Amid the spying by EU Member States' intelligence agencies, is EU law silent?

Some thoughts on how the hole in EU law can be further limited and patched

by

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Visiting Fellow, Yale University (Information Society Project)
Associate, Oxford Martin School, University of Oxford

August 2021

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Visiting Fellow, Yale University (Information Society Project)
Associate, Oxford Martin School, University of Oxford

References:

Judgments of the Court of Justice of the European Union (CJEU) and of the European Court of Human Rights (ECtHR) mentioned in this paper, with abbreviated references in brackets:

Court of Justice of the European Union judgments and opinion:[1]

- CJEU judgment of 8 April 2014 in joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* (***DRI***);
- CJEU judgment of 6 October 2015 in case C-362/14, *Maximillian Schrems v Data Protection Commissioner* (***Schrems I***);
- CJEU judgment of 21 December 2016 in joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* (***Tele2/Watson***);
- CJEU Opinion 1/15 of 26 July 2017 on the EU – Canada Draft PNR Agreement (***EU-CAN PNR Opinion***);
- CJEU Grand Chamber judgment of 16 July 2020 in case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (***Schrems II***);
- CJEU judgment of 6 October 2020 in joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others* (***LQDN***);
- CJEU judgment of 6 October 2020 in case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (***PI***).

European Court of Human Rights judgments:[2]

- ECtHR judgment of 6 September 1978 in *Klass and others v Germany* (***Klass***);
- ECtHR, plenary judgment in the case of *The Sunday Times v. the United Kingdom*, 26 April 1979 (***Sunday Times I***);
- ECtHR judgment of 26 April 1985 in *Malone v the United Kingdom* (***Malone***);
- ECtHR admissibility decision of 29 June 2006 on the application of *Gabriele Weber and Cesar Richard Saravia v Germany* (***Weber and Saravia***);
- ECtHR judgment of 1 July 2008 in *Liberty and others v the United Kingdom* (***Liberty***);
- ECtHR judgment of 18 May 2010 in *Kennedy v the United Kingdom* (***Kennedy***);
- ECtHR judgment of 4 December 2015 in *Roman Zakharov v Russia* (***Zakharov***);
- ECtHR Grand Chamber judgment of 25 May 2021 in *Big Brother Watch v the United Kingdom* (***BBW***).

- o – O – o -

[1] All CJEU judgments and opinions are available from the EU's *Curia* website at: https://curia.europa.eu/juris/recherche.jsf

[2] All ECtHR judgments and admissibility decisions are available from the Council of Europe's HUDOC website at: http://hudoc.echr.coe.int/sites/eng/Pages/search.aspx

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Visiting Fellow, Yale University (Information Society Project)
Associate, Oxford Martin School, University of Oxford

Amid the spying by EU Member States' intelligence agencies, is EU law silent?[3]

Some thoughts on how the hole in EU law can be further limited and patched

1. Introduction

In our recent report for the European Parliament's Civil Liberties Committee (LIBE),[4] Ian Brown and I described how the Court of Justice of the European Union (CJEU or "the Court") addressed in its important *Schrems II* judgment[5] the implications of there being, in a non-EU country (a so-called "third country" in EU legal parlance), laws that give powers to the authorities of that third country to demand or gain access to personal data on EU persons that may be transferred to that country (or that can be directly accessed by those authorities, even if the data are not physically transferred to the third country by the relevant EU controller or processor), when those laws do not meet basic European rule of law requirements of legal clarity and foreseeability, necessity and proportionality, protection against arbitrariness and discrimination, and of appropriate (in principle judicial) remedies for affected (EU) individuals.[6]

In that case, the Court held that US laws, in particular the US Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 (E.O. 12333) and Presidential Policy Directive 28 (PPD-28), did not meet those requirements and that the European Commission decision of 12 July 2016 on the adequacy of the EU-US "Privacy Shield" framework[7] was therefore invalid (just as it had earlier held, in its *Schrems I* judgment, that the European Commission's July 2000 decision on the adequacy of the EU-US "Safe Harbour" Framework was invalid); that personal data could therefore not be freely transferred from the EU to the USA, but rather, that "appropriate safeguards" should be adopted to ensure that the protection accorded to those data by EU law (*in casu*, the EU General Data Protection Regulation, GDPR) would not be undermined. The Court also held that the use of Standard Contractual Clauses for data transfers (SCCs) might not be sufficient in that regard because they could not override the laws of the third country, and that therefore further, unspecified "supplementary measures" might have to be put in place.[8]

