APPG on the Rule of Law

Data Processing and the Rule of Law

Date: 13 May 2019
Time: 18:30 -20:00
Location: Room A,
1 Parliament Street,
House of Commons

Meeting Aim

To provide MPs and Peers with an opportunity to discuss the rule of law issues that arise in relation to increased use of data processing in the public and private sector.

Proposed Schedule

18:30 – 18:35	**The Rt Hon Dominic Grieve QC MP (Chair)** Introduction
18:35 – 18:45	**Roger Taylor** **Chair of the Centre for Data Ethics & Innovation**
18:45 – 20:00	Roundtable discussion of the Rule of Law questions outlined below

Background

When government decisions are made about individuals' rights using data processing, it can be hard for an individual to know whether their data were accurate or processed correctly. Transparency and accountability in the adoption and operation of data processing and automated decision-making can help improve trust in such technology and enable it to function more effectively.

This briefing sets out some of the rule of law questions and includes two case study examples of government use of such technology. Following these examples, the briefing considers governance of data processing under the General Data Protection Regulation (GDPR) through Data Protection Impact Assessments, and finally outlines some other features of the regulatory and policy landscape.

Use of data processing by the private sector also raises rule of law questions, including issues of transparency and accountability in decision-making. The GDPR provisions for Data Protection Impact Assessments apply to private sector actors as well as government. Robust Data Protection Impact Assessment processes could not only form part of private sector compliance with the law, but also help to grow public trust and confidence in use of data processing through transparency and explaining data processing use to the public.

The Centre for Data Ethics & Innovation (CDEI)

The adoption of data-driven technology affects every aspect of our society, and its use is creating opportunities as well as new ethical challenges. The CDEI is an independent advisory body set up and tasked by the UK Government and led by a board of experts, to investigate and advise on how we maximise the benefits of these technologies.

The CDEI has a unique mandate to make recommendations to government on these issues, drawing on expertise and perspectives from across society, as well as advice for regulators, and industry, that support responsible innovation and help build a strong, trustworthy system of governance. The government is then bound to consider and respond publicly to these recommendations.

Rule of Law Questions

- How can law keep pace with technology? Are current concerns the result of a lack of laws and policy, or shortcomings in implementation of the law? When and why should the Centre for Data Ethics & Innovation recommend changes to law?

- How can the law and government protect against bias or discrimination in the operation of new data processing technologies? And what principles and protections might be appropriate for new groups that are legally unprotected at present?

- Do the cross-border nature of data flows require greater emphasis on the principle of international rule of law, i.e. compliance with international law as part of the rule of law?

- Where government uses digital administration to automate or partially automate implementation of the law, how do we ensure that the law is properly and correctly administered?

- When decision-making is partially or fully automated, who is responsible for the decision? How do long-standing principles of administrative law on proper government decision-making apply to a partially automated decision, for example, when is an algorithm-generated risk assessment a proper consideration for a decision-making to take into account?

- When government uses algorithms for risk-based verification as part of application processes, is it consistent with the principle of equality before law for different risk categories to be subject to different application processes?

- How can government ensure that its use of data processing is good value for money, and that data processing systems are not biased in their operation? For example, when assessing risk, an automated process may exclude categories such as race or sex, but use other data points that in effect profile and discriminate against people.

- When new automated decision-making systems are being designed and established, what obligations for conducting and disclosing impact assessment – as well as for meaningful consultation – should there be? Does meaningful consultation require disclosure of the Equality Impact Assessment and Data Protection Impact Assessment for proposed systems so that people can comment on proposals? Should the same obligations for Data Protection Impact Assessments apply to both private and public actors?

- What should the regulatory approach to automated decision-making be in terms of transparency as to the data that are used in the decision, accuracy of those data, and explanation of the logic for the decision? Could improved regulation along those lines prevent or mitigate bias in automated system?

