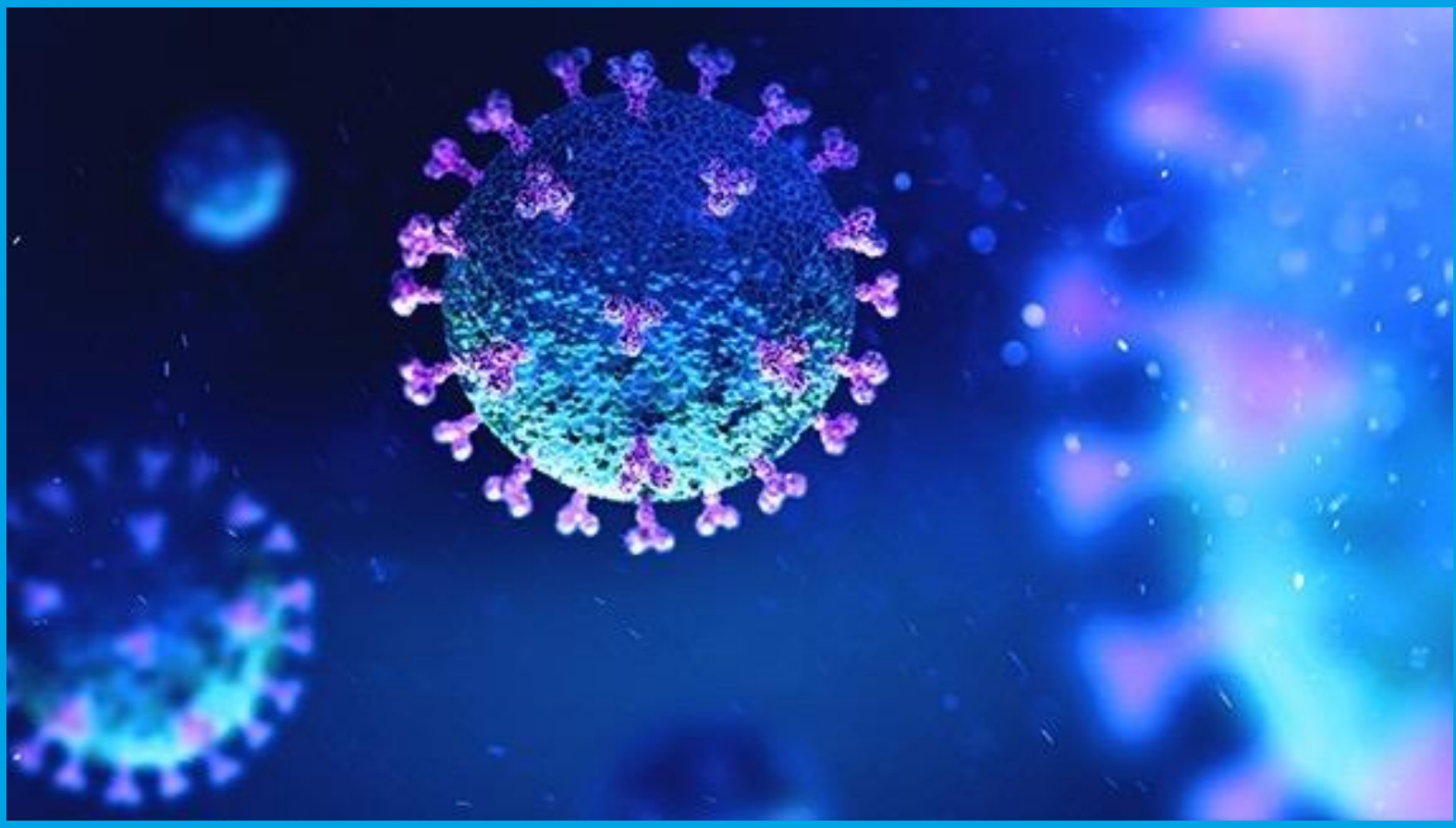
BINGHAM CENTRE FOR THE RULE OF LAW

Newcastle University

WP3-D3 Policy Brief: Good Governance and Rule of Law Principles for Data-Driven Technologies in Public Health Emergencies

Emma Irving, Lilian Edwards



November 2021

BICL
British Institute of International and Comparative Law

The Role of Good Governance and the Rule of Law in Building Public Trust in Data-Driven Responses to Public Health Emergencies

Funded by the UK Arts and Humanities Research Council, grant AH/V015214/1

This project, at the intersection of law, ethics, citizen deliberation, public health and data science, aims to develop a distinct values-based framework to help understand and address the challenges posed by data-driven responses to public health emergencies and the need to build public trust.

In their COVID-19 responses, states have relied on data-driven approaches to justify far-reaching measures, including closing entire business sectors and categories of travel, curtailing personal liberties and requiring compliance with new technologies for contact tracing and social distancing. To be effective, such measures must be internationally co-ordinated, nationally adopted and adhered to by a high proportion of the public. Trust underpins both national adoption and public adherence: trust in international institutions, in the measures adopted, and in their scientific foundations.

This project examines two critical enablers of that trust: good governance and the rule of law. It aims to provide practical guidance on how international and national institutions can build public trust in the processes by which they design and implement data-driven responses to public health emergencies. The research consists of four interconnected work packages which examine:
(1) International governance frameworks for public health emergencies.
(2) Values-based principles to guide data-driven responses by national institutions including governments, parliaments, courts and police.
(3) UK case studies and a literature review of data governance (national and international) in relation to the use of data driven technologies in the pandemic emergency
(4) A citizen jury deliberation on the trustworthiness of data-driven measures and what additional safeguards may be needed.

https://binghamcentre.biicl.org/projects/the-role-of-good-governance-and-the-rule-of-law-in-building-public-trust-in-data-driven-responses-to-public-health-emergencies

This report forms part of Work Package 3. This work package examines how good governance and rule of law principles can help to build public trust in data-driven technologies introduced in response to public health emergencies. The work package outputs address a range of technological responses to Covid-19 by discussing the legal frameworks that govern them and identifying the issues and challenges that they give rise to from a public trust perspective. The outputs comprise:

- Rapid Evidence Response Review of Data-Driven Responses to Public Health Emergencies (WP3-D1)
- 'No jab, no job'? Employment Law and Mandatory Vaccination Requirements in the UK (WP3-D2A)
- 'Venue Check-In' or 'Presence' Apps (WP3-D2B)
- Judicial Scrutiny of COVID-19 Regulations in the UK: Addressing Deference to Data-Driven Decision-Making in Human Rights Cases (WP3-D2C)
- Policy Brief: Good Governance and Rule of Law Principles for Data-Driven Technologies in Public Health Emergencies (WP3-D3)

The law, where applicable, is stated as of September 22, 2021. However, it has been possible to take account of some later events.