---

[3] Cf. Lord Atkins (dissenting) in *Liversidge v. Anderson*: "*[A]mid the clash of arms, the laws are not silent*", House of Lords, [1942] AC 206, available at: https://www.bailii.org/uk/cases/UKHL/1941/1.html

[4] Ian Brown & Douwe Korff, Exchanges of personal data after the Schrems II judgment, study carried out with Ian Brown at the request of the LIBE Committee into the future of EU – US flows of personal data, July 2021 (**hereafter, "the Brown-Korff Study", "the study" or "our study"**), available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf

[5] For all references to European cases mentioned in this paper, see page 1, above.

[6] See the Brown-Korff Study, section 2.3.1.3, *Requirements relating to access to personal data by state authorities*, under the sub-heading "*CJEU requirements relating to indirect or direct access to personal data by third country intelligence agencies*", pp. 41 – 45. The clarification that direct access by third country authorities to personal data on EU persons also constitutes a transfer of those data to the third country, even if the data were accessed by those authorities of the third country from that third country, is contained expressly in footnote 23 in EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on 18 June 2021, and reflected in subsequent guidance.

[7] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p. 1–112.

[8] *Schrems II* judgment, paras. 132 – 133.

The European Data Protection Board elaborated on both matters. In its November 2020 Recommendations on European Essential Guarantees for surveillance measures (EEGs),[9] it clarified the kinds of limitations and guarantees that should be in place in order to ensure that access to personal data by intelligence agencies meets the European – and in particular the EU Treaties and Charter – requirements. And in June 2021, it updated its Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.[10]

As we concluded in our study:[11]

> Laws in third countries that do not meet the … CJEU standards as reflected in the European Essential Guarantees for surveillance measures (EEGs) tests cannot be said to provide "essentially equivalent" protection to the GDPR.

And:

> [T]hird countries that do not provide effective judicial remedies to EU persons in relation to the processing of those persons' personal data in those countries, including in respect of access to those data by the third country's intelligence agencies, cannot be held to provide "essentially equivalent" protection to the GDPR.

Those conclusions apply to all third countries: personal data cannot be freely transferred to any third country that does not meet these tests; rather, "appropriate safeguards" such as SCCS must be adopted, and "supplementary measures" are also likely to have to be adopted, in relation to transfers of personal data to any third country that does not meet these strict tests.

In reality, there are few non-EU countries in the world that have laws that meet those standards (I will come to the EU countries below).[12]

The USA criticised the application of the EEGs to third countries, given that the Court of Justice of the EU cannot apply those guarantees to surveillance activities by EU Member States in relation to their national security because actions by EU Member States in that area are completely outside the scope of EU law including the Charter and the GDPR. In our study, we call this "**the 'hole' in the EU Treaties**".

In our study, we described how the CJEU limited the size of the "hole" (in particular, by ruling that the national security exemption in the Treaties does not apply to mandatory retaining and disclosing of personal data to EU Member States' intelligence agencies, required of entities that are, in this processing, subject to EU data protection law, specifically the GDPR – so-called "indirect access"); how the remainder of the "hole" – the applicability of the

---

9 EDPB, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, adopted on 10 November 2020, at:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

10 See footnote 6, above.

11 Brown-Korff Study, pp. 46 and 47.

12 See Douwe Korff, Ben Wagner, Julia Powles, Renata Avila and Ulf Buermeyer, Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, comparative report covering Colombia, DR Congo, Egypt, France, Germany, India, Kenya, Myanmar, Pakistan, Russia, South Africa, Turkey, UK, USA, prepared for the World Wide Web Foundation, global report, January 2017, available at: https://ssrn.com/abstract=2894490

exemption to "direct access" to data by intelligence agencies, typically through "hacking" into providers' systems – was (partially) "patched" by the Court (by reference to the standards set by the European Convention on Human Rights [ECHR] and national constitutional law, that do apply to the national security activities of EU member States including such direct access); and how that "patch" could perhaps, to some extent, be made to stick through EU law (through the Copenhagen criteria).[13] But we also concluded that:[14]

