Using procurement instruments to ensure trustworthy AI

A position paper by the AI Now Institute, City of Amsterdam, City of Helsinki, Mozilla Foundation and Nesta.

1. The challenges faced by the public sector

Public sector authorities are increasingly seeking to capture the opportunities offered by AI-enabled systems to improve the provision of services to the public.

However, public sector authorities and the wider general public have justified concerns over data governance, privacy, bias, discrimination, accountability, transparency and the overal opacity of AI-enabled systems. A landmark ruling by the District Court of the Hague in the Netherlands on the use of an algorithmic risk model (SyRi) to detect social benefit fraud illustrates how public sector use of AI-enabled systems in itself can result inadvertently in new risks or harms.

Public sector authorities further often rely on the expertise, and previously developed models, of technology providers and may lack the necessary skills to fully understand or audit AI-enabled systems. In those rare cases where flaws are found, public sector authorities are often faced with 'vendor lock in'. The more training an algorithm gets using the data provided by the city and its citizens, the more valuable and useful it gets for its user. This makes the user dependent on the vendor, as they are unable to use another vendor without substantial switching costs. At present, the vendor often holds intellectual property rights in the system, and can ward off liability or requests for information using IP, trade secrecy and broad indemnity clauses.

Finally, because there are no clear rules about public oversight of tech vendor contracts, government agencies may procure and use tech that could impact large numbers of people without ever needing to notify the public. Any use of an AI-enabled system by public sector authorities could be used in such a manner that significant risks can occur. As a result, citizens should rightfully expect a high level of transparency and accountability when those systems are procured.

2. Going beyond guidelines

Some governments have taken steps to create guidelines for government agency procurement of AI-enabled systems. In the U.K., the government published a "Guide to using AI in the Public Sector" to enable public agencies to adopt AI-enabled systems in a way that benefits society. Organisations like the World Economic Forum or Data Ethics have further elaborated useful guidelines specifically focused on procurement policies.

The Cities Coalition for Digital Rights, a coalition of 39 cities in the EU and the US, are taking steps to ensure that cities use technology in an open and transparent way. In its declaration, the coalition affirms several broad principles including the transparency, accountability, and non-discrimination of algorithms. This means in practice that the public "should have access to understandable and accurate information about the technological, algorithmic, and artificial intelligence systems that impact their lives," and they should be able to "question and change unfair, biased or discriminatory systems."

However, these guidelines have largely not been implemented. There is an urgent need to go beyond mere guidelines, and provide clarity on fundamental rights safeguards, testing requirements or modelling requirements when public sector authorities decide to procure AI-enabled systems.

3. Standard Contractual Clauses for Municipalities for Fair Use of AI-enabled Systems

Procurement and contract conditions are both very powerful and practical instruments for public sector authorities to assure AI-enabled systems comply with fundamental rights and democratic values. In Amsterdam 2 billion and in Helsinki 2.5 billion euros is annually spent through procurement.

The EU's High Level Expert Group (AI HLEG) recommended to strategically use public procurement to fund innovation and ensure trustworthy AI, by introducing "clear eligibility and selection criteria in the procurement rules and processes of EU institutions, agencies and Member States that require AI systems to be trustworthy".

The next step is to begin defining what these procurement standards should be and to operationalize and standardize their use. In October 2019 the City of Amsterdam has - together with the City of Helsinki and external experts - started this process by drafting standard contractual clauses which attempt to include such criteria. They are intended for use in those situations where a municipality purchases an AI-enabled system from an external supplier. The draft contractual clauses cover all algorithmic systems that when used by the Municipality, may affect citizens of the municipality, visitors to the municipality, or companies established in the municipality to a significant extent. In such an event, the municipality wishes to implement certain safeguards, including detailed procedural transparency in all cases and technical transparency in case of a mandatory cooperation of the contractor with an audit or other type of inspection.

There is also global momentum on this issue. In December 2019, in response to the New York City Automated Decision Systems (ADS) Task Force, an NGO coalition recommended a series of protections to be included in vendor contracts. These include specific waivers to trade secrecy; provision of training modules by vendors to help government staff understand the systems and to collaborate in developing public-education materials; restricting broad indemnity clauses; mandatory validation studies and an open, competitive bidding process for these arrangements.

4. Call to action: use procurement policies to encourage trustworthy AI

These are concrete examples of how public procurement policies can be leveraged to support the development and uptake of trustworthy AI. However, we hope that other public sector authorities, including the EU, will follow suit. When public procurers represent a critical mass, they can create new standards and new demands for certain safeguards in AI-enabled systems.

That's why we ask the European Commission to

- Adopt similar contractual clauses in its own procurement and tendering processes
- Facilitate the development of common European standards and requirements for the public procurement of AI-enabled systems