Policy Brief: Good Governance and Rule of Law Principles for Data-Driven Technologies in Public Health Emergencies

WP3-D3

Introduction

As the Covid-19 pandemic swept the world in 2020 and 2021, governments turned to data-driven technologies to help save lives and, ultimately, to pave a way out of lockdown and back to normality. Statistical data informed decisions on when and where to impose a lockdown, when to lift one, what safety measures to impose, and when to lift them, who to prioritise for vaccination, and many other types of future planning. One data-driven response has had more individualised impacts and accordingly been more controversial: the development of Covid-19 technologies or "apps" for use by individuals, companies, and governments to track the status of app-users as in some way safe, vulnerable or risky.

Technologies have been devised, adapted, and used during Covid-19 to limit the spread of coronavirus by tracing infections and enforcing quarantines; to ration resources such as vaccines; and to prove "immunity" status of various kinds. Different countries have built and deployed these technologies in different ways, with varying degrees of respect for notions such as privacy, transparency, and accountability. Some of the more invasive technologies collected or repurposed large amounts of personal data to track citizen movement and day-to-day activity (such as in China) or allowed data so collected to be used for other purposes, such as law enforcement (for example in Singapore). These early approaches, first seen in East Asia, rang alarm bells in the West as the coronavirus arrived, so that from the start of the pandemic, a lively debate was ongoing about how to reconcile public safety with civil liberties and social values of freedom, and indeed if the two goals could really be set up as a dichotomy.

Even in the liberal West though, early attempts at building rights-compliant technologies were conflicted. Much of the debate in the first part of the pandemic swirled around the hoped-for "silver bullet" of the contact tracing app. After some first failed attempts, most European countries deployed technologies that were more rights-protective, driven not just by public concern but by the need to cooperate with the infrastructure policies of large technology companies such as Google and Apple. These "contact tracing app" wars are of lasting significance but have been well documented already and are traced in summary in our Rapid Response Evidence Review (WP3-D1 pages 5-11). Here we have tried to break new(er) ground and provide useful advice to policymakers on how a wider range of data driven technologies have challenged principles drawn from human rights, rule of law and good governance literature[1].

[1] Our reports in WP3 analyse technologies built and deployed in the UK including its constituent devolved governments – health is of course a devolved competence. The picture is sometimes confused by the fact that Wales has separate legislative competence but sometimes shares apps with England, whereas Scotland has chosen throughout to develop its own suite of apps. Northern Ireland has in at least one example (venue check in apps) chosen not to develop its own app at all. On the whole, for lack of time we have concentrated in our research on England and Scotland. We hope our work is also relevant to policymakers in Wales and Northern Ireland (and elsewhere).

This policy document discusses four data-driven Covid-19 technologies deployed in the UK which we have studied in detail:

- contact tracing apps (part of WP3-D1)
- "vaccine passports" (WP3-D1 and WP3-D2A)
- vaccine allocation algorithms (QCovid), (WP3-D1 and in discussions with citizens juries run by the Ada Lovelace Institute)
- venue check-in apps (WP3-D2B)

We also analysed separately in WP3-D2C, the judiciary's attitude to scrutinising the actions of the executive during the pandemic - as there have been no decided cases directly on data-driven COVID technologies, we drew on cases involving data, and COVID-related cases not related to technology.

The success and effectiveness of these technologies rests on public trust and widespread participation. The more people use them or respect their decisions, the more successfully they can achieve their aims. Public trust is underpinned by respect for good governance and the rule of law on the part of the government implementing these technologies. Drawing on research carried out in other parts of this work package, and on insights from the Ada Lovelace citizens juries, the four technologies are thus examined in light of good governance and rule of law principles, with short case studies pulled out to illustrate problems.

The first principle discussed is *transparency*: clear and accessible communication with the public about decisions taken and the reasoning and data behind them. For venue check-in apps and contact tracing apps, transparency was not always ideal during the development process in the UK but has generally been improved by a combination of publishing source code, privacy notices and Data Protection Impact Assessments, as well as making available online statistical dashboards of "pings", venue check in alerts, etc. However, criticisms remain in our studies around vaccine passports, where the England and Wales authorities have been unwilling to provide full access to risk documentation; as well as around the algorithmic basis of QCovid (how it decides who is vulnerable).

The second principle examined is *non-discrimination*: the need for measures to be equal and inclusive, and not prejudice groups with protected characteristics without legitimate proportionate justification. It has been suggested that some Covid-19 technologies are inherently discriminatory; for others, steps may be possible to mitigate possible discrimination. This has of course been a key, heated and ongoing debate in relation to vaccine passports.

Privacy is the third principle discussed. As already noted, we felt the debate over privacy and contact tracing apps was already very well ventilated (see WP3-D1). However, it has been, interestingly, much less obvious as a part of public consciousness in relation to the later development of venue check-in apps. Vaccine passports are again, an apparent source of concern because of their capacity to become vehicles for tracking of movement domestically and internationally; the spectre of social exclusion; and the possibility of retention and scope creep beyond the pandemic raising fears of a "new ID card".

The final principle discussed is that of *democratic accountability and scrutiny*: the requirement, in our context, that executive measures be made according to correct process, subject to scrutiny and respect the rule of law and human rights in a way that is justified, legitimate and proportionate. Most of the Covid-19 technologies discussed in this paper attracted criticism on this basis, given the government's heavy reliance on secondary legislation during the pandemic and the lack of opportunity given, and sometimes perhaps taken, by Parliament and the courts to impose accountability and scrutiny.

We became aware while working through these papers that governance by app – "code as law" – is a relatively unaddressed problem in terms of rule of law and human rights scrutiny in the UK. This issue has come to the fore in COVID-19, where apps such as vaccine passports have the potential to substantially affect rights and freedoms yet are subject to little or no public or legislative scrutiny in their development phases.

This policy brief concludes with a series of recommendations aimed at government policy makers with respect to the development and deployment of data-driven technologies during public health emergencies. These are not intended to be specific to the Covid-19 pandemic, but rather take forward lessons learned from the experience in the UK with the four technologies discussed in this paper.

Covid-19 data driven technologies

Contact Tracing Applications

Contact tracing applications ("apps") for smartphones are used to track the people that an app user is in proximity to, over a period of time. "Proximity" can be defined variously but is typically within two metres for 15 minutes or more. If an app user tests positive for Covid-19, the people they have been in contact with will receive an alert. The aim is to reduce transmission by requesting those who have been exposed to self-isolate, watch for symptoms, and/or book a test.