> It nevertheless remains true that in the EU different standards apply to surveillance carried out by Member States under orders issued to providers of e-communication services (the standards set by the CJEU in *Schrems II* and *LQDN*, discussed [in the study]), and to surveillance carried out by their national security agencies through direct, surreptitious "hacking" into the providers' systems (the ECHR standards [also discussed in the study]) – while surveillance laws and practices of third countries have to "essentially" meet the CJEU standards in relation to both kinds of surveillance if a third country is to be held to provide "essentially equivalent/adequate" protection in relation to data transfers. In chart form:

	EU Member States must meet:	**Third countries must meet:**
Indirect access (access under orders issued to providers.)	EU CJEU *Schrems II* & *LQDN* standards	"Essentially equivalent" standards to the EU CJEU *Schrems II* & *LQDN* standards
Direct access (access through surreptitious "hacking" into providers' systems.)	ECHR and national constitutional standards	

However, we also found that:[15]

> A more pertinent claim of hypocrisy can be laid against the EU and the EU Member States in relation to actual compliance with either the ECtHR or the CJEU standards. [T]here have been serious questions about the general effectiveness of enforcement by the supervisory authorities in the EU Member States. More specifically, …, the EU and the Member States have been reluctant to come up with laws that actually meet the CJEU standards laid down in its *DRI* and *Tele-2/Watson* judgments, in spite of strong criticism by the European Parliament and civil society. The current laws in the EU Member States have also not yet been brought into line with CJEU judgments in *PI* and *LQDN*. And the surveillance laws and practices in many EU Member States would clearly fail the tests applied to the laws and practices of the USA in *Schrems II*.

---

[13] See the Brown-Korf Study, section 2.2.2, *The national security exemption in the EU Treaties*, sub-sections 2.2.2.1, 2.2.2.2 and 2.2.2.3, respectively.

[14] Brown-Korff Study, section 2.3.1.3, *Requirements relating to access to personal data by state authorities*, under the sub-heading "*Hypocrisy and 'Double standards'? US criticism of the EU and the EU Member States*", p. 58.

[15] *Idem*, pp. 59 – 60, footnote and cross-references to earlier sections in the study omitted.

We therefore suggested in our report that not only should the USA bring its surveillance laws into line with international human rights standards, but the EU and the EU Member States should ensure this in the EU and Member States' legal orders as well.[16] We felt – and still feel – that this would best be done within a broad international framework, beginning with:[17]

> a "minilateral" framework for the main advanced economy democracies (which have the financial resources to undertake the large-scale technical surveillance at issue) – in particular, the 30 EU and EEA states and the "Five Eyes" countries (USA, UK, Australia, Canada and New Zealand – which are now all "third countries" in terms of EU law). Because of the (regrettable) national security exemption in the EU treaties, the EU cannot be a party to such an agreement, but there is no reason why it cannot be a midwife (or part of a midwifery team).

This however may still be some time off. In the meantime, I have been thinking further about the implications in terms of the GDPR of undue access* to personal data on EU persons (and others) by EU Member States' intelligence agencies. I believe that the Court's recognition of the regrettable "hole" in the Treaties need not be the end in this regard. In the next section, I discuss my line of reasoning. In section 3, I discuss the implications (also in relation to "indirect access"); in section 4, the resulting dilemmas; and in section 5 I will note that the only way to address those dilemmas remains the above-mentioned international framework.

*NB: In this paper, I will from now on use the words "**undue access**" to personal data by state agencies as shorthand for access to such data under laws and procedures that do not meet the CJEU requirements set out in its *Schrems II* judgment, as further elaborated in the EDPB's EEGs.

2. Line of reasoning

In another important judgment, *La Quadrature du Net* (*LQDN*), the CJEU held that the rules on personal data processing operations by entities that are, in that processing, subject to EU data protection law (in that case, providers of electronic communication services, who are subject to the e-Privacy Directive), *including processing operations by such entities resulting from obligations imposed on them under the law by Member States' public authorities for national security purposes* – i.e., the rules on **indirect access** – can be assessed for their compatibility with the relevant EU data protection instrument and the Charter of Fundamental Rights.[18] If they do not meet the EEGs tests, those rules will be declared invalid.

