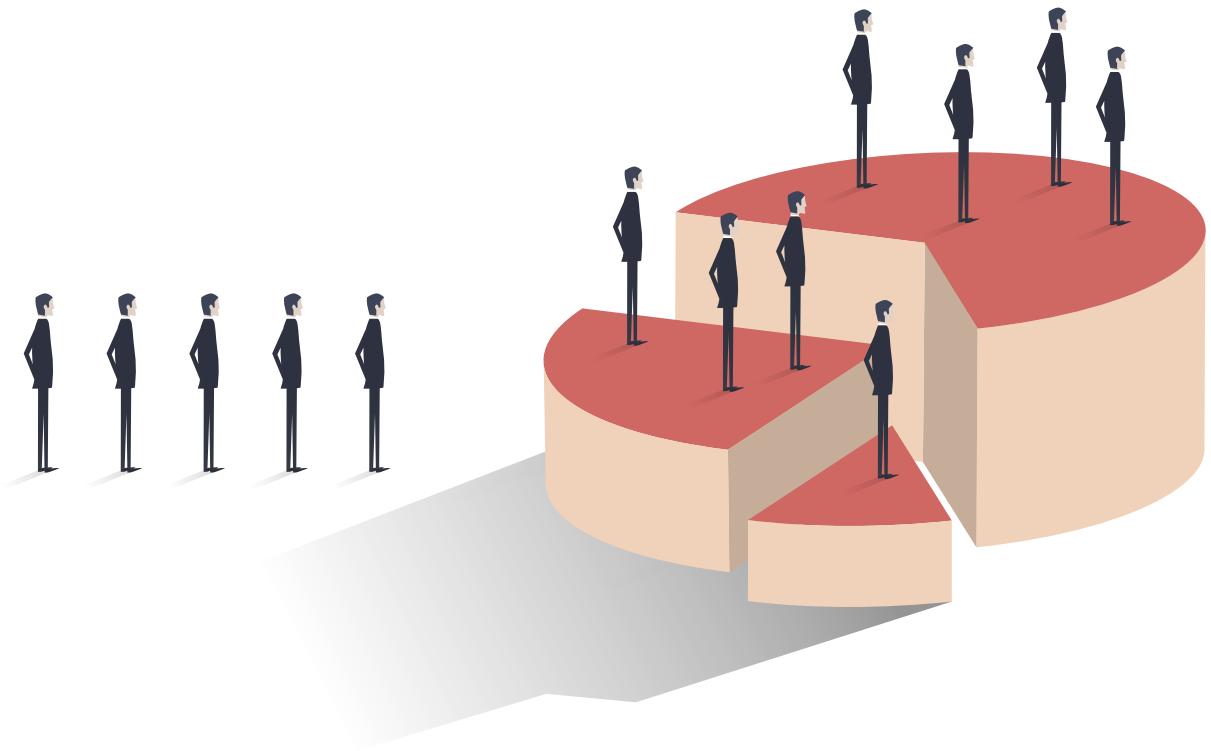
Anton Ekker – Ekker Advocatuur

Profiling the poor: Automated Decision Systems (ADS) in the digital welfare state



In recent years, there has been much debate about the use of algorithms by governments, specifically in the context of Automated Decision Systems (ADS). Currently, several of these systems are being challenged before the court.[1]

ADS and the welfare state

According to the United Nations Special Rapporteur on extreme poverty and human rights welfare, authorities are often at the forefront of digital innovation within government. During official country visits to the United States in 2017 and the United Kingdom in 2018, civil society actors and academics have underlined the severe human rights problems that emerge out of this.

The move towards ADS can be explained in a number of ways. Firstly, the number of individuals that receive benefits or interact with the welfare state in other ways is very large. In most countries the overall budget related to social security is huge as well. This leads to the idea that substantial savings can be used through the use of ADS.

There are also political factors. In many countries, the welfare state has been under attack. Politicians that are pushing to reform social security policies emphasize the need to reduce administrative costs and make welfare bureaucracies more 'efficient', 'cost-effective' and 'client-oriented'. There is also a demand to reduce the number of individuals who receive benefits, introduce stricter requirements and controls on those who do receive government assistance and investigate and punish the supposedly large numbers of individuals who commit welfare fraud.

> "The use of ADS clearly puts the trust of citizens in data processing by governments at stake."

MiDAS and SyRI

One striking example is the Michigan Integrated Data Automated System (MIDAS)-system. MIDAS was used by the state of Michigan to adjudicate and impose penalties for unemployment benefits fraud. To do so, it was programmed to automatically treat differences between income figures reported by beneficiaries and their employers as evidence of fraud.

[1] 'Litigating Algorithms: Challenging Government Use of Algorithmic Decision Systems', AI Now in collaboration with Center on Race, Inequality, and the Law, Electronic Frontier Foundation, September 2018. https://ainowinstitute.org/reports.html

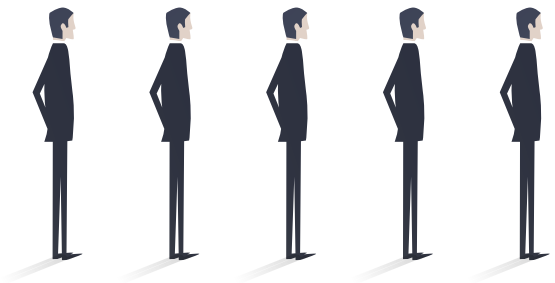
The system was not capable of investigating whether there are legitimate reasons for these discrepancies, such as employer error or pay disputes.

