BINGHAM CENTRE FOR THE RULE OF LAW

appg

APPG on the Rule of Law

Date: 16 April 2018
Time: 11:00-12:30
Location: Committee Room 8, Houses of Parliament

The Data Protection Bill: What Do Rule of Law Principles Mean for AI and Data Processing?

Briefing Note

Please note: all comments made by any person at the meeting are to be treated as comments made in public. Attendees may tweet and report as they wish.

Meeting Aim

To provide MPs and Peers with an opportunity to discuss the application of rule of law principles to data gathering, sharing and processing, including using artificial intelligence (AI), under the Data Protection Bill. There will be a particular focus on the potential risks and opportunities for the proposed 'framework for data processing by government' to undermine or reflect rule of law principles.

Proposed Schedule

11:00 – 11:05	**The Rt Hon Dominic Grieve QC MP (Chair)** Introduction
11:05 – 11:25	**4 expert speakers** (5 minutes each)
11:25 – 12:05	**Questions and comment** – MPs and Peers
12:05 – 12:30	**Questions and comment** – open to the floor

Background

The Data Protection Bill proposes to update the legal framework for data protection in the UK, replacing the Data Protection Act 1998, and to adapt the EU's General Data Protection Regulation (GDPR) while EU law applies in the UK, as well as ensuring legal continuity in the context of Brexit. The GDPR and Data Protection Bill apply to all people, organisations, companies or institutions that control or process personal data. Thus, these legal instruments are relevant to data gathering, sharing and processing in the private and public sectors for commercial or public purposes.

Clauses 183 to 186 of the Data Protection Bill provide for the Secretary of State to prepare a Framework for Data Processing by Government with 'guidance about the processing of personal data' for Government functions. Under the clause 3 definition, processing 'means an operation or set of operations which is performed on information, or on sets of information' including collection, alteration, retrieval, disclosure by transmission, alignment or destruction.

Examples of Data Processing by Government

BIICL
British Institute of International and Comparative Law
Registered Charity No. 209425
Company No. 615025

Examples of problems with data processing by Government illustrate the importance of rules for data processing by Government that promote good administration.

Migration of data

One example identified by Child Poverty Action Group concerns an apparent failure to migrate data on individuals' limited capability for work or limited capability for work-related activity to the Universal Credit (UC) system:

> Individuals who have the limited capability for work or limited capability for work-related activity element included in their Employment and Support Allowance (ESA) award, should automatically have the relevant element included in their UC award unless their ESA award ceased prior to them claiming UC. For example, someone who is receiving ESA making a new claim for housing benefit in a full service area would trigger a claim for UC. However we have collected a number of case studies that evidence the relevant elements are often not being included automatically and individuals are being told they will have to be re-assessed before the relevant element can be included in their award.
>
> A client with learning difficulties has been underpaid UC for five months. She was claiming income related ESA, but had to claim UC when she had to start claiming help with her housing costs. She should have had the limited capability for work-related activity element included in her UC award automatically, but has not and has been told that the will have to undergo another work capability assessment first.[1]

A gap in the feed

Another example in 2016 arose from a 'gap in the data feed' for the disability living allowance between the Department for Work and Pensions and HM Revenue & Customs:

> Thousands of families with disabled children have lost out on up to £4,400 a year in tax credits after an administrative blunder by the authorities.
>
> The error in processing their claims meant an estimated 28,000 families whose children qualified for disability living allowance (DLA) during 2011-14 missed out on an additional tax credit premium of between £60 and £84 a week.
>
> The Government revealed in the Autumn Statement this week that it had set aside £360m over six years to ensure these families receive child disability tax credits in future. However, the payments will be backdated only to April, meaning individual families may have lost out on entitlements totalling up to £20,000 over the past five years.[2]

---

[1] Child Poverty Action Group, Briefing for Peers – Debate: Impact of Universal Credit on claimants (16 November 2017) http://www.cpag.org.uk/sites/default/files/uploads/CPAG-Briefing%20for%20Peers-debates%20on%2016%20November%202017_0.pdf

[2] Patrick Butler, 'Tax credit error costs families with disabled children £4,400 a year', *The Guardian* (25 November 2016) https://www.theguardian.com/uk-