The Covid-19 pandemic prompted the development of a range of contact tracing applications with various designs.[2] The design which won out in the UK and in much of Europe uses the Google Apple Exposure Notifications (GAEN) infrastructure, a privacy preserving decentralised model. Using Bluetooth, phones communicate with each other through 'digital handshakes', exchanging anonymous keys to make a log of contact and proximity. The app looks for matches between the keys it has collected and the keys of users who have reported a positive test result in the app. As the matching happens on the phone itself, the user's contact log is never transmitted to a third party, and the identity of the positive individual cannot be known. If the app finds a match, it issues an alert to the user that they may have been exposed and should take measures.

The contact tracing apps in the UK are: NHS Covid-19 (England and Wales), StopCovid NI (Northern Ireland), and Protect Scotland (Scotland).

Vaccine Passports

Vaccine passports allow users to prove their immunity status in situations where immunity is a requirement for freedom of movement and for access to certain spaces and services. The aim is to allow countries to reopen safely by reducing the health risk of engaging in social contact, close contact services, and travel. Depending on the country in question, and the service, immunity can be established based on vaccination status, a negative test, or proof of having been recently infected with Covid-19. (We note that "immunity" is a risk-based not absolute characteristic as even full vaccination has a failure rate).

Different countries have different digital tools and applications for delivering an immunity passport. In England, the 'COVID pass' can be downloaded and installed on the NHS App and used for international travel and domestic events.[3] This app pre-dates the pandemic, and was designed to provide access to basic elements of a user's medical history and access to health services.[4] In Scotland, vaccination certification is available in the NHS Scotland COVID Status app,[5] in Wales, the covid pass can be

---

[2] See Rapid Evidence Response Review of Data-Driven Responses to Public Health Emergencies (WP3-D1) and Christiane Wendehorst, 'COVID-19 Apps and Data Protection' in Ewoud Hondius, Marta Santos Silva, Andrea Nicolussi, Pablo Salvador Coderch, Christiane Wendehorst, and Fryderyk Zoll (eds), *Coronavirus and the Law in Europe* (Intersentia, 2021) (freely available at <https://www.intersentiaonline.com/library/coronavirus-and-the-law-in-europe> accessed 27 October 2021).

[3] NHS, 'NHS COVID Pass', <https://www.nhs.uk/conditions/coronavirus-covid-19/covid-pass/> accessed 27 October 2021

[4] NHS, 'NHS App', <https://www.nhs.uk/apps-library/nhs-app/> accessed 27 October 2021

[5] NHS Inform, 'Download the NHS Scotland COVID Status app', <nhsinform.scot/covid-status> accessed 5 November 2021

accessed through a website and shown on a mobile phone,[6] and in Northern Ireland, Covid certificates can be downloaded on the COVIDCert NI app.[7]

Vaccine Allocation Algorithms

Risk assessment models have been developed to help identify individuals at a high risk of hospitalisation or death from Covid-19. As the pandemic develops, more data has been gathered regarding factors which contribute to a higher risk of serious illness or death in the event of contracting Covid-19. In England, the QCovid algorithm was developed to identify individuals who are 'clinically extremely vulnerable'. In the QCovid model, factors such as age, sex, ethnicity and existing medical conditions are assigned a risk value; the model is then applied to existing databases held by NHS digital and at-risk individuals are flagged.[8] Until September 2021 when the programme ended, these individuals were added to the Shielded Patients List[9] and were contacted with information about shielding for their own safety and prioritised for vaccination.

Venue Check in Apps

Venue check-in apps form part of the effort to restrain infectious spread by keeping a record of who has visited a venue and when. In the event of an outbreak being linked to that venue, or if a person who has tested positive reports that they visited this venue, other people who were there in the same timeframe can be alerted. The aim is to reduce the transmission of coronavirus by asking those who may have been exposed to self-isolate, watch for symptoms, or book a test. As with contact tracing apps, venue check-in apps can be built in various ways which are more or less privacy-preserving, but the public debate relating to this in the UK has been far more muted.

While it is always possible to check-in to a venue using pen and paper, digital check-ins mostly involve an individual scanning a QR code with their smartphone. In England and Wales, the official NHS QR code is scanned using the NHS Covid-19 app.[10] In Scotland, the QR code is scanned with the smartphone camera, which opens the Check In Scotland app (if downloaded) or a webpage where the user can enter their details.[11]

The England and Wales app works in a decentralised way, where the venue history is stored only on the phone and the match between venues visited and those flagged as risky is available only to the app user.[12] Exposure alerts are issued within the app to the person's phone. In Scotland the system is centralised, with venue history being transmitted to a central encrypted database and accessed only

---

[6] Welsh Government, 'Get your NHS COVID Pass' (11 October 2021) <https://gov.wales/nhs-covid-pass-prove-your-vaccination-status> accessed 27 October 2021
[7] HSC COVID-19 NI, 'COVIDCert NI Mobile App', <https://covid-19.hscni.net/covidcert-ni-mobile-app/? accessed 27 October
[8] NHS Digital, 'COVID-19 Population Risk Assessment', <https://digital.nhs.uk/coronavirus/risk-assessment/population> accessed 27 October 2021
[9] NHS Digital, 'Coronavirus (COVID-19) risk assessment', <https://digital.nhs.uk/coronavirus/risk-assessment> accessed 27 October
[10] UK Health Security Agency, 'Guidance: Maintaining records of staff, customers and visitors to support NHS Test and Trace' (20 July 2021) <https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace> accessed 27 October 2021
[11] Mygov.scot, 'How to use the Check In Scotland QR code' (9 August 2021) <https://www.mygov.scot/help-qr-check-in> accessed 27 October 2021
[12] UK Health Security Agency, 'Guidance: NHS COVID-19 app: anonymisation, definitions and user data journeys' (28 September 2021) <https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/anonymisation-definitions-and-user-data-journeys> accessed 27 October 2021

when a venue is associated with an outbreak.[13] Exposure notifications are communicated by phone, email, or post. Northern Ireland has not developed a check-in app and relies on paper records of customers visiting a venue.

The Legal Framework

Enabling legislation

This is an indicative rather than comprehensive list. One reason for this is that in almost all cases, these apps have been developed, and data gathered, using general statutory powers rather than "bespoke" laws. The main exception is vaccine passports, which were enabled in Scotland by the Health Protection (Coronavirus) (Requirements) (Scotland) Amendment (No. 2) Regulations 2021. Given the pause in roll out, there is no equivalent law in England mandating certification of immunity to enter certain venues or large events. There is however limited delegated legislation to mandate proof of immunity for care home workers. In both cases however, however, the law does not specifically mandate use of any particular digital app. It asks only (in Scotland) for there to be a "reasonable system" for checking that persons accessing designated events or premises are vaccinated or otherwise have immunity status; and in England, for there to be "evidence" of full vaccination or clinical exemption.

