Predictive Policing and the Automated Suppression of Dissent

Following a special workshop convened by the Media Policy Project on 'Automation, Prediction and Digital Inequalities', Lina Dencik, Lecturer in the School of Media, Journalism and Cultural Studies at the University of Cardiff, reflects on some of the implications of using large data-sets for policing purposes.

The collection and analysis of large data-sets for the purposes of policing forms part of a broader shift from 'reactive' to 'proactive' forms of governance. In these, state bodies engage in the analysis of 'big data' to predict, pre-empt and respond in real time to a range of social problems. However, we often do not know or understand how, and to what extent, different actors make use of big data in relation to social and political issues. Although big data is often said to deliver more efficient, rational and objective decision-making, the uses of big data for governance also introduce some fundamental challenges to the relationship between state and public, as well as notions of accountability and the practice of citizenship.

The use of big data and predictive analytics has emerged in the context of state conduct which is increasingly security-oriented and in an environment of perceived threats, in conjunction with the rapidly developing technological capacity to monitor and track human behaviour. The Snowden revelations, for example, illustrate in detail how big data technologies have become integral to a state-corporate regime of surveillance that has now extended into almost all aspects of everyday life. With a (state) security-centered discourse at its core, big data has emerged as a corner-stone of a surveillance-based mode of governance in many Western countries. The Snowden leaks revealed the United Kingdom as one of the most intrusive surveillance regimes in this regard.

Developments in policing, and protest policing in particular, have been significantly shaped by this wider context. Advances in 'Open Source Intelligence' (OSINT) situate current policing practices firmly within the big data-security nexus. OSINT gathers intelligence on the basis of collecting and analysing publicly available data (much of which is taken from social media activity) in order to predict and pre-empt crime and disorder. Concerned with the possibility of discerning patterns in human behaviour and identifying potential risks and threats, this form of intelligence gathering has become a growing part of police practice, and has come to inform strategies and tactics for the policing of protests and demonstrations.

As we have found in our research, the collection and analysis of social media data is perceived by police to be a more proportionate and fair form of intelligence gathering than other tactics, and provides a substantial resource for 'situation awareness', particularly in the lead-up to major events such as demonstrations and protests. The programmes and tools employed by the police for OSINT are predominantly developed by the commercial sector, and are often designed for marketing purposes rather than having been developed in-house by the police.

Whilst OSINT is situated within a hub of both human intelligence and existing databases to inform police strategies and tactics, these automated aspects of protest policing introduce some important questions about the possibilities for dissent. We are confronted here with an increasingly complex protest terrain in which blurred definitions of public/private online communication feed into not just the act of dissent in the present, but also the perceived intent of dissent in the future. This creates a relationship between data and publics based on 'mirroring', in which online activity is understood to be representative of human behaviour and intent. In other words, we are our data profiles.

This assumption is a necessary pre-requisite for the use of big data as a mode of governance, yet has little grounding in reality. It denies both agency and distortion. What is more, perceptions of threats become linked to the technical determination of risk based on decontextualised forms of data that are inevitably inconclusive. Ascertaining the probabilities of something happening in such a context will be riddled with high levels of uncertainty and unpredictability that can easily be interpreted as risks. In other words, what is (and inevitably will remain) 'possible' becomes interpreted as 'probable'. In a security-centered political environment, pre-emptive measures on this basis can therefore be endlessly justified. This also provides an environment conducive to over-intervention, such as the proliferation of extensive anti-radicalisation programmes, for example.

This is the case because, as Massumi argues, with an operative logic of pre-emption, the problem becomes one of perception and time: how to perceive what has not yet emerged; how to perceive potential occurences. Massumi goes on to argue that this problem comes to rely on the production of 'affective facts': threats may be 'real' (i.e., correspond to an actual danger), or they may be *felt* into existence (if I am afraid, I felt a threat). It is immaterial whether these threats were present or not, they come from the future and so the threat always *could have* occurred. With developments in big data we see other 'facts' intermingle with these 'affective facts'; facts that instead rely on the production of algorithmically produced patterns and abnormalities in data.

Unlike the politicised terrain of human feelings, this provides an avenue for the 'scientification' (or, rationalisation) of the operative logic of pre-emption, thereby facilitating a seemingly mathematical foundation for actions that can outsource responsibility to automated processes, and thus both *depoliticise* and dehumanise pre-emption. This attributes great value to (big) data in the management, control and suppression of dissent within the operative logic of pre-emption. It also highlights the need for us to continue to stress the agency and politics that underpins it.

This blog gives the views of the author and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics and Political Science.

This post was published to coincide with a workshop held in April 2016 by the Media Policy Project, 'Automation, Prediction and Digital Inequalities'. This was the third of a series of workshops organised throughout 2015 and 2016 by the Media Policy Project as part of a grant from the LSE's Higher Education Innovation Fund (HEIF5). To read a summary of the workshop, please click here.

June 1st, 2016 | Digital Inequalities, Featured | 1 Comment