However:[19]

> By contrast, **where the Member States directly implement measures** that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by [the e-Privacy Directive], but by national law only, subject to the application of [the Law Enforcement Directive], with the result that the measures in question must comply with, *inter alia*, national constitutional law and the requirements of the ECHR.

As already mentioned, we refer to such access by means of "directly implemented measures" as "**direct access**".

---

16 See the Brown-Korff Study, Chapter 4 and the Executive Summary.

17 *Idem*, section 4.3.3, *Long-term intelligence reform by international agreement*, at p. 122.

18 Para. 101 (see also para. 102).

19 Para. 103, emphases added.

It would appear from this that while the CJEU can judge whether any **direct or indirect access** to personal data on EU persons by *third country intelligence agencies*, and the *third country laws* authorising such access, meet the Court's tests (as reflected in the EEGs), and the CJEU can also judge whether any **indirect access** to personal data on EU persons by *EU Member States' intelligence agencies*, and the *Member States' laws* authorising such access, meet the Court's tests (as reflected in the EEGs), the EU Court has no jurisdiction to judge whether any **direct access** (in the form of "directly implemented measures" such as "hacking") taken by *EU Member States' intelligence agencies* meet those tests. The latter is why the USA is understandably talking about "double standards". But perhaps the issues are not quite as clear-cut as they seem. In particular, while the Court, in the above paragraph, refers to the direct measures, it says nothing about the laws authorising those measures.

(NB: The reference in the *LQDN* judgment to the measures having to comply with "*inter alia*, national constitutional law and the requirements of the ECHR" is, in that regard, somewhat disingenuous: yes, those measures must meet the ECHR tests in particular, because all EU Member States are party to the Convention. But whether they actually comply with the ECHR is not something the Luxembourg Court can determine: in spite of this reference to the ECHR "applying", the CJEU still has no jurisdiction to assess this, because of the broad national security exemption in the EU Treaties. The issue can only be judicially assessed by the European Court of Human Rights – which applies less strict tests than the CJEU, in more cumbersome proceedings – or by national constitutional courts – which may differ in many respects from either the EU or the ECHR tests – or raised in the EU under the Copenhagen criteria, but the latter's implementation is essentially political rather than legal, and tenuous.)

However, in my opinion, the fact that the EU Court has no jurisdiction to judge whether any "directly implemented measures" (such as "hacking") taken by EU Member States' intelligence agencies meet the Court's tests, does not mean that the quality of any laws authorising those measures has no implications under the GDPR at all. This is because any movement of personal data from any entity subject to the GDPR[20] to any other entity is subject to the regulation – even if the other entity is not subject to the GDPR, or to EU law of any kind.

In that regard, it is important to realise that any movement of personal data between two entities has two distinct aspects: the disclosure of the data by the entity that is subject to the GDPR is subject to the GDPR (even if that is passive, as when data are "hacked" or "pulled") because that disclosure is a form of processing.[21] The other aspect of the movement of the data – the other side of the same coin if you like – constitutes "obtaining" or "collecting" of the data by the recipient, *in casu*, by a Member State intelligence agency. Even if the latter (the collecting by an EU member States intelligence agency) is outside of EU law, the (passive or active) movement of the data to the agency is not. See the illustration, overleaf.

