Douwe Korff

Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

SHORT NOTE

The proposed new UK data protection regime & on continuing UK surveillance regime

NB: This short note follows on from a number of submissions by Ian Brown and myself on the inadequacy of UK data protection law, provided to the EP and others in late-2020, with updates in 2021.[1] The note summarises more comprehensive analyses of the proposed UK data protection regime that are still in preparation. It is provided for the information of members of the European Parliament's Civil Liberties (LIBE) Committee visiting the UK in November 2022. It also revisits the issue of UK surveillance. A one-page handout with the main conclusions is also provided. In several respects, I simply defer to the parallel note prepared by Michael Veale for the Committee. There are two attachments.

1. General context

The present UK government's actions, like the previous Boris Johnson and (brief) Liz Truss administrations, are driven by three main considerations:

- a desire for freedom to adopt laws for the UK without constraint from European or international law (*viz*. also the so-called "British Bill of Rights" that would be better named the British Get Rid of European Rights Bill);
- distrust of "judicial overreach" and especially of European court jurisdiction and European court interpretations of law; and (somewhat paradoxically):
- extensive use of executive legislative powers with limited oversight from Parliament.

(For details, see Attachment 1)

2. The DPDI Bill

These considerations also underpin the proposed new UK data protection regime, set out in the **Data Protection and Digital Information (DPDI) Bill**. More specifically, the Bill seeks to use the UK's "post-Brexit freedoms" to:

- reduce what it sees as "burdens on businesses that impede the responsible use of personal data", i.e., reduce data protection requirements;
- facilitate easier sharing of personal data, in particular between private companies and public bodies, and for secondary research purposes;
- make it easier for businesses to use automated decision making tools; and
- "*use … repatriated 'adequacy' powers from the EU to remove inappropriate barriers to the flow of UK personal data overseas in support of trade, scientific collaboration and national security and law enforcement cooperation*".

3. Overall conclusion concerning the DPDI Bill:

If the Bill is adopted as proposed, the UK data protection regime will be significantly less strict than – i.e., not "essentially equivalent" to – the EU GDPR regime. It could also:

- **impose on EU companies obligations that would conflict with the obligations that the EU GDPR imposes on them;**
- **allow EU companies to "launder" personal data through the UK in lightly pseudonymised form; and**
- **turn the UK into an offshore "data haven" through which data that cannot be sent from the EU/EEA to "inadequate" third countries such as the USA can be routed.**

3.1 Personal data

The Bill re-writes and qualifies the concept of "personal data" that is at the heart of data protection law in ways that significantly affect the application of the law:

- different from the EU GDPR, under the Bill, "**singling out**" of individuals without using identifiers or person-specific factors will not be regarded as "identifying" the individual;
- the Bill clearly seeks to facilitate the **making available of de-identified data to "other persons"** in ways that do not meet the EU GDPR standards; and
- processors and (especially) "other persons" who process **pseudonymised data** are treated as if they do **not** process "personal data" at all.

All of these changes directly contradict the clarifications of EU law set out in Recital 26 of the EU GDPR, the guidance from the EDPB, and the case-law of the Court of Justice.

(For details, see Attachment 2)

3.2 Lawful and necessary processing for specified purposes and compatible purposes

Disclosing data to UK public bodies:

The Bill will give all UK public authorities the right to determine unilaterally what data that are held by private entities – any private entities including e-communication companies, educational, health and financial institutions – they regard as "necessary" for their tasks; and the requested entity must then provide the requested data.

Contrary to EU law, such mandatory disclosures are stipulated to always be "necessary" for the requested purpose and always "compatible" with the original purpose for which the data were processed by the private entity. Moreover, under the extra-territorial clause in the Bill (see at 3.6, below), non-UK companies including EU companies would be subject to the same mandatory disclosure requirements – which can clearly lead to conflicts with the EU GDPR.

In respect of other kinds of disclosures, the bIll fails to stipulate (as the EU GDPR does) that such disclosures must "*respect the essence*" of the rights affected and must be "*proportionate*" to the stated aim of the disclosure.

Secondary uses of personal data for research, archiving or statistics (RAS)

The Bill greatly facilitates secondary uses of personal data, especially pseudonymised data (that will often not be regarded as personal data under the UK law, even if it is personal data under the EU GDPR: Recital 26) for research, archiving or statistical purposes (RAS). Under the Bill, in relation to such secondary uses, transparency towards data subjects and the need for consent are greatly reduced.