It was later established that, between October 2013 and August 2015, about 44,000 of the 62,784 determinations of fraud that MiDAS generated were in error. The U.S. Federal Court of Appeals for the region concluded that MiDAS "did not allow for a fact-based adjudication or give the claimant the opportunity to present evidence to prove that he or she did not engage in disqualifying conduct."[2]

"These principles, broadly considered as cornerstones of privacy law, protect the interests of citizens by establishing boundaries to the way in which data is processed."

The plaintiffs in the court case against MIDAS claim that the State of Michigan has violated their due process rights by taking their property without providing adequate notice and using unlawful collection practices. In the Court of Appeals of Michigan, they will also address the question whether an individual can file suit for money damages against the state for a violation of the Michigan Constitution.

The *'Systeem Risico Indicatie'* ('Risk Indication System' or '*SyRI*'), that is used in the Netherlands, bears resemblance to MiDAS. In 2018, a coalition of privacy organizations and the Netherlands Trade Union Confederation (*FNV*) initiated a lawsuit to end the use of *SyRI* by the Dutch authorities. *SyRI* is deployed under the responsibility of the Department of Social Affairs and Employment with the intention, in brief, to prevent fraud in matters of social security, employment, and taxes. In practice, *SyRI* is predominantly used in poor neighborhoods, with high concentrations of immigrants and other vulnerable groups.



Within *SyRI*, the Dutch government links and analyses great quantities of personal data from various governmental data banks. *SyRI* generates risk profiles of hundreds of thousands of citizens. In some cases, this profiling leads to a so-called 'risk notification': a notification regarding an increased risk of illegitimate conduct or of non-compliance with labour laws.[3]

Due process versus data protection

Around the world, NGOs, legal scholars and lawyers are looking for the most effective legal strategy to challenge the use of ADS by governments. In the US, legal actions are mostly based on due process claims. In the European Union, however, the European Convention of Human Rights and GDPR, provide additional legal arguments.

Under the GDPR, Member States have to demonstrate that ADS, and the data processing that is carried out to facilitate ADS, comply with privacy principles. First and foremost, it must be sufficiently clear that the data processing is necessary in a democratic society and that it meets the standards of proportionality and subsidiarity.

Furthermore, the principles of purpose limitation and compatible use must be respected. These principles, broadly considered as cornerstones of privacy law, protect the interests of citizens by establishing boundaries to the way in which data is processed. The Article 29 Working Party, the most important European advisory body in the field of privacy, formulates the importance of the limitation of purpose as follows:

[2] 'May 2019 Submission tot the UN Special Rapporteur on Extreme Poverty & Human Rights Regarding His Thematic Report on Digital Technology, Social Protection & Human Rights', Human Rights Watch 2019, https://www.hrw.org/news/2019/05/21/submission-un-special-rapporteur-extreme-poverty-human-rights-regarding-his-thematic

[3] The project website of the coalition can be found on: www.bijvoorbaatverdacht.nl

'When we share personal data with others, we usually have an expectation about the purposes for which the data will be used. There is a value in honouring these expectations and preserving trust and legal certainty, which is why purpose limitation is such an important safeguard, a cornerstone of data protection. Indeed, the principle of purpose limitation inhibits 'mission creep', which could otherwise give rise to the usage of the available personal data beyond the purposes for which it was initially collected.' [4]

[4] Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013, p. 4. Article 29 Data Protection Working Party.

"The widespread use of ADS poses a threat to human rights and jeopardizes the relation of trust between citizens and government."

The use of ADS clearly puts the trust of citizens in data processing by governments at stake. After all, citizens must be aware that virtually all data processed by government institutions can be used to secretly observe them.

Finally, the GDPR imposes a duty of transparency on governments that make use of ADS. In practice, however, the algorithms and risk models used are secret, resulting in a 'black box'.

Facing the challenge

The widespread use of ADS poses a threat to human rights and jeopardizes the relation of trust between citizens and government. While litigation to address some of these challenges is on the rise in the US, similar initiatives are limited in the European context until now. Therefore, it is important for human rights organizations, politicians and lawyers to come together and choose a strategy.

In short:

- The use of Automated Decision Systems (ADS) by governments is currently being challenged before the court.
- The welfare state has been criticized for its attempt to become more efficient and cost-effective by means of ADS.
- ADS have the potential to neglect data protection principles and jeopardize due process rights as well as the trust of the citizen in the government.

About the author
Anton Ekker is a lawyer, based in Amsterdam, The Netherlands. Together with Douwe Linders he represents a coalition of privacy organisations in the current legal proceedings against the State of the Netherlands regarding the *Systeem Risico Indicatie* (*SyRI*).