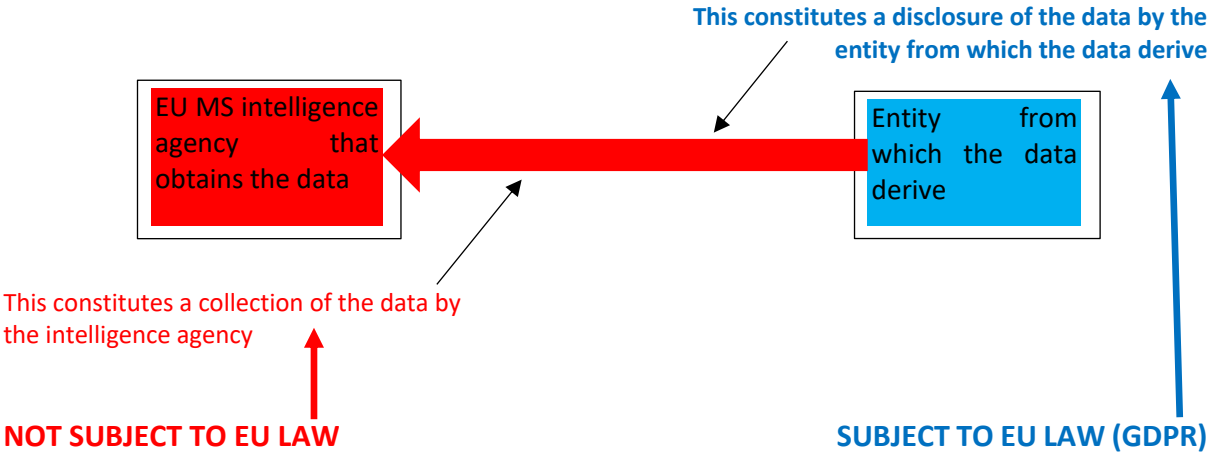
---

20 Or to the Law Enforcement Directive, but I will limit myself here to the GDPR.

21 Cf. the all-encompassing definition in Article 4(2): "***'processing'*** *means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*"

The question then becomes: are there any rules in the GDPR that apply to the movement of personal data from an entity that is subject to the GDPR to any EU Member State's intelligence agency, even if the entity from which the data derive is passive in this respect, i.e., when the data are taken "directly" from that entity by the intelligence agency? I believe there are such rules.

The two aspects of any movement of data between entities that are subject to EU data protection law and EU Member States' intelligence agencies:



Specifically, the GDPR requires controllers and processors to "implement appropriate technical and organisational measures to ensure a level of security appropriate to [the risk[s] of varying likelihood and severity for the rights and freedoms of natural persons]." (Article 32(1) GDPR). More specifically, such technical and organisational measures (TOMs) must protect the data from **personal data breaches**, defined as:

> a breach of security leading to the accidental or **unlawful** destruction, loss, alteration, **unauthorised disclosure** of, or **access** to, personal data transmitted, stored or otherwise processed. (Article 4(12), emphases added).

The core terms here are "**unlawful access**" and "**unauthorised disclosure**". In particular, the term "law", and thus also the term "unlawful", is an autonomous concept under EU and ECHR law. As explained in our study (with reference to the ECHR but that also applies in EU law):[22]

> In European law, in particular the ECHR, ["law"] is an "autonomous concept", meaning that a state cannot fulfil the condition that a rule (more specifically, a limitation of a right) is "law" or "based on law" by pointing to some existing legal rule in its domestic order, even if the rule in question is valid in domestic terms. Rather, under the Convention, the concept is linked to the "rule of law" and its opposite: arbitrariness. In order to qualify as "law" in the Convention sense, the legal rule in question must have certain qualities; it must have "the quality of law" in a state under the rule of law, and must not be capable of being arbitrarily applied. To this end:[23]
>
> Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to

22 Brown-Korff Study, p. 30.

23 ECtHR, *The Sunday Times v. the United Kingdom*, 26 April 1979, para. 49, emphasis added.

> enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. And thirdly, domestic rules that are relied on to limit fundamental rights – e.g., rules that allow for access to personal data by state authorities – should not grant excessive discretion to those exercising power on the basis of those rules.

As Ian Brown and I explained more specifically (and with detailed references) in relation to intelligence agencies' access to data in our 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 (slightly edited, with emphases added):[24]

> **1. The rules under which the interference [i.e., here: direct access] is authorised – i.e., the relevant national law of the country in question – must be accessible (i.e., published), legally binding, clear and precise (i.e., "foreseeable" in its application in the sense that "[t]he domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures").**
>
> References: All of these requirements are standard requirements under the ECHR and the CFR, reiterated in the EEGs paras. 27 – 31, with reference to CJEU cases *Schrems II*, paras. 175, 180 and 181, *EU-CAN PNR*, para. 139 (and further case-law cited there) and *PI*, paras. 65 and 68; and ECtHR cases *Liberty*, para. 63, *Weber and Saravia*, para. 95 and *Malone*, paras 65 – 66. The quote is from ECtHR judgment in *Zakharov*, para. 229.
>
> **2. The law "must itself define" the scope and application of the measure in question.**
>
> References: EEGs, para. 29, with reference to the CJEU *Schrems II* judgment, para. 175, repeated verbatim with a cross-reference in its *PI* judgment, para. 65, and in its *LQDN* judgment, para. 175. Cf. also its *DRI* judgment, para. 68 (re EU law). Repeated in EEGs, para. 36.
>
> Note: In its *BBW* judgment, the ECtHR has outlined "**six minimum requirements**" that surveillance laws must meet in order to ensure that they are "sufficiently foreseeable to minimise the risk of abuses of power" and which can be said to also indicate the "defining" that the CJEU says should be enshrined in the law itself. These are (in summary):
>
> - [the need for a specification of] the nature of offences which may give rise to an interception order;
> - [the need for] a definition of the categories of people liable to have their communications intercepted;
> - [the need for] a [stipulated] limit on the duration of interception;
> - [the need for an appropriate] procedure to be followed for examining, using and storing the data obtained;