Contact Tracing	• England: National Health Service Act 2006, section 2A duty to protect public health. • Scotland**:** Public Health etc. (Scotland) Act 2008, section 1 duty to make provision to protect public health. • Wales: Government of Wales Act 2006, section 83 agreement with the Secretary of State for Health and Social Care for provision of the NHS Covid 19 App. • NI: The Health and Social Care (Reform) Act (Northern Ireland) 2009, sections 2(1), 2(3)(g), and 3(1)(b) duties to promote the health care system and provision of services and programmes for health.
Vaccine Passports	• England: Under the Covid-19 Public Health Directions 2020, the Department of Health and Social Care has directed NHS Digital to collect and analyse data, and develop operating information and communication systems in relation to Covid-19. The legal basis for the directions can be found in the Health and Social Care Act 2021 and the National Institute for Health and Care Excellence (Constitution and Functions) and the Health and Social Care Information Centre (Functions) Regulations 2013/259. The COVID-19 vaccine passport requirements in care home settings are found in the Health and Social Care Act 2008 (Regulated Activities) (Amendment) (Coronavirus) Regulations 2021. • Scotland: Health Protection (Coronavirus) (Requirements) (Scotland) Amendment (No. 2) Regulations 2021 amending the Health Protection (Coronavirus) (Requirements) (Scotland) Regulations 2021, in force on 1 October 2021.
Vaccine Allocation Algorithms	• England: Under section 254 of the Health and Social Care Act 2012, NHS Digital has been directed to collect and analyse data for coronavirus under the Covid-19 Public Health Directions 2020

[13] NHS Scotland Test&Protect, 'The Check In Scotland digital service: Data Protection Impact Assessment' (20 April 2021), 29

Venue Check-in Apps	• England: prior to July 2021 venue check-in was mandatory under The Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020, passed using powers in the Public Health (Control of Disease) Act 1984 • Scotland: Health Protection (Coronavirus) (Requirements) (Scotland) Regulations 2021

Limiting Legislation

As above, limits to the lawfulness of apps come from general regimes of law, not from bespoke statutes (as has been the case in some other jurisdictions such as Australia.) This is not a comprehensive list, but it is indicative of the major sources of challenge. We do not go into details here about the common law of judicial review, which to date has been the main vehicle for challenge.

Data Protection Law	**Privacy Law**	**Equality Law**	**Medical Law**
The GDPR, implemented into UK law by the Data Protection Act 2018, is the key data protection legislation in the UK. The GDPR applies whenever personal data is collected and processed. Article 5 lists the data protection principles at the heart of the instrument: • Lawfulness, fairness and transparency • Purpose limitation • Data minimisation • Accuracy • Storage limitation • Integrity and confidentiality (security) • Accountability The data used by the technology discussed in this brief is often health data, which is a special category of data and subject to additional protection under Article 9 GDPR.	Whenever personal data is involved, the right to privacy will be applicable. Article 8 of the European Convention on Human Rights (ECHR) protects the right to private life, and was incorporated into UK law by the Human Rights Act 1998. The right is a qualified right, which means that the state can interfere with privacy when necessary in a democratic society, to protect particular interests, including health. In order to lawfully limit the right to privacy, there needs to be a legal basis in domestic law and the interference must be necessary and proportionate. The European Court of Human Rights determined that the right to privacy includes medical data (*Z v Finland (1988)*[14])	The Equality Act 2010 protects people from discriminatory treatment unless said treatment is a proportionate means of achieving a legitimate aim. Discrimination based on the following protected characteristics is unlawful: age, disability, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation (s.4).	Medical devices, including software used for medical purposes, must meet certain regulatory standards. Devices that meet these standards are marked with 'CE'. The standards are set out in the Medical Devices Regulations 2002 (SI 2002 No 168, as amended), which incorporates into UK law Directive 93/42/EEC on medical devices (EU MDD). The Medicines and Healthcare Products Regulatory Agency is responsible for medical devices in the UK market.

[14] Case of *Z. v. Finland, App no. 22009/93* (ECHR, 25 February 1997)

TRANSPARENCY & England and Wales COVID Pass

Since May 2021, people in England have been able to display and download their COVID status through the NHS App. The COVID pass certifies a person's immunity status, whether through vaccination, testing, or infection. The decision to use the NHS App instead of the NHS Covid-19 app to certify health status was driven by issues with Apple's privacy policy and the Google/Apple Emission Notification (GAEN) technology which underlies the NHS Covid-19 app. The NHS App pre-dates the pandemic, but was then little used and an updated DPIA has not been published to explain how data is collected and processed in relation to the COVID pass function. While there is not always an obligation under the GDPR to publish a DPIA, this has come to be seen as good practice when societally impactful new technologies are introduced by public bodies, and particularly in the context of Covid-19 responses. Uncertainty therefore remains as to how the app uses data and who the data is shared with.

Good governance and rule of law principles

Building trust in data-driven technologies requires that these respect good governance and rule of law principles. The principles discussed in this section are those that feature prominently in the research carried out for the other outputs of this work package, and those noted as particularly relevant in citizen jury discussions.

Transparency

Transparency in the context of public health emergencies means communicating to the public in a clear and accessible way the decisions being made and the reasons behind them. When it comes to data driven responses to these emergencies, it also means being open about the quality, robustness, and shortcomings of the underlying data.[15]

A clear concern that arises for all the data driven technologies is who will have access to data that relates to identified or identifiable individuals, and how will it be used. People have a right to this information, as transparency is a legal requirement under the GDPR. Data controllers are responsible for processing data in a transparent way in relation to the data subject, and must communicate about a person's data in a 'transparent, intelligible and easily accessible form, using clear and plain language' (Art. 12). This includes where there has been a data breach (Art. 34).

Efforts to comply with this requirement can be seen in the publishing of Data Protection Impact Assessments (DPIA) and privacy notices. For example, the DPIAs for contact tracing and venue check-in apps state clearly who will process data and under what conditions, and indicate how long data will be retained for. Despite these measures, a lack of transparency is an ongoing concern among members of the public,[16] and questions such as the following continue to arise:

> *"Who will my covid vaccination status be shared with, and how will they use that information? If I am placed on the Shielded Patients List, who will see that and how will that status affect me? Can my venue check-in data be passed onto the police or other third parties?"*

[15] Rachel Allsopp, 'Mapping the Data-Driven Landscape' (*OMDDAC,* 25 January 2021) <https://www.omddac.org.uk/news/mapping-the-data-driven-landscape/> accessed 17 September 2021

[16] Discussions during the Ada Lovelace citizens juries that were held as part of this project

Part of building trust through transparency is extending transparency to the data sets themselves, especially as the success of data-driven technologies rests on the quality of the underlying data. Concerns have been raised about a lack of transparency surrounding issues with the data, including errors, omissions, and out-dated information.[17] A related set of concerns touch on the presentation of data as objective and factual, which obscures the biases, values, and assumptions present in the data.[18] Surfacing these issues requires that the data driving the technologies be disclosed and open to enquiry.

