**Virtual Race, Tech and Borders Expert Group Meeting: 16 – 17 June 2020**

**Jean Monnet Professor *ad personam* Elspeth Guild, Queen Mary University of London**

**Mapping the Actors in New Information Technologies and Border Enforcement**

The changing face of border controls is largely being driven by electronic developments which include electronic port-of-entry gates tied to databases and computer programmes designed to identify who should be able to enter a state and who should not. Much of these developments are packaged under the heading: Artificial Intelligence (AI). It is based on the promise that machines can mimic human intelligence through the use of algorithms and driven by data. As a branch of computer science, it includes many subfields such as machine learning/intelligence which all have in common the attempt to analyse environments using either predetermined rules and related algorithms, or machine learning models designed to recognise patterns with the objective of making or assisting in the making of decisions based on those analyses. AI becomes an issue for law in a number of ways such as consumer protection, product liability or negligence. Here I will examine only one challenge which AI constitutes for law – the protection of human rights, and in particular the right to privacy.

AI has advanced rapidly in the 21st century because of the growth in technical capabilities which have made available massive amounts of data, and the maturing of ideas that has led to ever more sophisticated algorithms. AI technologies have become the driving force behind online global services that have been commercialised by the rapidly concentrated technology industry, resulting in the increasing profitability of AI-based approaches to problem solving. Governments have been increasingly interested in using AI technologies for policy objectives in border controls, immigration, criminal justice, security surveillance, and – as the responses to COVID-19 crisis demonstrated - responding to a global health crisis. The promise of efficiency and effectiveness in decision-making process that otherwise could not be achieved by human agents has been one of the driving forces behind the AI boom.

The way state authorities make decisions which affect individuals (eg border controls, immigration, social security entitlements, criminal prosecution, covert surveillance) is closely regulated by law. The full power of the state is exercised in its decision-making capacity including over the lives of individuals. The consequences of any decision by a state authority on a person’s life may be enormous which explains the duty of state authorities to give grounds for their decisions. Challenging a state decision which has negative impacts on a person depends crucially on the strength of the grounds given for the decision. It is also costly, time consuming and difficult for the individual. For these reasons, Council of Europe states signed and ratified a convention in 1981 which prohibits automated decision making.[[1]](#footnote-1) Yet, the availability of data and rising collaboration between the big technology companies and the public sector are raising renewed concerns over the protection of the right to privacy, non-discrimination and the compatibility of AI-based solutions with data protection law, in particular in respect of automated decision making.

The starting place of AI is the availability of data. Without data there is no AI – to develop AI software applications to analyse environments, two things are needed: (1) objectives set out by humans, what is to be achieved? (2) a lot of data on the basis of which the application can be trained to search for specific characteristics or recognise patterns. Both of these requirements raise issues in law. First, both the objectives established may constitute prohibited discrimination either direct or indirect and the data sets used may be discriminatory. For instance, using an AI tool to search for ways to make decisions on visa applications to reduce the risk of people overstaying will discriminate on the basis of the state’s decision on which countries’ nationals are required to have visas and which are not. This may be a justifiable form of discrimination, but it needs to be argued. Similarly, using data sets which are based on a norm which is male will discriminate against women, searching for terrorists among data sets of men between particular ages or on the basis of religion may also be flawed.

The most profound challenge to AI, however, is the right to privacy. This is because this right potentially deprives AI developers of access to personal data which may be essential to the development of their products. The right to privacy is guaranteed, amongst other ways, by state regulation of data protection. The Council of Europe and European Union principle is that the individual is entitled to consent to the use of his or her data in each application of its use. To ensure that data is only used in accordance with the individual’s express consent, there are strict rules of the duty to destroy personal data as soon as the purpose for which it has been collected has been fulfilled. A number of judgments of the European Court of Human Rights have been exactly about this duty to destroy data. European states have appeared very reluctant to destroy personal data which they have collected about individuals – finding endless excuses to hang on to it – national security being one of the favourites as among the least susceptible to intense judicial investigation. State authorities, when unchallenged, succeed in collecting and retaining enormous quantities of personal data, making these data sources particularly attractive to AI developers. The incentive to work together which the AI developers present to state authorities is the promise of quick, accurate and very cheap assessment of individual claims – be it for social benefits, immigration status or surveillance within and outside the criminal justice systems. For the AI developers it is access to personal data.

The state, however, is also critical to access for AI developers to data collected by the private sector. Data protection rules for the private sector require the destruction of data as soon as possible after use. Only state authorities have the capacity to create exceptions to this rule of destruction which allows the retention of data and thus is potential availability to AI developers. Again, the interests of some state authorities and AI developers converge. If the state can be convinced to create obligations on the private sector to retain data (rather than destroy it) and to make it available to either the state directly or to its agents (in the form of AI developers) massive amounts of data become available for training AI tools. The EU saga on the fate of the Data Retention Directive is a good example of this controversy.[[2]](#footnote-2)

The Snowden revelations of mass surveillance around the world carried out by a US state agency (the National Security Agency) published in 2013 destroyed public complacency that mass surveillance coupled with AI tools was anodyne. The detail of the revelations and the different AI tools which were being used to analyse massive amounts of data became the focal point of concerns about privacy and data protection. It proved to be a chilling example of pervasive state surveillance, the source of which had been the data collected by the private sector and passed to the public sector.

The actors which are critical to these developments are:

1. The technology companies which sell uses for their programmes to state authorities;
2. Immigration ministries which purchase programmes which they can run through multiple state data bases on individuals to find individuals in respect of whom enforcement action will eb taken (an example of this is the so-called Windrush scandal in the UK;
3. Border guards and their authorities: personal data which is gathered at borders can be extensive. That gathered in visa and other related procedures is even more voluminous. The use of no fly lists and other technological tools to use databases of personal information to make border control decisions is critical.
4. Passenger Name Records: the travel industry has consolidated in five main companies the personal data of their customers who are travellers. These are called PNR. Since 2001, and begun in the US, access to PNR data has been demanded by US border authorities in order to search for unwanted travellers. This has led to a web of international agreements on PNR permitting it to be transferred from the private sector in one country to the public sector in another. It is used for the purpose of running programmes to determine which travellers should be lowed entry. But many of the travellers whose PNR data is transferred to states under these agreements are nationals of the state and without PNR data the state would have much less data on their own nationals who travel.
5. Agreements on exchange of immigration related information: interior ministries among some of the Five Eye countries have entered into agreements to exchange information acquired in the process of border, immigration and asylum procedures with one another. The most (legally) developed is the US- UK Agreement but the database is held in Australia. The database provides access to the national databases on border, migration and asylum including access to biometric data. This area is under researched.
6. The arguments: serious crime and terrorism: national security.

1. Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, 28 January 1981, ETS 108, available at: https://www.refworld.org/docid/3dde1005a.html [accessed 21 May 2020] [↑](#footnote-ref-1)
2. Lynskey, Orla. "Data Retention Directive is Incompatible with the Rights to Privacy and Data Protection and Is Invalid in Its Entirety: Digital Rights Ireland, The." *Common Market L. Rev.* 51 (2014): 1789. [↑](#footnote-ref-2)