[24] Douwe Korff & Ian Brown, The inadequacy of UK data protection law in general and in view of UK surveillance laws, Part Two, *UK Surveillance law*, 30 November 2020, p. 31, available at: https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-Part-Two-DK-IB201130.pdf
For the full references to the cases mentioned in the quote, see again p. 1, above.

- [the need for appropriate] precautions to be taken when communicating the data to other parties; and
- [the need for limitations on] the circumstances in which intercepted data may or must be erased or destroyed

(*BBW* judgment, para. 423, summarising the more detailed overview of the six requirements in para. 307, with indents and words in square brackets added. See also the EEGs, para. 30).

The first two of the above requirements correspond to the CJEU requirement that there must be some reasonable link between the individuals whose data are collected and the offences or threats to national security in relation to which their data are collected. In other words: the law itself should expressly preclude the collection of personal data (including metadata) on individuals who have no personal link, or some link in time or place, to the offences or threats in question. **General, indiscriminate, "dragnet", bulk collection of personal data (including metadata) – collecting of the "hay" from a "haystack" in order to find a "needle" buried in it – is fundamentally incompatible with EU fundamental rights law; and the laws covering surveillance should themselves, explicitly make clear that such bulk collection is not permitted.** This cannot be left to vague language such as instructing a government minister authorising surveillance to do so only in a "proportionate" manner.

The above "rule of law"/"quality of law" tests are clearly demanding, and directly relevant to EU Member States national security laws. Those still often fail to meet those test.[25]

<u>Conclusion</u>:

It follows from the broad general, autonomous application of the above tests that any law of any EU Member State that authorises its intelligence agencies to "directly access" (i.e., "hack" into) the servers of private entities and to extract from those any personal data that does not meet these tests cannot be regarded as "law" in any EU legal context. <u>Such access is not lawful access – in EU law, it constitutes *un*lawful access. And under the GDPR, any controller or processor must protect any personal data they process from such unlawful access.</u>

Similarly, "authorised access" can only mean access authorised either by the entities processing the data (the controller or processor) or access authorised by "law". And if the national law in question does not constitute "law" in the ECHR/EU sense (and the access is also not authorised by the controller or processor), then the access based on such an inadequate legal instrument can also not be regarded as "authorised". <u>Consequently, any direct access of ("hacking" into) the data by the intelligence agencies on the basis of such a "non-law" also constitutes "*un*authorised access". And under the GDPR, any controller or processor must protect any personal data they process from such unauthorised access.</u>

[25] See Douwe Korff, Ben Wagner, Julia Powles, Renata Avila and Ulf Buermeyer, <u>Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes</u> (footnote 12, above), sections and *passim* information on France and Germany (and the UK that was at the time also still an EU Member State).

3. Implications of undue direct (and indirect) access to personal data by EU Member States' intelligence agencies

As noted above, if an EU Member State's intelligence agency directly accesses ("hacks" into) personal data on the basis of a national law that does not meet the above-mentioned "rule of law"/"quality of law" requirements (or more broadly, the EEGs tests), then that constitutes a personal data breach in terms of the GDPR on the part of the controller or processor concerned. This has significant implications, not only for when such undue access (such a data breach) can be shown to have happened – which will often not be possible given the secrecy surrounding the activities of the intelligence services (although I will still make some comments on that below) – but also if there is a real risk that in a particular case, i.e., in relation to a specific personal data set or a specific personal data processing operation, such undue access by an EU Member State intelligence agency may occur.