A Framework for Data Processing by Government

Clauses 183 to 186 were introduced as amendments by the Government to the Data Protection Bill on the last day of Committee in the House of Lords, and consequently received less scrutiny in that House than provisions that were in the Bill when it was introduced. Lord Ashton gave the following explanation for the clauses:

> All Government and public sector activities require some form of power to process personal data, which is derived from both statute and common law. In light of the requirements of the GDPR, such processing should be undertaken in a clear, precise and foreseeable way. The Government's view is that the framework will serve further to improve the transparency and clarity of existing Government data processing. The Government can, and should, lead by example on data protection. To that end, the proposed clauses provide the Secretary of State with the power to issue guidance in relation to the processing of personal data by Government under existing powers. As I have already stated, Government departments will be required to have regard to the guidance when processing personal data.[3]

Under clause 183, the Framework would apply to data processing relating to functions of:

> (a) 'the Crown, a Minister of the Crown or a United Kingdom government department, and
>
> (b) a person with functions of a public nature who is specified or described in regulations made by the Secretary of State.'

Such regulations would be subject to the negative resolution procedure.

Notably, clause 183 is presently drafted in broad terms such that it concerns any processing of all 'personal data' for the broad scope of purposes set out above. Accordingly, the Framework would be relevant to personal data held by intelligence and security services, and to processing by those agencies. Personal data as defined by clause 3 'means any information relating to an identified or identifiable living individual'.

The Bill does not clearly provide the Framework's relationship to the data protection principles already established in UK law, and reflected in the GDPR and Data Protection Bill. These data protection principles go some way to reflecting the rule of law in principles for data processing by requiring that:

1. Processing of personal data be lawful, fair and transparent
2. The purposes of processing personal data be specified, explicit and legitimate
3. Personal data be adequate, relevant and not excessive

---

news/2016/nov/25/tax-credit-error-costs-families-with-disabled-children-4400-a-year

[3] House of Lords Hansard, Data Protection Bill Public Bill Committee (22 November 2017), v787 c228

4. Personal data be accurate and kept up to date
5. Personal data be kept for no longer than is necessary
6. Personal data be processed in a secure manner
7. Accountability[4]

The GDPR also provides for rights of data subjects, but again, the relationship between these rights and the proposed Framework are unclear:

1. Right of access, by which subjects are entitled to confirmation on whether their personal data is being processed and for what purpose
2. Right to erasure
3. Data portability
4. Mandatory breach notification
5. Strengthened conditions for consent.[5]

Clause 184 of the Bill requires that the Secretary of State lay the Framework before Parliament and it cannot be issued by the Secretary of State if either House of Parliament resolves not to approve it. If no such resolution is made, then the Framework will be issued and come into force after 21 days. Amendments to the Framework are subject to the same process for approval.

Once issued, the Framework must be published, and the Secretary of State is required by clause 185(4) to amend the Framework if the Framework could result in a breach of an international obligation of the UK.

Clause 186 sets out the proposed legal effect of the Framework:

> (1) When carrying out processing of personal data which is the subject of a document issued under section 184(3) which is for the time being in force, a person must have regard to the document.
> (2) A failure to act in accordance with a provision of such a document does not of itself make a person liable to legal proceedings in a court or tribunal.
> (3) A document issued under section 184(3), including an amendment or replacement document, is admissible in evidence in legal proceedings.
> (4) In any legal proceedings before a court or tribunal, the court or tribunal must take into account a provision of any document issued under section 184(3) in determining a question arising in the proceedings if—
> (a) the question relates to a time when the provision was in force, and
> (b) the provision appears to the court or tribunal to be relevant to the question.

[4] Art 5of the GDPR and clauses 35-40 and 86-91 of the Bill.

[5] Arts 15, 17, 20, 34, and 4(11) of the GDPR.

(5) In determining a question arising in connection with the carrying out of any of the Commissioner's functions, the Commissioner must take into account a provision of a document issued under section 184(3) if—

(a) the question relates to a time when the provision was in force, and

(b) the provision appears to the Commissioner to be relevant to the question.

The Data Science Ethics Framework — an existing model?