UK courts have been deferential to the government's approach of limited disclosure of the data underlying Covid-19 responses. In *Manchester Airport v SS Transport* (2021), claimants argued that the data used by the government to make decisions about international travel was not clear. The decisions to designate a country as red, amber, or green (with consequences for restrictions placed on individuals when they returned to the UK) were made without sufficient explanation, it was claimed. The Court held that the government did not need to disclose how decisions were reached, and that the decision to publish the data behind the decisions was a political judgment not a legal duty. In so doing, the Court missed an important opportunity to set down an expectation of transparency surrounding data.

Discrimination

Responding to public health emergencies with data-driven technologies must be approached carefully to ensure that the technology neither excludes parts of the population it is designed to help nor adversely and unfairly impacts them. Discrimination can be direct or indirect. In the Covid-19 context, direct discrimination would arise if, for example, an employer refuses to employ an otherwise qualified individual because they refuse the vaccine on religious grounds. Indirect discrimination could occur if, as a result of mandatory vaccines in the workplace, fewer individuals from particular racial, ethnic, or belief backgrounds are employed because of lower vaccine uptake rates among those communities. Indirect discrimination arises where measures are put in place for everyone, but they affect some individuals unfairly based on protected characteristics. Both forms of discrimination are unlawful if connected to a protected characteristics listed in the Equality Act 2010 (see above), unless there is an objective justification, and the means are proportionate to achieving a legitimate aim.

Much of the discussion on discrimination and Covid-19 technologies focuses on vaccine passports ("COVID passes"). Many groups have raised concerns that vaccine passports will lead to unlawful discrimination, including the UK Equality and Human Rights Commission and the Public Administration and Constitutional Affairs Committee.[19] Such measures may exacerbate

TRANSPARENCY & QCovid

When automated decisions are made by AI technologies, transparency is often challenging. Algorithmic logic is often described as a "black box"; it is difficult to know what caused the decision reached or accordingly how to challenge it. The developers of QCovid, which ranked vulnerable people for access to vaccination, implemented full transparency by making their algorithm open source and available to public view. However, source code is not understandable to much of the general public; comprehending the details of how QCovid works requires expertise. The goal of transparency – to facilitate understanding and allow informed questioning – is therefore not met by simple disclosure of code. NHS Digital stepped into this gap with an accessible explanation on their website of how the QCovid algorithm worked and the factors taken into account for risk assessments. Despite these positive efforts, QCovid has remained controversial with evidence that patients were incorrectly added to the Shielded Patients List. In such cases, the failure may be as much down to erroneous or biased data as the actual algorithm; scrutiny access to datasets is thus also important, raising difficult issues about privacy/ confidentiality.

[17] Rapid Evidence Response (*supra* n2)
[18] Rapid Evidence Response (*supra* n2)
[19] Rapid Evidence Response (*supra* n2); Big Brother Watch
Under Covid Certification' (2 April 2021) <https://bigbr
Denied-Big-Brother-Watch.pdf> accessed 15 September 2
19 vaccine passports have in society? Findings from a rapid expert deliberation to consider the risks and benefits of the potential roll-out of digital vaccine passports' (17 February 2021) <https://www.adalovelaceinstitute.org/summary/covid-19-vaccine-passports/> accessed 15 September 2021; 'No jab, no job'? Employment Law and Mandatory Vaccination Requirements in the UK (WP3-D2A)

social inequalities, particularly among groups that are already marginalised and disadvantaged, and which have lower vaccine uptake rates. Undocumented migrants and refugees may be fearful to come forward to receive the vaccine or to access their vaccine passport for fear that their information will be used for other purposes. In addition to these groups, vaccine passports may exclude individuals who cannot receive the vaccine due to medical issues, disability, pregnancy, or age, though some of these issues have diminished in the UK as vaccine access has widened.

As between different countries, vaccine passports reinforce mobility and connectivity divides by deciding who can travel internationally. While the West has largely carried out a successful vaccine roll out, much of the developing world is lacking vaccination supplies and more than a billion people are undocumented and unable to prove their identity.

Discrimination can result from barriers to accessing the technology, including money, language, and literacy barriers. The UK contact tracing apps for smartphones require certain technical specifications to work, excluding those with older phones, or no smartphone at all. In some cases, paper alternatives are offered, such as with venue check-in and vaccination passports, but these can have downsides (paper-based venue check-in is often less privacy friendly and can have more onerous self-isolation requirements[20]). For people whose first language is not English, language can be a barrier: the NHS Covid-19 app for England and Wales is available in 12 languages but Protect Scotland and StopCOVID NI are only available in English. Another barrier is digital literacy. Certain groups, including the elderly, are less accustomed to using technology and may require additional assistance.

A final point concerns the discrimination that can arise when the data underlying data-driven technologies is biased and/or incomplete. Levels of trust in healthcare and health institutions among minority communities in the UK are low, with members of those communities being less likely to seek care when they need it.[21] This can affect how well minority communities are represented in NHS data, and therefore how tailored the data-driven responses and technologies are to their needs. Members of minorities are also less likely to use Covid-19 related technologies, reinforcing the data gap.[22]

DISCRIMINATION, SCRUTINY & mandatory vaccination in care homes

As vaccination rates rise in developed countries, rules requiring certain workers to be vaccinated are becoming more common. In England, regulations that came into effect in November 2021 require care home workers to prove they have received a full course of an approved vaccine. In addition to regular employees, this requirement extends to other workers who enter a care home to provide a service. This requirement will be extended in spring 2022 to all NHS workers.

The regulations provide for an exemption on medical grounds, but belief-based objection to the vaccine is not accepted. Guidance issued alongside the regulations describe them as exempt from certain provisions of the Equality Act, relating to claims of unfair dismissal on the basis of age, disability, religion, or belief, justifying this on the basis that the measure is proportionate. However, this assertion is legally questionable. Effectively, guidance is being put forward as trumping primary legislation and repelling the judgment of the courts. This is worrying under the rule of law as guidance has no legislative status.