In view of the new data transfer rules (below, at 3.6), this is likely to benefit major global UK and US companies including in the pharmaceutical sector, who will be allowed to use personal data, including data transferred from the EU/EEA if the UK's adequacy decision is retained, more easily in the UK, or after further transfer, elsewhere including in the USA, than they would be able to do at home under the EU GDPR in the EU/EEA.

(For details, see again Attachment 2)

3.3 Data subject rights

As Michael Veale's note points out:

> The DPDI Bill introduces new limitations to [data subject rights such the right to object, to have one's data corrected or erased, or to be provided with a copy of one's data]. While in the GDPR, requests can be refused if "manifestly unfounded or excessive", the DPDI Bill changes this to "vexatious or excessive".

The stipulation that rights can be denied if they are too cumbersome for a controller creates a loophole that serious ly undermines those rights and makes them clearly less strong than under the EU GDPR.[2]

(For details, see Michael Veale's note)

3.4 Automated decision-making and profiling

To again defer to Michael Veale:

> [In the DP DI Bill,] the UK Government proposes the significant weakening of the automated decision-making provisions present in the EU GDPR. In short, these prevent a significant, solely automated decision being made about an individual unless there is a legal basis, such as explicit prior consent, necessity to enter into a contract, or a legal obligation to make such a decision. The DPDI Bill removes this protection, limiting it only to decisions based on sensitive data such as ethnicity or religious belief. Decisions not based on such data are subject only to the safeguards that exist after the decision has been made, rather than requiring authorisation to make. As a result, decisions where the impact is immediately felt, such as a decision to block an online worker or content creator in real-time, can be made without human review and impact individuals immediately.

(For details, see again Michael Veale's note)

This too is a very significant departure from the EU GDPR – especially because, after the Court of Justice *PNR* judgment, in the EU, automated decision based on machine-learning artificial intelligence should never be allowed if the self-learning, self-modified algorithms underpinning such a decision cannot be fully or properly understood even by the entity that relies on them, and can therefore also not be meaningfully reviewed or challenged.[3]

It would appear that if the Bill is adopted as proposed, the use of impenetrable and unchallengeable algorithms in the taking of automated decisions will be allowed in the UK whereas they will have to be banned in the EU.

This again could include decisions made by UK private and public entities in relation to EU citizens and residents.

3.5 Data Protection Officers and Data Protection Impact Assessments

To yet again defer to Michael Veale:

> The DPDI Bill proposes the removal of the obligation on some controllers to have a data protection officer, and it removes the obligation to carry out data protection impact assessments (DPIAs) [that, in combination with] the [UK] Freedom of Information Act 2000, … allowed oversight of government data processing operations and revealed poor or incomplete analysis. … Relatedly, the DPDI Bill proposes that law enforcement agencies no longer have to record the "justification for" accessing data in their systems, which may allow them to claim to be relying on a different legal basis after the fact.

(For details, see again Michael Veale's note)

The effect of these changes, too, is to reduce the UK data protection regime to below the EU GDPR standards, here in relation to accountability and internal oversight arrangements that were crucial innovations in the Regulation.

3.6 Extra-territorial application and data transfers: guarantees of serious conflict

Just as the EU GDPR applies not only to controllers and processors in the EU/EEA but also to controllers and processor outside the EU/EEA that "offer goods or services" to individuals in the EU/EEA or that "monitor the behaviour" (including the online behaviour) of such individuals, so the UK GDPR also applies to controllers and processors outside the UK (including controllers and processor in the EU/EEA) that "offer goods or services" to individuals in the UK or that "monitor the behaviour" of individuals in the UK.

If the UK GDPR and the EU GDPR were to be "essentially equivalent" this might not be too problematic. ***However, if the UK regime becomes significantly less strict than the EU regime, as is clearly intended, this will cause serious conflicts***, e.g., if, as noted at 3.2, above, the UK GDPR imposes on EU-based companies disclosure obligations, compliance with which would breach the EU GDPR.

