complex human language to the sensitive issue of classifying potentially radical users. One audience member mentioned a very recent decision by the Austrian constitutional court pertaining to mass surveillance. The court had declared parts of the so-called *Safety Package* unconstitutional, in part because the indiscriminate surveillance also allowed for discovery of minor criminal behaviour – in the light of that, the infringement of fundamental rights was not proportional.[5]

Way forward? Given the potential of AI and big data for counter-terrorism, renouncing these tools does not seem to be an option. The threats to human rights are obvious as well and, so far, mass surveillance has been judged to be disproportionate by the ECJ. Will an adaptation of the proportionality test lead to a reconciliation of conflicting interests? Only time – and society's preferred balance between security and freedom – will tell.

Johannes Huber, January 2020

[5] Verdict of the Austrian Constitutional Court of 11 December 2019, G 72-74/2019-48, G 181-182/2019-18.