**Artificial intelligence and the control of ‘algocracy’ in security issues**

*Hager Ben Jaffel and Didier Bigo*

For the past decades, security bureaucracies and the like – ranging from police and intelligence services to the military and technology companies – have progressively harnessed artificial intelligence to frame enhanced ‘solutions’ to security problems. Conducting counter-terrorism, cyber-security or a military operation today increasingly involves AI driven modes of surveillance and control, including machine learning, crowd behavior analysis, pattern detection, and bulk data collection among others. This shift in identifying behavioral patterns, detecting ‘anomalies’ online, and profiling ‘suspicious’ individuals has accelerated the same old rationale underpinning security actions: anticipating and even predicting the future.

The rise of algorithms – a ‘mathematical recipe formulated as a finite set of rules to be performed systematically’ (Martignon 2001: 382) – has made possible the progressive introduction of AI in security practices. As Amoore and Raley note, algorithms can ‘filter, expand, flatten, reduce, dissipate and amplify what can be rendered of a world to be secured’ (2017: 5) while embody new forms of authority in their own right (ibid). In sorting out data, categorizing ’abnormal’ behavior and activities and orienting security responses accordingly (Kaufmann et al, 2018), algorithms supervise and conduct security professionals’ actions and the ways in which they govern others, amounting to what Aneesh terms ‘algocracy’. Despite this, little has been said about the control of ‘algocracy’, of those who design and command algorithms – software companies, programmers, developers, among others – and their end users, such as data analysts, intelligence units, and other tech-people. If AI driven tools are usually portrayed as self-automated functions, the formulas, codes and resulting algorithms behind AI are determined by the practices of their producers and users as well.

The CJEU stated on 6 October 2020 in a court case led by Privacy International that the national legislation requiring providers of electronic communications services to disclose traffic and location data to the security and intelligence agencies exceeds the limits of what is strictly necessary, and cannot be considered to be justified within a democratic society, even in the name of national security. This clarifies previous judgements on intelligence services’ ability to collect, and use via algorithms, lists of data suspects generated through data retained by internet providers, and engages with the limits that they have to respect. The immediate answer by some services may be to activate even more real-time capture flows and predictive analytics, but this headlong rush to avoid control on data is not a solution. ‘Algocrats’ will be the next to be obliged to explain their practices to the courts. This struggle between the social use of technologies and judicial controls over predictive analytics will be at the core of our transdisciplinary discussion.

To address the stakes of the control of ‘algocracy’ in security matters, this workshop will invite papers working from distinct epistemological and ontological perspectives to examine the professionals and practices behind AI in order to understand how AI is enacted – for instance, what are the logics, assumptions, routines behind their performance – and hence its implications for the control of ‘algocracy’ in terms of transparency and accountability.

Possible questions for participants to reflect upon include the following:

* What are the stakes in ‘algocracy’?
* Who are the professionals and what are the practices of ‘algocracy’?
* Who are those who manufacture and use algorithms and AI? How do they understand them?
* What are the end products of AI-oriented tools (i.e. watch lists, diffusion of rumours, etc)?
* Is comprehensive, integral and maximum security possible and desirable?
* How can we control AI driven security methods, especially the ones on predictive analytics?
* How can oversights and courts impose limits on these practices endangering freedom by their in-built surveillance and democratic understanding of the limits of actions done by the secret services?
* What are the modalities of control to be foreseen, in technological (privacy-oriented AI), legal and political terms?