Moreover, the Bill will allow the UK government, *by executive order that is subject to minimal parliamentary scrutiny* (i.e., a statutory instrument that can be adopted in a so-called "negative process" without amendment or debate), to declare any country to provide **"adequate" protection** in terms of the UK GDPR, even if that country has not been held to provide "adequate" (i.e., "essentially equivalent") protection to the EU GDPR – and personal data can then be freely transferred from the UK to the other country *and personal data transferred from the EU/EEA to the UK can then be also freely onwardly transferred to the other (in EU terms: non-adequate) country.*

In other words: ***if the Bill is adopted as proposed, the UK is set to become a "data haven" through which personal data that cannot be directly transferred to an, in the view of the EU, "non-adequate", country, can be thus indirectly transferred.***

In fact, the UK has already held that **Gibraltar** provides "adequate" protection in terms of the UK GDPR, even though there is no comparable ruling on the territory from the EU. There can be little doubt that the UK is keen to declare that the **USA** provides "adequate" protection of personal data in UK GDPR terms, and would certainly offer that as part of its trade negotiations with the USA.

More generally, the UK government wants to see "*greater [global] interoperability of regulatory frameworks on data and more stable principles for trusted government access to data*", to encourage more liberal global free flows of data for business, scientific – and national security – purposes. The relevant minister can simply declare that, e.g., all states that are parties to the Council of Europe Convention (**Convention 108**) (or the "modernised" version of that Convention, **Convention 108+**), or the APEC Cross-Border Privacy Rules (**APEC CBPR**) System, provide "adequate" protection in terms of the UK GDPR – and that all flows of personal data under the Convention or the APEC scheme are therefore allowed without the nees for "appropriate safeguards".

That would seriously undermine the current pre-eminence of the EU GDPR "golden global standard".

3.7 The UK data protection authority

In our November 2020 submissions, Ian Brown and I noted that "*although the UK data protection supervisory authority, the ICO, is one of the largest in Europe, it has been severely criticised for not effectively enforcing the law, both in terms of its minimum application of sanctions and in terms of its lack of real support for data subjects that bring complaints.*" In spite of some headline-grabbing fines, enforcement remains weak. Moreover, the new proposals seek to further undermine, not just the effectiveness but even the independence of the Commissioner. As Chris Pounder already reported in 2021:

> The DCMS [the UK Department for Digital, Culture, Media and Sport – the department responsible for data protection and the DPDI Bill] propose to change the duties of the Information Commissioner (ICO) in such a way that they decrease the prospect of enforcement on data protection grounds; in this way the changes reduce the protection afforded to data subjects.
>
> This prospect arises as the Commissioner will have a duty to consider factors relating to the economy, public safety or the Government's international agenda prior, for example, to exercising the ICO's powers of enforcement against a controller.
>
> The Secretary of State is also seeking powers to determine the Commissioner's priorities. These include vetting the ICO's Guidance to ensure it is appropriate for a business friendly, data protection era in the UK.
>
> ("*Ministers want to pull the strings and rein-in the ICO's independence*", 8 November 2021, at: https://amberhawk.typepad.com/amberhawk/2021/11/ministers-want-to-pull-the-strings-and-rein-in-the-icos-independence.html For details, see the full blog)

This is reflected in the Bill which stipulates that the Commissioner, in ensuring protection of personal data, must also "have regard" to such matters as "*the desirability of promoting innovation [and] competition*", and which allows the Secretary of State to set the "*strategic priorities*" for the activities of the Commissioner. The Secretary of State must also approve codes of conduct prepared by the Commissioner.

In my opinion, the ICO does not provide protection in procedural/enforcement terms that is "essentially equivalent" to what the EU GDPR requires, and the proposed changes seriously affects its independence, also contrary to the EU standards.

4. Continuing bulk surveillance by the UK intelligence agencies

In the second part of our 2020 submissions,[4] Ian Brown and I set out the UK surveillance laws and practices in some detail, and compared to them to the EDPB's "Essential European Guarantees" (EEGs) for surveillance that in turn reflected the case-law of the CJEU. These laws and practices have not materially changed since then. It will therefore suffice to reproduce our summary and conclusions from the executive summary of our submissions:

We reached the following conclusions with regard to the UK surveillance practices and laws:

As to the UK surveillance practices:

- The UK, working jointly with the US National Security Agency (NSA), taps into a large number of selected Internet communications link (especially but not only underseas cables), including cables through which most of the communications of EU individuals, institutions and officials travel (in particular, most EU – UK – USA communications). These communications include not only emails and social media exchanges but also the data flows between EU users of US-based cloud services and the relevant US cloud servers.