While there are clear arguments in favour of compulsory vaccination in care homes, the measure is likely to have a disproportionate impact on BAME groups that statistically have higher rates of vaccine hesitancy. The question of whether there is unjustified indirect discrimination here, which is an important one, which cannot be settled by fiat of guidance and court challenges have been almost always repelled during the pandemic in the English courts.

[20] See 'Venue Check-In' or 'Presence' Apps (WP3-D2B)
[21] Public Health England, 'Beyond the data: Understanding the impact of COVID-19 on BAME groups' (June 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/892376/COVID_stakeholder_engagement_synthesis_beyond_the_data.pdf> accessed 28 October 2021, 7-8
[22] Liz Dowthwaite, Joel Fischer, Elvira Perez Vallejos, Virginia Portillo, Elena Nichele, Murray Goulden, Derek McAuley, 'Public Adoption of and Trust in the NHS COVID-19 Contact Tracing App in the United Kingdom: Quantitative Online Survey Study' (2021) vol. 23(9) *Journal of Medical Internet Research*

Respect for Human Rights: Privacy

Public health emergencies impact a number of human rights, including the rights to life, to freedom of movement, and to liberty. This section will focus on the right to privacy, as this right and its balance with public safety has been particularly controversial during the pandemic.

The right to privacy – found in article 8 ECHR - protects individuals from unjustified intrusion into their private lives. The collection of data about someone's movements, who they come into contact with, and their medical history, certainly qualifies as intruding into the private domain;[23] the question, in the Covid-19 context, is whether the intrusion is necessary and proportionate in order to protect health or the rights and freedoms of others.

Ascertaining whether a measure is necessary involves asking if there was a less intrusive way of protecting the aim. The UK contact tracing apps are very privacy protective, as they are all built on the Google and Apple Exposure Notification (GAEN) protocol, which prohibits the collection of location data through GPS and requires that proximity and contact data be stored only on the phone and not shared centrally. Such data as is shared is anonymised so that it does not qualify as personal data.[24] It is hard in such a case to argue that a less intrusive method was possible.

By contrast, the QCovid algorithm which was built to identify and rank vulnerable patients for access to vaccine priority, processes health data, an especially sensitive category of personal data. However, it cannot be anonymised as identification of individuals at particular risk of hospitalisation or death from Covid-19 would not then be possible. A less intrusive approach would not therefore achieve the same ends. In the case of vaccine passports, consensus is lacking on whether they achieve the aim of protecting health by encouraging vaccination [25] and preventing infection.[26] Their necessity is therefore still subject to debate.

The privacy assessment then turns to proportionality. Is the intrusion into private life through the collection and processing of personal data proportionate to the aim of protecting health

PRIVACY & Venue Check-In Apps

When designing their respective venue check-in apps, authorities in England/Wales and Scotland took different approaches. The former, constrained by Apple and Google's privacy policy, opted for a decentralised, privacy protective protocol. The latter, not so constrained, opted for a centralised system. Any time personal data is kept in a central store, privacy is an immediate concern, and the DPIA for the Check In Scotland app acknowledges that the public would likely perceive a centralised system negatively. Despite this, the Scottish authorities argue that the system is proportionate because of the safeguards in place. There are strict rules on data retention (21 days), access to data (multiple layers of approval needed), and encryption (personal data double encrypted).

In terms of necessity, the DPIA sets out that collecting venue check-in data centrally protects against data loss, as users cannot delete data before being alerted of an outbreak. This assertion is untested and seems contestable given the different architecture adopted in England for the same result. Interestingly the kind of controversy over privacy and centralised systems that contact tracing apps attracted in the early days of the pandemic was not replicated in relation to venue check in in Scotland.

[23] For an overview of how article 8 ECHR covers personal data, see European Court of Human Rights, 'Guide to the Case-Law of the European Court of Human Rights: Data protection' (30 April 2021) <https://echr.coe.int/Documents/Guide_Data_protection_ENG.pdf> accessed 20 September 2021
[24] 'COVID-19 Apps and Data Protection' (*supra* n2)
[25] See WP3-D1. See also : Alexandre de Figueiredo, Heidi J. Larson, and Stephen Reicher, 'The potential impact of vaccine passports on inclination to accept COVID-19 vaccinations in the United Kingdom: evidence from a large cross-sectional survey and modelling study' (medRxiv, 1 June 2021) <https://www.medrxiv.org/content/10.1101/2021.05.31.21258122v1.full> accessed 15 September 2021
[26] Smriti Mallapaty, 'Can COVID vaccines stop transmission? Scientists race to find answers' (*Nature*, 19 February 2021) <https://www.nature.com/articles/d41586-021-00450-z> accessed 28 October 2021

or the rights and freedoms of others? Much of the discussion around Covid-19 technologies focuses on this question.

Relevant considerations for proportionality include, for example, the fact that using contact tracing apps is voluntary and no personal data is shared (in the GAEN model), and for QCovid, the existence of limits on who can access the risk assessments (only GPs and clinicians who owe duties of professional confidentiality). For vaccine passports, context is particularly important: requiring a passport to access essential services may be disproportionate whereas for accessing an entertainment venue it may not be. These concerns are weighed against the importance of the aims the technologies seek to achieve.

Questions of privacy versus effectiveness are also relevant to proportionality. It is often thought that the more data collected, the more detailed the data set, and the more accurate the conclusions that can be drawn from the data; this allows for better understanding of the pandemic and can produce more effective responses to it. However, the more data collected, the more privacy invasive a technology is. In the early stages of the pandemic, some countries built contact tracing apps that collected personal data, such as location data, and stored this in a centralised database. In England, the first version of the NHSX contact tracing app did not collect location data as such but did store proximity data collected by Bluetooth in central databases. This approach was justified as providing broader epidemiological insights to help control the virus, though this assertion remains contested. In the event, partly due to privacy concerns, but primarily due to the action taken by Google and Apple to impose its own policies via its mobile phone duopoly, England and almost all European countries quickly changed to privacy preserving GAEN based apps instead. The contact tracing privacy wars thus stand as a natural experiment into the (asserted) balance between privacy and effectiveness. They also illustrate the power a few private tech companies now assert in controlling technological infrastructures, even in a domain like health and safety in emergency times where state sovereignty would normally be unquestioned. We return to this point below.

Proportionality should be a continuing assessment. Several privacy concerns around Covid-19 technologies relate to issue of scope creep and post-pandemic retention, particularly in relation to vaccine passports. Once the infrastructure is in place to require users to provide health credentials, other statuses can easily be added – immigration and citizenship status, residence, employment – and checked by a variety of actors such as law enforcement agencies or state welfare bodies as well as private service providers. This has created concern that vaccine passports may become a way of “introducing ID cards through the backdoor” and perpetuating illegitimate state or other surveillance, particularly of disempowered groups such as BAME or immigrant communities. That a technology is deemed proportionate at its introduction, does not mean it will remain so as use evolves.