In that regard, the GDPR stipulates the following in Article 35(1):

> Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, **prior to the processing**, carry out **an assessment of the impact** of the envisaged processing operations on the protection of personal data. (emphases added)

It follows that if, in the light of the "nature, scope, context and purposes of the processing", a personal data processing operation or set of personal data is likely to attract the attention of an EU Member State's intelligence agency/ies, the controller of the processing should carry out a data protection impact assessment (DPIA) before the processing is undertaken.[26] If the assessment indicates that there is indeed a significant risk of undue access, "**measures**" must be taken to address the risk of undue access –

> including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned. (Art. 35(7)(d))

(NB: Although Article 35(1) suggests that a DPIA must only be carried out if a processing operation "*is* likely to result in a high risk", in fact the assessment should seek to determine *whether* there is such a high risk, and how that risk can be mitigated. This follows from Article 36(1) which, as noted below, requires a controller to consult the relevant supervisory authority "where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk".)

The assessment should include the question of whether the law under which direct access may be happening meets the EU rule of law/EEGs standards. If it is concluded that the law does not meet those standards, technical and organisational measures (TOMs) must be adopted to counter the undue access.

---

[26] Article 35 GDPR places the onus for the carrying out of a DPIA on controllers. However, in practice, processors are increasingly deeply involved in the processing, e.g., by providing the relevant infrastructure or software. It will often make sense for processors – especially processors who provide Software as a Service (SaaS) or Infrastructure as a Service (IaaS) services to a range of controllers – to undertake (much of) this task, as they will be often be best able to assess the technical feasibility of the intelligence agencies seeking direct access to the data they process.

In effect, this means that controllers (and processors)[27] who are subject to the GDPR should treat the risk of undue access to the data they process by the EU Member States' intelligence agencies in essentially the same way as the risk of undue access to those data by third countries' intelligence agencies in cases in which a transfer to a third country is considered: the risk assessment (including the assessment of whether the relevant national law meets the EU rule of law/EEGs standards) is essentially the same, and the TOMs that may have to be adopted to counter undue access by EU Member States' intelligence agencies are essentially the same as the "supplementary measures" that may have to be adopted to counter undue access by third countries' intelligence agencies.

If the controller (or processor) concludes that the data are at "high risk" of being "directly accessed" by an EU Member State's intelligence agencies, and that there are no TOMs that can effectively protect the data against this, then the controller (and the processor, possibly through the controller) must "consult the supervisory authority prior to processing" (Art. 36(1)) and:

> Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. (Art. 36(2))

Those powers include the power to order the controller (and/or the processor) to not go ahead with the processing operation, or to adopt further specific measures to counter the possibility of "unlawful" or "unauthorised" access to the data by the relevant intelligence agency (see Article 58(2)(f) and (d), respectively).

In other words, in my opinion, the EU data protection supervisory authorities have the power to order controllers and processors who are subject to the GDPR to not carry out processing operations if the data involved are at "high risk" of being directly accessed by any EU Member State intelligence agency acting under a law that does not meet the EU rule of law/EEGs standards, or to adopt special measures to protect the data against such undue ("unlawful" and "unauthorised") access – i.e., to adopt essentially the same measures as the "supplementary measures" that may be require in relation to any transfer of personal data to a third country where the data may be exposed to undue access by the third country's intelligence agencies.

A further implication is that if a controller (or processor) fails to carry out a DPIA, or fails to adopt effective measures to prevent a data breach in the form of undue access to the data by an EU Member State's intelligence agency, or fails to consult the supervisory authority, or fails to abide by an order of the authority, a significant administrative fine can be imposed on them (Art. 83(4)(a) and (6)); and the controller and processor may also be liable for compensation if any data subjects suffer (material or immaterial) harm as a result (Art. 82).

[27] See previous footnote.

In fact, **the above reasoning can also be extended to issues of indirect access**. This is because such indirect access – access to personal data by means of measures that are imposed on the relevant controllers and/or processors – must also have a basis in "law". Specifically, private entities that are ordered to pass on personal data to intelligence agencies (e.g., by "pushing" specified or broadly-defined classes of data to the agencies) or to build "back doors" into their systems through which the agencies can directly "pull" such data – will be acting on the basis of Article 6(1)(c) GDPR which stipulates that "[p]rocessing [of personal data] shall be lawful" if:

> [the] processing is necessary for compliance with a legal obligation to which the controller is subject.