- Very large amounts of data – including all communications metadata (including traffic- and location data) are extracted by the UK from all selected bearers indiscriminately, in bulk, and retained for some time.
- The metadata are highly revealing of the lives of potentially hundreds of thousands of individuals to which they may relate, but the vast majority of data subjects to which the metadata relate – which for many selected bearers will include large numbers of EU persons – will have no links with terrorism, threats to national security or serious crime.
- While much of the other data are filtered out fairly quickly through "simple" or "complex" queries, the metadata and the not-filtered-out data are retained for longer, to allow for their use in algorithmic analyses and profiling.
- At least some of those data are retained for purposes that are not aimed at countering serious threats to national security, but rather, to gain some politically or economically advantageous insights into actions of adversaries and allies alike.
- The not-filtered-out data, including all metadata, are subject to automatic analyses by means of self-learning (AI-based) algorithmic datamining, to "identify" (i.e., label) individuals as or linked to "Subjects of Interest" ("SoI") – but this processing suffers from major, unavoidable defects: built-in biases, mathematically unavoidable excessive numbers of "false positives" or "false negatives" (or both), and the fact that because of their complexity they become effectively unchallengeable. It is unavoidable that many individuals who are labelled or linked to "SoI" are innocent and have no links to serious crime or terrorism.

As to the law:

- Under UK data protection law, metadata are not meaningfully protected against undue access and bulk collection by the UK intelligence agencies.
- The UK Investigatory Powers Act clearly does not "itself define" the scope and limitations of the use of the powers it grants the intelligence agencies, in particular in relation to direct access to the systems of communication and Internet service providers, or to direct tapping into underseas cables. The IPA therefore does not meet the requirement set in that regard by the CJEU in *Schrems II*.
- The UK IPA rules that allow for the extraction, in bulk, of at least all the metadata of all communications that flow through a selected bearer, are clearly incompatible with the standards set out in a range of CJEU judgments and arguably (given the now-recognised inherent sensitivity of metadata) compromise the very essence of the rights to privacy, confidentiality of communications and data protection.
- The law allows for broadly phrased bulk interception warrants and for vague search criteria to be applied to stored data; the law itself does little to preclude targeting of improper targets. Rather, almost complete reliance is placed on the institutional oversight of the use of the powers. This too is at odds with the EU requirements.
- Rather than oversight over "the selection of bearers, the application of simple selectors and initial search criteria, and the complex searches which determine which communications are read" being clearly and expressly provided for in the law (i.e., in the IPA), the issue has been left to an "assurance" from the Home Office to the Independent Reviewer of Terrorism Legislation that such oversight is "inherent" in

various clauses in the Act. That is hardly a hard-and-fast legal assurance; the assurance was not even made by a minister in Parliament.

The situation in relation to oversight over complex selectors and search criteria is still unclear, while oversight over the much more sophisticated data mining analyses appears to not have been addressed at all. This means the situation in this regard, too, clearly does not (yet) meet the EU standards as set out, in particular, in the CJEU *LQDN* judgment, referenced in this regard in the EEGs.

- The remedies accorded by the Investigatory Powers Tribunal were essentially held to be effective in terms of the ECHR, partly because the Tribunal was clearly independent and impartial, and issued strong rulings in appropriate cases – but also because in its rulings it had the power and the duty to ensure that both practice and the law were compliant with EU law including the Charter of Fundamental Rights.

  But of course, this will fundamentally change from 1 January 2021 [has now fundamentally changed – DK], when the IPT will no longer be able to rely on EU law (including the Charter) in assessing the validity of various elements of the UK surveillance regime – which is deficient in several respects as shown above.

  This raises serious doubts as to whether, at least in relation to the compatibility of the legal regime as such with European fundamental rights standards, the IPT will still be able to provide a judicial remedy in terms of Article 6 ECHR, or even an "effective remedy" in terms of Article 13 ECHR, or an "effective remedy before a tribunal" in terms of Article 47 of the Charter (to which much attention was given by the CJEU in its *Schrems II* judgment).
- Data on individuals in the EU, extracted in bulk from the underseas cables by GCHQ, and the results of the analyses of those data, are shared with the USA – which has been specifically held to not provide "adequate"/"essentially equivalent" protection to personal data in *Schrems II*.
- The carrying out of automated profiling by GCHQ (in cooperation with the US NSA), and the taking of decisions about individuals – including EU individuals – on the basis of the (secret) results of that profiling, does not meet the requirements of Article 22 GDPR – and this deficiency in UK law and practice, too, stands in the way of a positive adequacy decision on the UK.