The Government has not yet released a draft of the Framework proposed by the Bill, so for some indication of what might be contained in the Framework, we can look to the Data Science Ethical Framework produced by the Government Digital Service (GDS) in the Cabinet Office in May 2016.

The Data Science Ethical Framework identifies six principles:

1. Start with clear user need and public benefit
2. Use data and tools which have the minimum intrusion necessary
3. Create robust data science models
4. Be alert to public perceptions
5. Be as open and accountable as possible
6. Keep data secure[6]

For the fifth principle to be 'as open and accountable as possible without putting your project at risk', the framework states:

> Aim to be publicly transparent about what you are doing and be open about the tools, data and algorithms used and its intention (unless there are serious public interest reasons not to, such as fraud or counter-terrorism) and provide your explanations in plain English.
>
> Try and ensure that for new digital services and elsewhere, where possible people can view and extract their own personal data held by the government service and that they are told about how their data will be used at the point of collection.
>
> Make sure there is oversight and accountability throughout the project. Oversight needs to cover both the initial assessment of purpose and method, but then how it is carried out and what is done as a result.[7]

[6] Cabinet Office, Data Science Ethical Framework (Version 1.0, published 19 Mary 2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/524298/Data_science_ethics_framework_v1.0_for_publication__1_.pdf

[7] Cabinet Office, Data Science Ethical Framework (Version 1.0, published 19 Mary 2016), page 15 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/524298/Data_science_ethics_framework_v1.0_for_publication__1_.pdf

That existing framework has been criticised for suggesting that a privacy impact assessment could fit on a single side of A4, to encourage public bodies to adopt an approach to data sharing that is closer to 'Facebook-style'.

The Rule of Law in a Digital Age

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. The risk of algorithms operating in a discriminatory fashion also arises where, for example, the algorithm is developed using machine learning which depends on data sets 'teaching' the algorithm how to operate as those data can be skewed.

One response has been the idea of a 'right to an explanation', which is somewhat reflected in the GDPR although only to a limited extent as identified by Edwards and Veale (emphasis in original):

> art 15…includes a right to access to "*meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing*" (art 15(1)(h)). This provision, notably, only applies in the context of "*automated decision making in the context of*" art 22. This leaves it unclear if all the constraints on art 22 (discussed below) are ported into art 15 (though our view is that it does not). …
>
> art 22 does not in its main thrust even contain a "*right to an explanation*": merely a right to stop processing unless a human is introduced to review the decision on challenge. However Art 22 does refer at points to a requirement of "*safeguards*", both where the right to prevent processing (paradoxically) does *not* operate, and where it does *but* sensitive personal data is processed.
>
> Art 22 applies only to systems where decisions are made in a "*solely*" automated way—i.e. there is no "human in the loop"—and there are very few of these and fewer that are "significant"... How "meaningful" this input has to be is subject to recent regulatory guidance …, but still unclear.[8]

Selbst and Powles have argued that arts 13–15 of the GDPR provide rights to "meaningful information about the logic involved" and that:

> First, because Articles 13–15 all relate to the rights of the data subject, "meaningful information" should be interpreted in relation to the data subject. That is, the information about the logic must be meaningful to her, notably, a human and presumably without particular technical expertise.

[8] Lilian Edwards and Michael Veale, 'Enslaving the algorithm: from a 'right to an explanation' to a 'right to better decisions'?, Pre-print, January 2018. Accepted for publication in IEEE Security & Privacy, http://discovery.ucl.ac.uk/10042153/1/SSRN-id3052831%281%29.pdf ; see also S Wachter, B Mittelstadt, and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76

> Second, the test for whether information is meaningful should be functional, pegged to some action the explanation enables in the data subject, such as the right to contest a decision as provided by Article 22(3).
> …
>
> Third, and relatedly, there should be a minimum threshold of functionality for the information provided. That is, the information should be at least meaningful enough to facilitate the data subject's exercise of her rights guaranteed by the GDPR and human rights law.
> …
>
> Fourth, the requirement should be interpreted flexibly. Specific rules defining the right methodologically may be too rigid, unnecessarily constraining research and development.[9]

Rule of Law Questions

A Framework on Data Processing by Government could be an opportunity to address the following rule of law questions that arise in the context of Government data processing:

- Where the law is implemented by Government through an algorithm how can the algorithm be accessible, intelligible, and clear?
- How should the law on data and data processing reflect the human right to privacy?
- To what extent should an individual's consent be required for data sharing between Government departments and disclosure to third parties such as caseworkers?
- Where public decisions are to be made by data processing, what obligations does the Government have to ensure that the decisions are made properly, fairly and in accordance with the law?
- What obligations do Government officials have when using data processing as part of public decision making to ensure that the decision is made properly, fairly and correctly, for example when the data processing produces an error?
- What are the consequences for access to justice when the Government has control over data and data processing? For example, where officials can amend individuals' data so that initially wrong decisions are effectively erased and shown to have been correct when made?
- If the Framework offers an opportunity for developing the application of rule of law principles to data processing and AI, should its application be limited to Government, or should it also apply to the private sector?

[9] Selbst, Andrew D. and Powles, Julia, Meaningful Information and the Right to Explanation (November 27, 2017). International Data Privacy Law, vol. 7(4), 233-242 (2017), 7-8. Available at SSRN: https://ssrn.com/abstract=3039125 (citations omitted)

The Bingham Rule of Law Principles

The rule of law questions above are based on eight rule of law 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.

Speakers' Biographies (Speaking Order)

Steph Pike
Steph Pike is the Welfare Rights Adviser (Food Bank) and Acting Head of Advice and Rights at Child Poverty Action Group (CPAG). CPAG is a registered charity with objects to prevent poverty among children and families and to promote action for the relief of such poverty. CPAG advocates evidence-based solutions to policymakers and provides information and advice to enable families to access necessary financial support. The organisation also conducts strategic litigation on matters that promote the rights of working families and children in both England and Scotland.

Professor Lilian Edwards
Professor Lilian Edwards is a leading academic in the field of Internet law. She has taught information technology law, e-commerce law, and Internet law at undergraduate and postgraduate level since 1996 and been involved with law and artificial intelligence since 1985. Her current research interests, while broad, revolve around the topics of online privacy, intermediary liability, cybercrime, Internet pornography, digital assets and digital copyright enforcement. Since 2012, Edwards has been Deputy Director of CREATe, the Centre for Creativity, Regulation, Enterprise and Technology, a £5m Research Councils UK research centre about copyright and business models. She is also a frequent speaker in the media and has been invited to lecture in many universities in Europe, Asia, America, Australasia and most recently, South Africa.

Sam Smith
Sam Smith is a coordinator at medConfidential, which is an independent non-partisan organisation campaigning for confidentiality and consent in health and social care, which seeks to ensure that every flow of data into, across and out of the NHS and care system is consensual, safe, and transparent. Sam has worked on a range of human rights technology

projects including building search engines about violence in Chechnya, wrangling data about political violence in Zimbabwe, and making research about modern slavery more accessible, and volunteered on a range of digital projects in support of an engaged and engaging democracy. He previously spent a decade working on research infrastructure in academia. From 2012-2013, he worked for Privacy International on export controls and other aspects of UK policy.

Professor Lorna Woods
Professor Lorna Woods is Professor of Internet Law at the University of Essex and a member of the Human Rights Centre. She started her career in practice at a commercial solicitors' firm advising in the field of commercial law, specifically that relating to the ICT sector. She then moved to academia where she has taught and researched in media and telecommunications regulation at both national and EU level, publishing widely in these fields. She has extensive experience in the field of media policy and communications regulation, including social media and the Internet, and she has published widely in this area (see list of publications) as well as contributed to a range of studies and parliamentary inquiries. She has co-authored books including, 'European Broadcasting Law and Policy' (Cambridge University Press) and 'Steiner & Woods on EU Law' (OUP) currently in its 13th edition.