Vaccine passports also present data protection challenges. In particular, the use of vaccine passport apps by private actors - hospitality venues, shops, hairdressers, etc. – may involve the collection of sensitive personal data which for private actors, usually requires explicit consent under the GDPR. This also requires them to collect as little data as possible, have a lawful basis for processing this data, and adequately protect it.

Democracy, Accountability, and Scrutiny

Good governance and the rule of law require that data-driven technologies be subject to democratic scrutiny in order to hold the government to account. Such scrutiny helps to ensure that measures comply with procedural and substantive rules, including the protection of individual rights. The UK government has come under significant criticism on several points in this respect.

First, extensive use has been made of regulations – which are a form of delegated legislation – during the pandemic, with primary legislation largely avoided. Regulations can be passed more quickly, but are subject to much more limited parliamentary debate and scrutiny compared to primary legislation.[27] The legal requirement for care home staff in England to be fully vaccinated against Covid-19 by November 2021 was brought into effect using regulations, despite the impact such a measure has on autonomy, privacy, and employment. Similarly, throughout the vaccine passports debate, many stakeholders have stressed that such a measure should only be introduced through primary legislation. However even in the parts of the UK where vaccine passport schemes have been mandated, delegated instruments have so far been employed, with minimal debate.

Second, and even more challenging from a parliamentary scrutiny point of view, is the repeated use of guidance during the pandemic to effectively make law and sometimes even challenge primary law. In August 2021, guidance on the regulations requiring care home staff in England to be fully vaccinated asserted that these regulations formed an exception to part of the Equality Act 2010 (see above, Discrimination). This exception is not explicitly included found anywhere in the regulations themselves, creating legal uncertainty.

Third, a less discussed point about scrutiny is that technology – in the wide, non-data-specific sense of the word - is generally simply seen as a means to an end in terms of public policy; developing software to implement policy is no more important or special than buying an office to do it, or using railway track. Yet software design – especially in a data-driven algorithmic world – is not a mere practical step, but a process which embeds and enforces values in regulatory "code". As the pandemic has proven, how software or an app is built, what data it uses (or doesn't), how it is deployed, who are the target users, can all crucially affect rights and freedoms; yet we have no established "due process" rules about building or using public sector high-stakes apps. Regimes are beginning to emerge, such as the EU's proposed AI Act, that recognise that it is important to have rules about how "high risk" AI is built and deployed, especially where it uses machine learning. As matters stand in the UK though, the only legal tools during

ACCOUNTABILITY, SCRUTINY & Judicial Deference

UK courts have heard a number of cases brought as challenges to government measures in response to Covid-19. These have included challenges to the closure of places of worship and businesses, the legal requirement to self-isolate, restrictions on gatherings, and the calculation of economic assistance to those whose employment was affected by Covid-19 measures. In most cases, the courts have deferred to government decision-making and proportionality assessments, granting a wide margin of appreciation and refusing to second guess the government's approach. This extends to not questioning the data underlying decisions - taking this data to be accurate without examination from a scientific perspective

One case that did not follow this trend of judicial deference was *Philip v Scottish Ministers (2021)*, in which the judges of the Scottish court assessed in detail the proportionality of the closure of places of worship, deeming the interference unlawful.

This widespread judicial deference is concerning given the lack of parliamentary scrutiny of Covid-19 regulations. The result is a lack of oversight of government action both before and after the introduction of data-driven responses.

[27] Brigid Fowler, 'The care home Covid vaccination Regulations: a case study in problems with the delegated legislation system' (*Hansard Society,* 9 August 2021) <https://www.hansardsociety.org.uk/blog/the-care-home-covid-vaccination-regulations-a-case-study-in-problems-with> accessed 28 August 2021

the pandemic to control or even observe how COVID-19 technologies were designed and used are derived from general law (see boxes earlier) : data protection, especially impact assessments; FOI; privacy notices; actions for judicial review. Only one technology deployment has so far been rejected as invalid by judicial review – police use of face recognition in *Bridges v S West Police,*[28] a non-COVID case – so we are at the very start of work here.

Lack of *judicial* oversight of data-driven technologies is also a feature of pandemic governance. This has several causes. First, our research shows what seems a high degree of judicial deference to executive acts during the pandemic and the grant of a very wide margin of appreciation. This is understandable in a national crisis, but combined with the lack of legislative scrutiny already noted, this has added up to a near vacuum of democratic oversight. If we then add in the fact that, as noted, the legal system has not yet really worked out how to apply scrutiny to software with regulatory impact, we end up with a worrying lack of accountability.

Finally, we add an observed tendency by the government to limit the number of cases against executive measures reaching adjudication by the courts, eg by conceding at a pre-action letter stage, rather than proceeding to contest. When a measure is challenged, the government's tendency has been to alter or withdraw the guidance or practice, or even change the law, rendering the case 'academic'. In such circumstances, cases will rarely proceed further as a "point of principle". This strategy limits the opportunities for oversight by the courts and defers or impedes the creation of useful precedents.

A last issue is that the power of private companies in the pandemic has also raised democratic concerns. The GAEN protocol became the predominant system used for contact tracing apps in Europe, in part due to privacy concerns but mainly because non GAEN apps did not function properly on Apple phones. Because of their control of communications infrastructure, technology companies were arguably able to dictate what approach sovereign states took towards balancing privacy and public safety.

Recommendations for Policy Makers Developing and Deploying Data-Driven Solutions in Public Health Emergencies

Our cases studies show that data-driven technologies, especially those developed to impinge on important freedoms such as the right to leave the home, go to work or partake in public life, or liberties such as to access health resources and vaccines, have the potential to infringe upon human rights and discriminate against particular groups or individuals. Accordingly, we make the following recommendations to policymakers.

Transparency

- The nature, goals and functionality of data-driven technologies, including details as to data collected and processed, who it is shared to, the use of algorithmic logic, the impacts on users, and the design choices made eg as to training sets or testing, must be made transparent and accessible to the public, ideally before time of deployment.
- We recommend this should be done by means of the publication of a Technology Impact Assessment (TIA – see further below).

[28] [2020] EWCA Civ 1058. See further discussion on this issue in L. Edwards, R. Wiliams and R.Binns *Legal and Regulatory Frameworks Governing the use of Automated Decision Making and Assisted Decision Making by Public Sector Bodies (*Legal Education Foundation, 2021) at https://docs.google.com/document/d/1EhkiaIlko_9Yccn9u2YLHzFEZ6TEq2JH8ThRM7m8l-4/edit .