Overall conclusion reached in relation to surveillance:

- In our opinion, it is highly doubtful whether the processing of personal data by UK intelligence agencies, especially its bulk collection of communication data, is in line with the EU Charter of Fundamental Rights. In particular, the UK's indiscriminate bulk collection of communications metadata ("related communications data") from selected "bearers" in the underseas communication cables would appear to be contrary to principles established by the European Court of Human Rights (*Big Brother Watch v. the UK*) and the CJEU (*Tele2/Watson*, *Digital Rights*, *Schrems II*, *Privacy International* and *La Quadrature du Net*), as reflected in the recent EDPB's "European Essential Guarantees for Surveillance Measures".

This remains my opinion.

Overall conclusions:

The UK should not have been granted a positive adequacy decision under the EU GDPR in June 2021. But that aside, the proposed changes would move the UK data protection regime considerably further apart from the EU regime: it would move even further from "essential equivalence" with the EU GDPR.

Moreover, the UK surveillance laws and practices, which did not meet the standards of the EDPB's European Essential Guarantees at the time the positive adequacy decision was issued (which should in itself have stopped the Commission from issuing the decision) continue to fall foul of those standards.

On both these grounds, the EU Commission's adequacy decision on the UK should be rescinded, if not rightaway then certainly if the UK government proceeds to adopt the DPDI Bill in its present form.

In the light of my earlier conclusions, I conclude in particular that if the EU adequacy decision on the UK is not rescinded when the Bill becomes law:

- EU companies will be able to "launder" personal data through the UK in lightly pseudonymised form; and
- the UK would become an offshore "data haven" through which data that cannot be sent from the EU/EEA to "inadequate" third countries such as the USA can be routed.

- o – O – o -

Prof. Douwe Korff
Cambridge (UK), 27 October 2022

NOTES:

[1] See:
Douwe Korff and Ian Brown, The inadequacy of UK data protection law in general and in view of UK surveillance laws (with some comments on the adequacy decisions on Guernsey, Jersey and the Isle of Man & on the implications for other countries and territories including Gibraltar & EU Member States), submission to the European Union bodies involved in assessing whether under the EU General Data Protection Regulation (GDPR) the United Kingdom should be held to provide "adequate" protection to personal data:

- Part One on general inadequacy of UK data protection law, submitted on 9 October 2020, available at: https://www.ianbrown.tech/2020/10/09/the-uks-inadequate-data-protection-framework/
- Part Two on UK surveillance law, submitted on 30 November 2020, available at: https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-Part-Two-DK-IB201130.pdf
- Executive Summary and discussion of the implications, also submitted on 30 November 2020: https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-ExecSumm-DK-IB201130.pdf

Also: Douwe Korff, The inadequacy of the EU Commission's Draft GDPR Adequacy Decision on the UK, 3 March 2021, available at:
https://www.ianbrown.tech/2021/03/03/the-inadequacy-of-the-eu-commissions-draft-gdpr-adequacy-decision-on-the-uk/

[2] How this will work out is already becoming clear in practice, as evidenced by the response by the Cabinet Office to a journalist's subject access request. It was denied because the Office said that, while "*[t]he initial search … returned more than 1900 results*" (i.e., pieces of information relating to the data subject), the Office "*would have to go through all of these results, to extract [the data subject's] personal data*" and they "*would consider this to be excessive*" and therefore refused the request. See:
https://twitter.com/kennardmatt/status/1584942706765492224
As I noted in a comment:

"*It is absurd to argue that because some state (!) entity has a *lot* of data on a data subject, that is a reason to deny access! So the more they hold, the less accountable they are? That cannot be the law!*"
https://twitter.com/DouweKorff/status/1585364195071373312

[3] Douwe Korff, Opinion on the implications of the exclusion from new binding European instruments on the use of AI in military, national security and transnational law enforcement contexts, written at the request of the e European Center for Not-for-Profit Law (ECNL), October 2022, available at:
https://ecnl.org/sites/default/files/2022-10/ECNL%20Opinion%20AI%20national%20security.pdf (full opinion)
https://ecnl.org/sites/default/files/2022-10/ECNL%20Opinion%20AI%20national%20security_exec%20summary_0.pdf (executive summary)

[4] See note 1, above, second indent.

- o -0 – o -