Speakers' Summaries

Speaker Number 1

Steph Pike: Further Examples of Data Processing by Government

1. The examples illustrated above in the 'Migration of Data' and 'A gap in the feed' sections of this briefing underline the importance of rules that promote good administration.
2. Further to those examples, in December 2017, the Secretary of State for Work and Pensions accepted that some 75,000 individuals may have been underpaid when transferred from IB to ESA due to the failure to consider whether they qualified for income-related ESA and not just contribution based ESA. However, while the IB to ESA transfer process began in 2011 and therefore many of the underpayments will date back to before 2014, DWP says it will only make backdated payments to 21 October 2014, the date of a Upper Tribunal decision it claims establishes that it was making the wrong decisions. The National Audit Office has said that the decision not to make backdated payments for periods prior to 21 October 2014 will result in disabled claimants, as a group, losing out on between £100 and £150 million pounds. On 29 March 2018, CPAG issued judicial review proceedings challenging the decision of the DWP to limit backdated payments to those disabled people who had been underpaid when they had transferred from incapacity benefit ('IB') to employment and support allowance ('ESA') to a 21 October 2014 date.
3. For Universal Credit (UC), claimants have to take documents to the Job Centre (JC). The JC should scan the documents and send them to the UC processing offices. Our evidence shows that there are often problems with this data being shared with the correct offices, causing delays in claims being correctly assessed causing financial hardship. One client we worked with took her proof of rent to the Job Centre. Although the UC Department had confirmation that she had done so, as the documentation was not sent through to them by the Job Centre they failed to pay her housing costs for 5 months, leaving her in thousands of pounds arrears and at risk of eviction. It was only through the intervention of the CPAG adviser that the situation was resolved.

4. Government Departments do not routinely share data with each other or with other departments, e.g. local authority Housing Benefit Units. For example, an award of PIP may lead to additional premiums in ESA, IS, JSA, HB etc. Although there is no legal requirement for government departments to share data in these circumstances, the need to inform different departments can be difficult and confusing to claimants and can mean the loss of significant sums of money. To adopt a policy of data sharing as good practice could ensure that claimants receive their correct entitlement, and prevent overpayments.
5. With UC, some of the information shared by the DWP with claimants is misleading and lacks clarity, making it difficult for claimants to understand how decisions have been made and creating barriers to challenging decisions and therefore to accessing justice:
    a. where revisions have been made, for example where housing costs have been included months after the start of a UC claim, the payments record on the UC journal does not record when housing costs have been awarded and arrears have been paid, rather the payments records are amended to give the impression that housing costs were correctly paid from the start of the claim.
    b. UC decision notices and journals do not contain enough detail for claimants to fully understand how their benefit has been calculated. This makes it difficult for claimants to spot errors and make informed challenges to benefit decisions. For example, where someone is working the decision notice simple gives the total income that has been used rather than a breakdown of how that income has been calculated.

Speaker Number 2

Professor Lilian Edwards: Ensuring Accessibility, Intelligibility and Clarity

It is now well known that systemic biases and partialities embedded in training set data tend to produce similarly biased algorithmic models, and thus, results. The most famous instance in the public sector is the COMPAS recidivism scoring system which ProPublica showed in 2016 to have discriminatory effects on certain racial groups. COMPAS was proprietary and "closed code" not open source i.e. the public could not see what data the system drew on or how it made its decisions. This has become known as the "black box" problem and as the briefing notes, a solution has been seen in an alleged "right to an explanation" offered by the GDPR in art 22. However that right does not differ markedly from a remedy available since 1995 and still has several inclarities and gaps. Key drawbacks include:

- It only applies to "solely automated decisions" (how many public sector decisions does this apply to?)
- Which have legal or other "significant" effects (?)
- It is not clear what is a "decision" (e.g. is a targeted "nudging" message a "decision")
- Most importantly the primary remedy is to stop processing, **not** offer an explanation. This right **does** appear as a "safeguard" only where (a) the right to object does not operate (see art 22(3)) or (b) it does, but **sensitive personal data** is processed. In the latter case this "safeguard" only appears in recital 71 which may be seen as interpretative not mandatory.
- An alternative route to a right to an explanation is art 15(1)(h) which is more promising in requiring "meaningful information

about the logic involved" but also has difficulties, primarily whether it imports all the constraints of art 22 above.