Case Study 1: Housing Benefit (HB) and Council Tax Benefit (CTB) Applications

As explained in a Department for Work and Pensions (DWP) Local Authority Insight Survey:

> Risk Based Verification (RBV) assigns a risk rating to each Housing Benefit (HB)/Council Tax Benefit (CTB) claim which determines the level of verification required. It allows more intense verification activity to be targeted at those claims which are deemed to be at highest risk of involving fraud and/or error.
>
> It is practiced on aspects of claims in Jobcentre Plus and The Pension, Disability and Carers Service (PDCS). In April 2012 DWP extended RBV on a voluntary basis to all local authorities (LAs).[1]

DWP gives the following examples of the kind of risk ratings or categories that RBV assigns in the circular setting out guidance on Risk-Based Verification of HB/CTB Claims

- Low Risk Claims: Only essential checks are made, such as proof of identity. Consequently these claims are processed much faster than before and with significantly reduced effort from Benefit Officers without increasing the risk of fraud or error.

- Medium Risk Claims: These are verified in the same way as all claims currently, with evidence of original documents required. As now, current arrangements may differ from LA to LA and it is up to LAs to ensure that they are minimising the risk to fraud and error through the approach taken.

- High Risk Claims: Enhanced stringency is applied to verification. Individual LAs apply a variety of checking methods depending on local circumstances. This could include Credit Reference Agency checks, visits, increased documentation requirements etc. Resource that has been freed up from the streamlined approach to low risk claims can be focused on these high risk claims.

The circular also explains (citations omitted):

> Some IT tools use a propensity model which assesses against a number of components based on millions of claim assessments to classify the claim into one of the three categories above. Any IT system must also ensure that the risk profiles include 'blind cases' where a sample of low or medium risk cases are allocated to a higher

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/633018/s11-2011.pdf paragraph 9.

> risk group, thus requiring heightened verification. This is done in order to test and refine the software assumptions.
>
> Once the category is identified, individual claims cannot be downgraded by the benefit processor to a lower risk group. They can however, exceptionally, be upgraded if the processor has reasons to think this is appropriate.[2]

There appears to be no information on what data points these RBV systems use to make their assessments of risk.

Furthermore, the DWP guidance on governance leaves rule of law questions unresolved. Local authorities are required to produce an RBV Policy and a baseline against which to assess the impact of an RBV, and to undertake monthly monitoring of RBV performance. However, rule of law questions remain, for example, there are no criteria for monitoring impact in relation to protected characteristics under equality law. There are no requirements for transparency in the governance arrangements, in fact, DWP advises that the RBV policy should not be made public 'due to the sensitivity of its contents'.

The underlying concern is that information on the system would allow applicants to game the system because they would know the risk profiles. However, it is not clear how the proper exercise of public power can be verified when people are not told that they have been subject to an RBV nor the basis for its assessment of them which leads to different process thresholds for applicants. Furthermore, there would not be the same individual fraud risk in relation to the disclosure of aggregate baseline information, nor the aggregate findings of performance monitoring.[3]

While this example concerns decision-making by public authorities, there is evidence that private sector companies such as Xantura, Callcredit, and Capita have provided the RBV systems to local authorities.[4] As such, there are a set of roles, relationships, and obligations raised, including the:

1. Procurement relationship between the local authorities and the private sector;
2. Role of private sector producing these RBV systems for public sector use;
3. Role of local authorities as decision-maker using RBV systems.

---

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/633018/s11-2011.pdf paragraphs 12 and 13

[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/633018/s11-2011.pdf [14]-[18]

[4] Data Justice Lab, *Data Scores as Governance: Investigating uses of citizen scoring in public services* (December 2018).

Case Study 2: Settled Status Application Process for EEA Nationals

The settled status scheme has been established by the Home Office in the context of Brexit to regularise the immigration status of EEA nationals and their families living in the UK. Difficulties with the identify verification aspect of the application process have been relatively high profile because it relies on mobile phone technology, but does not work on Apple devices at this point in time. The automatic checks of welfare and tax data to verify residence have received much less attention, but are an automated part of the application process of great significance, albeit a partially automated decision not fully automated.