- However, when dealing with technology, which is often inherently complex and inaccessible to large sections of the population, publishing technical details such as source code, or legal documents such as privacy notices and TIAs, is insufficient to satisfy the need for transparency. For the public to genuinely understand the way a certain technology has been developed and deployed, additional efforts must be taken to "translate" technical and legal details. Issues of age, language, and lack of technical literacy must also be considered.
- The data sets that underlie data-driven responses and technologies should, as far as possible, be made publicly available for scrutiny throughout the life of the technology. Ways to resolve conflicts with the privacy rights of individual data subjects eg decentralised access as in Open Safely,[29] anonymisation, and data trusts,[30] should be explored.
- If an existing technology has been adapted to assist with a public health emergency, there should be transparency surrounding the changes made and the new ways in which data may be collected, processed, and the purposes to which it will be put.

Human rights, privacy and discrimination

- Privacy has been perhaps the issue most hotly debated in relation to the use of data-driven technologies during the pandemic, but other human rights are also impacted such as freedom of speech, of assembly, of worship, freedom from detention.[31] We recommend, as discussed in detail below, that existing requirements for DPIAs should be supplemented by a Technology Impact Assessment (TIA) which should be introduced to restrain ex ante disproportionate breaches of rights and freedoms and ensure good governance.
- We also recommend that as a default the most privacy protective option for building technologies in these circumstances must be taken. For example, when building a contact tracing or venue check in app,[32] a decentralised approach must be preferred unless it is clearly shown on scientific evidence that it is necessary a less privacy-preserving approach be taken.
- The government should regulate when and under what conditions private actors can require customers or employees to prove health status ; and provide an easy way to challenge such mandates eg by resourcing existing regulators such as the EHRC and ICO to provide bespoke help, or by appointing an ombudsman to receive complaints and challenge decisions or launch legal proceedings where appropriate.
- Data-driven technologies which impinge on human rights and civil liberties must be terminated, and data they have collected deleted, once the public health emergency has ended, unless there is a new explicit consent. Benchmarks should be identified in connection with infection rates, mortality rates, and other relevant data points that signal the moment at which the use of data-driven technologies is no longer needed. These benchmarks should be publicly available and specific. A plan for termination should exist as part of the TIA (see below).

Democratic scrutiny and accountability; issues of private power

- Despite the need to act quickly in times of emergency, the democratic process must not be side-stepped. The *legislative basis* for introducing data-driven technologies in a public health emergency should be clear, and where possible, specific. Where reliance is placed on broadly formulated powers in primary legislation or common law, an assessment should be made by the appropriate Select Committee of whether such reliance is appropriate, or

[29] OpenSafely : https://www.opensafely.org/.
[30] See eg Ada Lovelace Institute *Exploring legal mechanisms for data stewardship* (4 March 2021) at https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/
[31] See WP3-D1.
[32] See WP3-D2B.

whether the technology requires more in-depth parliamentary scrutiny and explicit legislative approval.

- The use of secondary legislation to introduce measures that affect rights and freedoms should be minimised.
- The use of guidance to guarantee or impinge on rights and freedoms rather than merely interpreting or elucidating the law is unlawful and must be avoided.
- We suggest the courts should develop guidelines for *post factum* scrutiny of the use of data driven technologies, since they already receive little or no legislative scrutiny during development and guiding precedent is currently minimal.
- We recommend that guidance be drawn up as to best practice in the handling by the courts of scientific, statistical, and technological evidence. We also promote for consideration the idea of an independent agency to act as "friend" to the court to explain such evidence, who acts neither for complainant nor public body. This role might be taken by a new agency or by relevant existing regulators as long as their independence is secure.
- The government should investigate whether adequate measures exist to restrain the power of private companies which provide vital technological infrastructure to determine the impact and deployment of data driven technologies, or if extra legal measures to protect human rights are necessary.
- Private sector actors effectively performing public roles during public health emergencies should be subject to similar level of scrutiny as public bodies. We recommend laws such as FOI, judicial review, data protection, equality law and procurement are examined to see if this result is guaranteed and if not what reform is necessary.

Technology Impact Assessments

- We recommend that before a public body can deploy a data-driven technology which substantially affects rights or freedoms of individual or groups, they should be required to publish a Technology Impact Assessment (TIA). We note the many current parallel initiatives proposing IAs for tech and AI, such as the proposed EU AI Act,[33] the forthcoming White Paper of the Office for AI and the Algorithmic Impact Assessment proposal of the APPG on the Future of Work;[34] and we suggest an independent commission should draft a proposal for a TIA to be in operation before future health emergencies, when as we have seen, legislative and judicial scrutiny tends to be constrained.
- TIAs should move beyond current data protection impact assessments, which are in any case not always mandatory and not required to be published, towards more holistic impact assessments, which investigate risks related to all human rights, as well as efficacy, practicability, sustainability and ethical concerns. TIAs should at minimum consider whether a technology meets a legitimate aim, meets transparency, rule of law and good governance standards in its development, and, ensure the impact of a given technology is proportionate to the aim it seeks to achieve.
- We recommend this assessment should as far as possible be repeated during the lifecycle of the technology and fed back into design decisions (including a decision that the technology should not be further pursued).
- TIAs should be mandatory for data-driven technologies rolled out by government, law enforcement and public sector agencies to track, profile and make automated decisions about individuals, groups, or entire populations, especially during a national emergency.

[33] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS COM/2021/206 final.

[34] See https://www.theguardian.com/technology/2021/nov/11/algorithmic-monitoring-mental-health-uk-employees

- We also commend TIAs as best practice for the private sector. If private sector bodies are taking on public sector roles eg as providers of primary healthcare apps, they should be subject to the mandatory requirement.
- TIAs should involve consultation of the public, especially vulnerable or marginalised groups likely to be affected. The views of the public should be given due regard including in decisions whether not to pursue the development or deployment of certain technologies.
- TIAs should be made public, except in exceptional circumstances in a state of emergency, before the technology in question is deployed, with sufficient opportunity and a procedure for challenge from the public and civil society.

BINGHAM CENTRE FOR THE RULE OF LAW

Newcastle University

Charles Clore House
17 Russell Square
London WC1B 5JP

T 020 7862 5151
F 020 7862 5152
E binghamcentre@biicl.org

www.binghamcentre.biicl.org

The Bingham Centre for the Rule of Law is a constituent part of the British Institute of International and Comparative Law (www.biicl.org).

Registered Charity No. 209425

BIICL

British Institute of International and Comparative Law