A better approach might simply be to legislate ab initio for mandatory user rights to transparency especially in "high stakes" public sector decisions. Respecting maximum harmonisation with the GDPR is a constraint on DP Bill autonomy, but an amendment was nonetheless introduced by Lord Clement-Jones during the DP Bill passage, inspired by French law, as follows:

Before Clause 171

LORD CLEMENT-JONES
LORD PADDICK

183★ Insert the following new Clause—

"Right to information about individual decisions by public bodies based on algorithmic profiling

(1) Where—

(a) a public authority profiles a data subject (within the meaning of Article 4(4) of the applied GDPR), and

(b) the results produced by this profile are applied to a data subject, including informing a decision about them,

the relevant data subject is entitled to request from the public authority meaningful information relating to the profiling.

(2) Information provided on the basis of a request made under subsection (1) must include, at least—

(a) the degree and the mode of contribution of the profiling to the decision made;

(b) the provenance of the data that forms the basis of the profile applied;

(c) the data of the relevant data subject used to describe the profile in accordance with Article 15 of the applied GDPR;

(d) the weightings, or, where appropriate, the output of a comparable explanation facility, of the profiling system, applied to the situation of the person concerned; and

(e) where applicable, information on activities undertaken to ensure the compliance of the profiling system with the public sector equality duty (within the meaning of section 150(1) of the Equality Act 2010).

(3) For the purposes of this paragraph a "public authority" means a public authority within the meaning of the Freedom of Information Act 2000 or a person who is engaged by a public authority to exercise a public function.

(4) A public function is a function that is a function of a public nature for the purposes of the Human Rights Act 1998.

(5) Where a data subject makes a request under subsection (1), the controller must comply with the request without undue delay."

The proposed Framework for Data Sharing could avoid the simplistic response that the innards of an algorithmic model offer no "meaningful information" by putting in guidelines this kind of approach. Useable research on meaningful non-decompositional explanations using "pedagogical" or "counterfactual" approaches is emerging[10]. Multiple forms of explanations are possible and research might establish which work best in what domains for what data subjects. Guidelines could create

[10] See Binns et al "It's Reducing a Human Being to a Percentage';Perceptions of Justice in Algorithmic Decisions" , 2018 at https://arxiv.org/pdf/1801.10408.pdf ; Wachter et al "Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR", 2018 Harvard Journal of Law & Technology.

uniform expectations as to remedies. Transparency to be useful must be "effective" as well as "meaningful"[11] otherwise it may be less helpful not more. There is no point disclosing data without adequate arrangements for user challenge, audit and accountability. These may well already exist in different public sector domains; a sectoral approach then seems far more useful than a single "Algorithm Regulator". Overall it seems crucial that public sector systems are not bought off the peg as COMPAS was but are developed internally and open to audit, allowing tweaking, transparency and accountability[12]. AI Now have developed an Algorithmic Impact Assessment specially designed for public agency accountability[13] – this might be drawn on when adding guidance on prior impact assessment and post-audit to the Framework. Note that most ML systems are likely post GDPR to require a DPIA: art 35(3).

Speaker Number 3

Sam Smith: The Rule of Law: For Everyone In A World With AI

Decisions made by public bodies today must satisfy the Principles on the Rule of Law as identified by Lord Bingham.[14] The principles have been tested, internationalised, and localised to jurisdictions and cultures around the world. They are universal, robust, and can be applied to any decision framework. They also apply to uses of technology such as 'data processing'.

The Data Protection Bill introduces the "Framework for Data Processing by Government"[15] for which there is no published draft. It is broad, powerful, and completely opaque. As written, it covers any data in any public body, including the SIAs, processed in any way, including AI.

Data processing risks systemic failure. For example, families with a disabled child missed out on up to £84 per week, *for years,* because of errors in data processing by Government.[16] When the problem was finally addressed in 2016, some families may have lost over £20,000 of entitlements because payments were backdated for less than the five year period that the Government errors had underpaid these families. The error arose from a basic failure of the Department for Work and Pensions and HMRC to process data correctly - and neither had no incentive to detect it. Most data processing errors are more common and smaller scale, derived

---

[11] Council of Europe Study STUDY ON THE HUMAN RIGHTS DIMENSIONS OF AUTOMATED DATA PROCESSING TECHNIQUES (IN PARTICULAR ALGORITHMS) AND POSSIBLE REGULATORY IMPLICATIONS, final, October 2017 at 36.