Part of the settled status scheme involves sharing data between government departments and algorithmic assessment of those data. EEA nationals who have lived in the UK for at least five years are entitled to 'settled status'. Those who have lived in the UK for less than five years are entitled to 'pre-settled status' and will need to apply for settled status when they reach the five year threshold. The Home office application process uses automated data processing to analyse data from the Department of Work and Pensions (DWP) and HM Revenue and Customs (HMRC) to verify how long applicants have been in the UK. Where the application process finds a 'partial match', the applicant is granted pre-settled status unless they challenge that decision.

The EU Settlement Scheme private beta testing phase 2 report stated:

> 11 such administrative review applications had been received and processed by 14 January 2019, with a further 13 pending. In all 11 cases the applicant was challenging a grant of pre-settled status rather than settled status. One of these grants of pre-settled status was upheld following the administrative review and the other 10 were instead granted settled status. Of these 10, nine of the applicants had originally accepted a grant of pre-settled status when making their application and then provided additional evidence of their eligibility for settled status with their application for administrative review[5]

8,106 applicants—30% of the decisions that had been made at the time of the report—were granted pre-settled status, but there were no measures reported to check whether those applicants had been granted the correct status. For example, the date on which applicants commenced residence was not included as a question in the application, and therefore could not be used to assess the accuracy of the automatic checks.

There was a proposal for manual checks to mitigate the risk of errors in the automatic checks resulting in applicants being wrongly granted pre-settled status instead of settled status, to which the Minister responded:

> Informing an applicant of why data has not matched is likely to increase the risk of fraud and identity abuse. The new clause would change the focus of the scheme from granting status to investigating the data quality of employers or of the DWP and HMRC. We consider that a distraction that would cause unnecessary delays for applicants…. In most cases, it would be far simpler and more

[5] https://www.gov.uk/government/publications/eu-settlement-scheme-private-beta-2/eu-settlement-scheme-private-beta-testing-phase-2-report#pb2-performance-data

straightforward for applicants to submit other evidence to prove residence, rather than seeking to resolve why data has not matched. Of course, the applicant can take up that issue with HMRC or the DWP if they wish.[6]

Many problems with the automated checks have been reported by applicants, including employed and self-employed applicants, and there are particular concerns for applicants who are low-income or vulnerable.[7] Coram are concerned that 'a number of vulnerable groups will be negatively impacted by the current functioning of the automated data checks, used to verify length of residence:

- A number of benefits are not included in the automated data checks, including Child Benefit (which can only be paid to one person – the person considered to have the main responsibility for caring for a child) and Child Tax Credit. This disproportionately impacts on women who are more likely to be receiving these benefits.

- Disabled people and their carers who rely on welfare benefits will need to provide additional proof of residence. This places an additional burden on these groups who may struggle to provide relevant documentation.

- Currently, Universal Credit can only be used as proof of residence for the main recipient. This impacts on women who are less likely to be in receipt of it, and particularly those who are in abusive or controlling relationships.'[8]

Although the Home Office has consulted with user groups, there has been a lack of transparency and information on the data processing used in the settled status scheme. The memoranda of understanding for data sharing between the Home Office and DWP, and the Home Office and HMRC were published at the end of March in response to a proposed amendment from Stuart McDonald MP.[9] The Data Protection Impact Assessment for the settled status application process has not been published, nor has the Equality Impact Assessment.

What GDPR governance exists for these government digital administration processes?

Art 22 of the General Data Protection Regulation (GDPR) is often cited as the relevant protection in data protection law concerning automated decision-making. Art 22 provides that people have the right not to be subject to decisions, including profiling, based solely on automated processing. Where processing is covered by art 22, individuals need to be informed about the processing, there need to be mechanisms for them to request human

[6] Public Bill Committee: Immigration and Social Security Co-ordination (EU Withdrawal) Bill (5 March 2019), col 376.
[7] https://www.politics.co.uk/blogs/2019/02/06/warning-lights-flashing-over-eu-settled-status-app
[8] Coram Children's Legal Centre, *Uncertain futures: the EU settlement scheme and children and young people's right to remain in the UK* (March 2019).
[9] Public Bill Committee: Immigration and Social Security Co-ordination (EU Withdrawal) Bill (5 March 2019), col 375.

intervention or challenge the decision, and there need to be regular checks.[10] However, Art 22 only applies to fully automated decisions, and does not apply when there is a 'human in the loop', i.e. a human is in some way involved in the decision.

