Digital Technology, Social Protection and Human Rights

Data Justice Lab submission

May 17th, 2019

1. Specific case studies involving the introduction of digital technologies in national social protection systems.

In the UK, there has been significant focus on the very important 'Digital by Default' agenda that incorporates the recently introduced Universal Credit System. Less attention has been paid to the data systems being implemented to inform decision-making pertaining to benefit claims and child protection. We have listed some specific case studies for this as part of a previous submission: https://www.ohchr.org/Documents/Issues/EPoverty/UnitedKingdom/2018/Academics/DataJusticeLabCardiffUniversity.pdf

2. What lessons can be learned from the ways in which digital technologies have been introduced in other parts of government.

Based on research we have carried out particularly in the areas of policing and border control, we can identify 3 major lessons:

a) *The technology does not 'work'*: Policing in the UK has a longer history of using digital technologies, including predictive analytics. There have therefore been more auditing and assessments of the technology carried out in this field. In recent times, we have seen that technologies that have been piloted and rolled out have very high error rates (especially for recognition technology such as in the case of South Wales Police).[1] Furthermore, some police forces are now moving away from using neighbourhood mapping for predicting crime in part because of a lack of evidence that this will reduce crime (e.g. Kent police cancelling its contract with PredPol).[2] This has raised questions about why and for what purpose digital technologies are introduced and the extent to which proper assessments of whether the technologies will meet those aims are carried out.

[1] https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival

[2] https://www.bbc.co.uk/news/uk-england-kent-46345717

b) *Technologies become weaponized*: In our research into digital technologies in border control, looking across Europe, we have found that personal devices such as mobile phones, become subsumed within governance structures. This can mean that digital technologies used for communication amongst particularly vulnerable groups, such as displaced people forced to migrate, are now used to inform decision-making about asylum and mobility within Europe. Similarly, the turn to cash cards for aid distribution systems run through interoperable databases (e.g., the Greek Cash Alliance programme) is a way to overcome the need for paper documentation but is also used to reinforce geographical restrictions on refugees arriving to Europe.[3] This raises questions about the extent to which control is the guiding logic for the implementation of digital technologies.

c) *Technological dependency*: In our research on policing and border control we have found a tendency amongst professionals (police officers, immigration officers etc.) to point to a restructuring of practices to adhere to databases and data models without a clear sense of the purpose of such practices. In this sense, data collection is often carried out just for the sake of it. This raises questions about the extent to which the implementation of digital technologies leads to a self-fulfilling logic and the extent to which professional practices become dependent on the technology rather than the other way around.

It is also worth noting that some technology companies (e.g. Palantir) are providers across areas of policing and border control, and are now also providing software for public health and social care in the UK.[4] This raises questions about the extent to which social protection adopts the same kind of logics of governance as those prevalent in policing and border control.

3. What human rights concerns might arise in connection with the introduction of digital technologies in social protection systems.

A range of data harms that include human rights concerns in relation to social protection systems can be found in our Data Harms Record which can be accessed here: https://datajusticelab.org/data-harm-record/.

4. Contextual circumstances affecting the impact of digital technologies

In our report on the implementation of data systems in UK public services, we outline a number of contextual issues as part of our discussion. Here we highlight just a few. The full report can be accessed here: https://datajustice.files.wordpress.com/2018/12/data-scores-as-governance-project-report2.pdf

I. UK Austerity: In our research we found that the austerity measures of the UK was frequently referred to as a way of explaining the rationale for implementing digital technologies in social protection. In discussions with professional associations, this was also raised as an important aspect for understanding the ability for social workers to assess, negotiate, and express concerns about the implementation of technologies. This will be significant for future discussions on the 'human-in-the-loop' as a safeguarding mechanism

[3] https://firstmonday.org/ojs/index.php/fm/article/view/9934/7749

[4] https://www.digitalmarketplace.service.gov.uk/g-cloud/services/196119321177256

for automated decision-making as proposed in the EU General Data Protection Regulation Act (GDPR). Furthermore, the context of austerity raises questions about the actions that can be taken in relation to data-driven risk assessments and decision-making.

II. Public engagement: In our research we found that there had been limited consultation with citizens about the implementation of digital technologies in social protection in the UK, and there has been little public debate or engagement with these developments. The UK Centre for Data Ethics and Innovation has just launched a consultation process pertaining to algorithmic bias. This consultation includes a section on how to advance public engagement.[5] This is significant for the ability for citizen to exercise rights in relation to data, such as the right to an explanation for automated decision-making. If people are not properly informed, it is unlikely that they are able to challenge decisions.

III. Public-private partnerships: Whilst a few local authorities are implementing digital technologies in social protection in-house, several are contracting data systems from private companies. Prominent companies in the area of social protection include Xantura and CallCredit. This has created different levels of transparency about the workings of the model and raises concerns about the way government might become 'locked-in' and reliant on external expertise.

IV. Targeting and stigmatisation: In our research with civil society groups that work with service-users about the implementation of digital technologies in public services, concerns about stigmatisation and feelings of being targeted were more prominent than privacy concerns per se. This is also connected to the Universal Credit System that is seen to be moving social protection towards conditionality-by-design with a dominant punitive framework rather than an enabling framework.

V. Personalising risk: Household-level and individual-level data relies on a fundamental personalization of risk, attaching risk factors to individual characteristics and behaviour that can lead to individualized responses to social ills being privileged over collective and structural responses, such as issues of inequality, poverty or racism.

5. Recommendations

In addition to the recommendations outlined in our previous submission, we have the following recommendations:

1. The implementation of digital technologies in social protection should be subject to full transparency, including a easily accessible list over where and for what purpose new technology systems are being implemented. Purpose statements should be provided for all existing systems in order to inform auditing and assessments.
2. The collection and use of data in social protection needs further oversight and regulation and cannot rely on self-regulation or ethical guidelines. Whilst GDPR cover some aspects of the handling of data, social protection provision is also exempt from some aspects of data protection law, and sector specific regulation needs to be developed.

[5] https://www.gov.uk/government/publications/the-centre-for-data-ethics-and-innovation-calls-for-evidence-on-online-targeting-and-bias-in-algorithmic-decision-making

3. There is a need to develop proper impact assessments of the implementation of digital technologies beyond privacy impacts assessments. These should include the experiences of service-users and other impacted communities and should include an assessment of actions taken on data systems (including resources allocated to such actions).
4. A greater focus on citizen participation and oversight. We have seen the growing emphasis on citizen assemblies and citizen juries in other parts of government decision-making. This should be tested for the implementation of digital technologies in social protection. We have also seen the use of community-based oversight bodies in the area of technologies and policing (e.g. in Oakland in the United States)[6]. Similar initiatives could be tested in social protection.
5. Efforts should be made to ensure public ownership over technologies and data. In such sensitive areas as social protection, the implementation of digital technologies by private companies risks the privatisation of welfare provision 'through the back door'. Taking back public ownership over public services and infrastructure is a very current issue in the UK[7] and should be extended to digital technologies in government. This may be most effective at local or city-level, as currently being advanced in Barcelona.

[6] https://www.aclunc.org/news/oakland-becomes-latest-municipality-reclaim-local-control-over-surveillance-technologies-used

[7] See for example the 2019 When We Own It report: https://weownit.org.uk/sites/default/files/attachments/When%20We%20Own%20It%20-%20A%20model%20for%20public%20ownership%20in%20the%2021st%20century.pdf