[12] A good example is the HART scoring system developed by Durham police: see M Oswald et al "Algorithmic risk assessment policing models: Lessons from the Durham HART model and 'Experimental' proportionality", Information & Communications Technology Law

[13] Resiaman et al *AI Now Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability* (draft, March 2018)

[14] Bingham: The Rule of Law https://www.penguin.co.uk/books/56375/the-rule-of-law/

[15] Clauses 183-186 of the Data Protection Bill

[16] https://www.theguardian.com/uk-news/2016/nov/25/tax-credit-error-costs-families-with-disabled- children-4400-a-year

from something as basic as a spelling mistake in someone's name,[17] or misreading someone's date of birth on a form.[18]

A small data processing mistake by Government can have catastrophic implications for a resident. To avoid the arbitrary exercise of power, entitlements and obligations of individuals must be understood - ie decisions must be explained. The same applies with data processing.

If a different, lower, standard of 'ethics' is created to apply when AI is involved, then this erodes the rule of law on which our society is based. This is a choice made simply because it is easier. Is it really expected that we would create a lower standard because someone wishes to use a tool such as AI and doesn't want to do the work to understand the decision making process?[19]

Tools that process data[20] to inform decisions by public bodies must meet the standard we have set for ourselves as a democracy: the rule of law.

We have encouraged the rule of law around the world as an independent and high standard. Rights and liability should be determined by application of a known process, and not the exercise of discretion. As the Bingham Centre has explained:[21]

> "The rule of law can be understood in contrast with the 'rule of man', meaning a society in which one or more individuals rules arbitrarily exercising power unconstrained by law where the ruler(s) are above the law."

The principles identified by Lord Bingham, and the checklist from the Venice Commission,[22] provide a basis for a clear and impartial informed debate on the uses of data processing. A debate that the 'Framework for Data Processing by Government' has at every stage sought to evade. The existing non-statutory 'Data Science Ethics Framework', also owned by DCMS, believes you can deal with all privacy and propriety questions in a single side of A4.[23]

---

[17] https://www.theguardian.com/uk-news/2017/sep/26/leave-uk-immediately-scientist-is-latest-victim- of-home-office-blunder

[18] https://www.independent.co.uk/news/uk/home-news/nhs-letter-newborn-baby-eight-day-old-identity- documents-free-healthcare-right-violet-nik-horne-a7955211.html

[19] https://medconfidential.org/2017/on-what-principles-will-data-be-used-in-the-single-government-department/

[20] AI is simply data processing. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/artificial- intelligence-committee/artificial-intelligence/written/69500.html

[21] pg 11 https://www.biicl.org/documents/1284_briefing_paper_-_parl_and_rol_in_brexit.pdf

[22] http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)007-e

[23] https://medconfidential.org/2016/data-in-the-rest-of-government-the-cabinet-office-data-programme/

In an increasingly digital world, public confidence in Government requires Government to handle data in a transparent way in accordance with the rule of law. That requires not only transparency to citizens on how data about them has been used, but an understanding in public bodies that the principles of the rule of law apply to decisions around data processing as they do to any other.

The Framework for Data Processing by Government should be amended at Report to require a published statement explaining compliance of all data processing with the principles of the Rule of Law. That statement can provide an evidence base for those subject to data processing errors.

Private entities

Public law requires a clear legal basis for all acts of public bodies. Private bodies are treated very differently, with regulations constraining certain acts.

AI development tools are broadly application agnostic and often freely available, and because every AI used by public bodies must be explained to the satisfaction of the Principles, those same tools can be reused by any entity who wishes to show their AIs meet the highest standards of data processing. There is no compulsion, but there can be an expectation.

As an example, Facebook claim they wish to act ethically and in their users' interests, but the customers of Cambridge Analytica have made clear that is not quite as true as Facebook chose to believe. There should not be an arbitrary standard of ethics applied to data processing; after all, no tyrant has ever failed to justify their actions.