The current governance process for most data processing systems, including partially or fully automated decision-making systems, is Data Protection Impact Assessments (DPIAs). The Information Commissioner's Office (ICO) explains that DPIAs are 'a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan' and are 'a key part of … accountability obligations under the GDPR'.[11]

Art 35 of the GDPR provides (emphasis added):

> 1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the **rights and freedoms of natural persons**, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
>
> …
>
> 7. The assessment shall contain at least:
>
> (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
>
> (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
>
> (c) an assessment of the risks to the **rights and freedoms** of data subjects referred to in paragraph 1; and
>
> (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

There are no GDPR obligations for transparency or public engagement and consultation on DPIAs. DPIAs must be sent to the ICO, but there are no routine mechanisms for public disclosure of DPIAs. There is an obligation of prior consultation with the ICO before action where a DPIA indicates that the proposed data processing 'would result in a high risk'.

---

[10] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

[11] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/

What Does a DPIA Process Include?

The ICO identifies the following key elements of a DPIA process:

- Step 1: identify the need for a DPIA
- Step 2: describe the processing
- Step 3: consider consultation
- Step 4: assess necessity and proportionality
- Step 5: identify and assess risks
- Step 6: identify measures to mitigate the risks
- Step 7: sign off and record outcomes[12]

This process as described by the ICO means that DPIAs should explain the function, purpose, and anticipated consequences of proposed data processing systems for the rights and interests of individuals. Under step 2 the description of the processing must include the nature, scope, context and purposes of the processing. Under step 3, the ICO recommends consulting with individuals, unless there is good reason not to. Under step 5 to identify and assess risks, the ICO advises: 'look at whether the processing could contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage.'[13]

To assess the risk to the rights and freedoms potentially affected by data processing, DPIAs need to look at all human rights, not just privacy. For example, data processing in the settled status scheme could affect applicants' rights to housing, to work, and to access healthcare because of the immigration law restrictions on the right to work, right to rent, and access to health services in the context of the hostile environment/compliant environment.

The Human Rights, Big Data and Technology Project (HRBDT) has proposed a human-rights based approach to the design, development and implementation of big data and AI projects. HRBDT's report shows that these technologies can affect all of the rights set out in the Universal Declaration of Human Rights—not only equality and privacy, but other such as the rights to education, healthcare, social care of the elderly, and law enforcement.

[12] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/

[13] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/

The proposed human-rights based approach would include undertaking full human rights impact assessments against all human rights.[14]

While the above discussion focuses on government use of data processing, the GDPR provisions for DPIAs apply equally to private sector use of data processing. Developing robust human rights approaches to DPIAs could assist the private sector to develop trustworthy and responsible technology.[15]

Other Parts of the Legal and Policy Landscape

In addition to the GDPR and data protection law, there are other laws and policies of relevance to the design and implementation of data processing systems including:

- Administrative law — administrative law is part of public law in the UK, and has been developed through case law, i.e. court decisions, as part of what is called 'common law'. Administrative law provides the framework for the proper exercise of power by government, meaning Ministers, government departments, public authorities. Key principles or tests in administrative law include:
    - Legality – acting within the scope of powers and for a proper purpose, taking into account relevant factors and not deciding on the basis of irrelevant factors;
    - Procedural fairness; and
    - Reasonableness.[16]

- Equality law — Under section 149 of the Equality Act, all public authorities must, in the exercise of their functions, have due regard to the need to eliminate discrimination, harassment and victimisation in relation to protected characteristics such as age, sex, pregnancy and maternity, and race. To assist compliance with equality duties, public authorities carry out Equality Impact Assessments for proposed policies to look at whether the policy would have a disproportionate impact on persons with protected characteristics.

- The DCMS Data Ethics Framework, Principle 6 of which is 'Make your work transparent and be accountable'. The Guidance for this principle states:

---

[14] Lorna McGregor et al, 'The Universal Declaration of Human Rights at 70: Putting Human Rights at the Heart of the Design, Development and Deployment of Artificial Intelligence', (20 December 2018) https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2018/12/UDHR70_AI.pdf

[15] Heleen Janssen, 'Detecting New Approaches for a Fundamental Rights Impact Assessment to Automated Decision-Making', (December 17, 2018). Available at SSRN: https://ssrn.com/abstract=3302839 or http://dx.doi.org/10.2139/ssrn.3302839.

[16] The Judge Over Your Shoulder (January 2006) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/256111/judge.pdf , pages 9 and 12; see also, Cobbe, Jennifer, Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making (August 6, 2018). A pre-review version of a paper in Legal Studies, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3226913 or http://dx.doi.org/10.2139/ssrn.3226913

> Your work must be accountable, which is only possible if people are aware of and can understand your work.
>
> Being open about your work is critical to helping to make better use of data across government. When discussing your work openly, be transparent about the tools, data, algorithms and the user need (unless there are reasons not to such as fraud or counter-terrorism). Provide your explanations in plain English.[17]

- The 7 principles of public life (the 'Nolan principles'), include:

> 4. Accountability
> Holders of public office are accountable to the public for their decisions and actions and must submit themselves to the scrutiny necessary to ensure this.
>
> 5. Openness
> Holders of public office should act and take decisions in an open and transparent manner. Information should not be withheld from the public unless there are clear and lawful reasons for so doing.[18]

Notably, the Committee on Standards in Public Life is undertaking a review into 'artificial intelligence and its impact on standards across the public sector'.[19] The deadline for written submissions is Friday 17 May 2019.

Despite the emphasis on the principle of transparency and openness in UK government policy, the use of data processing by public authorities in the UK in their exercise of public power often lacks transparency. The UN Special Rapporteur on Extreme Poverty and Human Rights made the following observations after his visit to the UK in 2018 (citations omitted):

> A major issue with the development of new technologies by the UK government is a lack of transparency. Even the existence of the automated systems developed by DWP's 'Analysis & Intelligence Hub' and 'Risk Intelligent Service' is almost unknown. The existence, purpose and basic functioning of these automated government systems remains a mystery in many cases, fueling [sic] misconceptions and anxiety about them. Advocacy organizations and media must rely on Freedom of Information requests to clarify the scope of automated systems used by government, but such requests often fail.[20]

[17] https://www.gov.uk/guidance/6-make-your-work-transparent-and-be-accountable
[18] https://www.gov.uk/government/publications/the-7-principles-of-public-life/the-7-principles-of-public-life--2
[19] https://www.gov.uk/government/collections/ai-and-public-standards
[20] https://www.ohchr.org/documents/issues/poverty/eom_gb_16nov2018.pdf

The Bingham Rule of Law Principles

The Rule of Law questions above are based on eight core principles that were identified by Lord Bingham, which can be summarised as:

1. The law must be accessible and so far as possible, intelligible, clear and predictable;
2. Questions of legal right and liability should ordinarily be resolved by application of the law and not the exercise of discretion;
3. The laws of the land should apply equally to all, save to the extent that objective differences justify differentiation;
4. Ministers and public officers at all levels must exercise the powers conferred on them in good faith, fairly, for the purpose for which the powers were conferred, without exceeding the limits of such powers and not unreasonably;
5. The law must afford adequate protection of fundamental human rights;
6. Means must be provided for resolving without prohibitive cost or inordinate delay, bone fide civil disputes which the parties themselves are unable to resolve;
7. Adjudicative procedures provided by the state should be fair; and
8. The rule of law requires compliance by the state with its obligations in international law as in national law.