Speaker Number 4

Professor Lorna Woods: Privacy Protection and the Framework

Approach to privacy

State storage of citizens' data constitutes an intrusion into privacy[24]. The consolidation of data from various sources, e.g. through data sharing, increases the severity of the intrusion, especially where those sources relate to multiple aspects of a person's life and include confidential, sensitive and/or biometric information. Privacy is not unlimited but any intrusion must lawful, necessary for a legitimate objective and proportionate; the essence of the right must be respected. The lawfulness requirement reflects rule of law principles: the challenged measure must be based in domestic law, be accessible to the person concerned and be foreseeable as to its effects.[25] Discretion should be limited both in terms of scope and manner of exercise[26] – e.g. what data should be collected, how long information should be held, who has access and for what purpose.[27] In principle, data sharing runs

[24] S and Marper v UK (Grand Chamber), judgment 4 December 2008
[25] e.g Zakharov v. Russia 4 December 2015 (Grand Chamber)
[26] L.H. v. Latvia, judgment 29 April 2014
[27] Copland v UK, judgment 3 April 2007, para 46; Rotaru v Romania, judgment 4 May 2000 (Grand Chamber)

counter to the data protection principle of purpose limitation[28] and the development and maintenance of databases could give rise to a concern about ongoing state monitoring of individuals and is therefore particularly intrusive[29]. Oversight mechanisms are important where the use of data is not visible – for example in the context of surveillance, but arguably also in the context of unforeseen data sharing and profiling. These factors also affect any proportionality assessment. Data protection rules can operate to provide such safeguards (though data protection and privacy are not identical).

The Framework

The Secretary of State's discretion is broad. Clause 183(5)(a) requires that the ICO be consulted but there is no obligation on the Secretary of State to take the ICO's opinion into account. While the ICO and the Secretary of State may agree as to on standards, there is no guarantee of this, with a consequent risk of regulatory fragmentation and lack of clarity of law. It would seem preferable to strengthen the role of the ICO here, and/or expressly identify the orientation of the code towards transparency of public sector practices and the protection of citizens' privacy.

Further, there is no explanation as to how the guidance will interact with other regimes: the codes under Part V of the Digital Economy Act and the oversight regime under the Investigatory Powers Act.

The guidance may provide a mechanism where the data protection obligations are interpreted to provide a lower level of protection (which may also not meet the requirements of Article 8(2)). From the perspective of the data their rights could potentially be undermined. The risks may be mitigated by establishing that the baseline is that established by the GDPR or, in the case of the security services, Article 8. Guidance is needed in relation to identification of the purpose for which data are processed, rather than reliance vague terms (e.g. '"better service delivery" or "more efficient"), so as to facilitate a critical assessment of whether the processing is necessary (in the terms of Article 8) and proportionate. The use of AI may suggest the acquisition of more data is desirable, yet this is in tension with the idea that the State should limit data acquisition to what is strictly necessary (in data protection terms, data minimisation), ensuring accuracy and the desirability of deleting data in a timely manner.[30]

The framework has an effect not just in terms of the procedures and processes that a data controller might put in place but also in terms of enforcement, whether by the ICO or an aggrieved data subject. Cl 186 requires the courts and the ICO to take the guidance into account when determining proceedings or questions relation to the ICO's functions presumably providing some defence to enforcement actions or civil claims. This could be a significant weakness although, in the case of detailed guidance providing a high standard, could support accountability.

Conclusion

[28] See e.g. Bara and Ors v Președintele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF) (Case C-201/14) ECLI:EU:C:2015:638, judgment 1 October 2015

[29] See e.g. Tele2 AB v Post-och telestyrelsen (Case C-203/15) and Secretary of State for the Home Department v Watson et al (Case C-698/15), ECLI:EU:C:2016:970, judgment 21 December 2016 (Grand Chamber)

[30] See e.g. S. and Marper, para 103; MM V UK, judgment 13 November 2012

Data sharing is problematic in terms of privacy protection. The Framework guidance could operate to undermine substantive safeguards elsewhere in the Data Protection Bill and unnecessarily confuse an already complicated legal framework in which the powers for collecting and sharing data are scattered across a number of statutes. Potentially this could lead to divergence from the GDPR, and open the way for claims that the system for state acquisition and processing of data (whether generally or in specific sectors) falls short when viewed against the rule of law requirements in Article 8 ECHR (and the EU Charter.[31]).

[31] See e.g. Tele2 Sverige; Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Ors (Case C-623/17), pending.