Both the reference to "lawful" and the use of the words "legal obligation"[28] again link back to the concept of "law" as discussed above.

In my opinion, a law of an EU Member State that imposes on controllers and processors who are subject to the GDPR duties to (retain and) provide access to any personal data they process to the intelligence agencies of that Member State, but that does not meet the CJEU/EEGs tests, is not a "law" in the EU legal sense – and any such obligations are therefore not "legal obligations" in the EU legal sense.

The implication is that controller and processors faced with such demands of access under such "unlawful laws" should refuse to comply: the access demanded is not made in relation to a "legal obligation" but to an "illegal" one in EU terms, and the access would not be lawful but "unlawful" in the EU terms. The disclosure (which is a form of processing)[29] is therefore not justified under Article 6(1)(c).

There is one further intriguing implication. According to Article 36(4):

> Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

Although this stipulation is set out in the context of DPIAs, it is clear from Recital (96) that it applies to any "legislative measure" that "relates to" processing of personal data – for which one can read in particular: any law that regulates specific kinds of processing. In my opinion, this clearly covers any law that grants the relevant Member State's intelligence agencies powers of direct access to ("hacking" into) any personal data, including in particular any personal data processed by private entities (domestic or foreign).

It should be clear from my analysis at 2, above, that in my opinion the question of whether such laws meet the CJEU/EEGs standards is <u>not</u> a matter outside the scope of the GDPR, because they have a bearing on the issue of personal data breaches (i.e., on whether such access is "lawful" and "authorised" in the EU legal sense).

---

[28] The French version of the GDPR has, respectively, "*licite*" and "*une obligation légale*"; the German version, "*rechtmäßig*" and "*eine rechtlichen Verpflichtung*". If anything, these terms are more demanding than just "lawful" and "legal obligation". In particular, the tests of *licite* and *rechtmäßigkeit* go beyond mere formal legality to include elements of fairness and legitimacy.

[29] See footnote 21, above.

In my opinion, it follows that under the GDPR the data protection supervisory authorities of the EU Member States must be consulted on any draft law regulating direct access by the EU Member States' intelligence agencies to personal data held by other entities (including in particular private entities (domestic or foreign). If those authorities advise their legislator that in their view the draft law does not meet the CJEU/EEGs standards, the Member States in question would adopt the law unamended at their peril: it would raise doubts about the commitment of the relevant Member State to the rule of law and would create unpalatable dilemmas for the controllers and processors processing the personal data that could as a result be unduly accessed by the intelligence agencies.

I will turn to those dilemmas now.

4. Resulting dilemmas

One clear advantage of accepting my line of argument is that the intelligence agencies of EU Member States – who are not subject to EU law, the Charter or the GDPR – are effectively, and rightly, treated on a par with the intelligence agencies of third countries (which are treated with caution by the CJEU and the EDPB because they are not subject to EU law, the Charter or the GDPR):

Gelijke monninken, gelijke kappen

(as they say in Holland)

What is good for the goose is good for the gander

(as they say in England)

However, as is becoming very clear in relation to data transfers from the EU to the USA, requiring entities that engage in such transfers to adopt measures that effectively prevent the US intelligence agencies from gaining access to the data if they need to be accessed "in the clear" in the USA is (a) technically well-nigh (in practice, actually completely) impossible, especially for SMEs but also for large firms and (b) exposes the data exporter to serious legal dilemmas. And those same issues arise in relation to the EU Member States' agencies.

On the technical side, Ian Brown tells me that it is barely feasible to adopt technical safeguards that can resist concerted interest from the US National Security Agency (NSA) in such "in the clear" data (and even in pseudonymised or lightly encrypted data), and I guess the same is largely true in relation to the intelligence agencies of the UK and the other "Five Eyes" countries, Australia, Canada and New Zealand – and probably those of the major EU Member States (and Russia and China). It is possible to make access by well-equipped, technically advanced agencies more difficult – and that has the positive effect of at least forcing them to focus their efforts on data that may actually be really relevant to their operational purposes (rather than engage in fishing expeditions and in "adding hay to the haystack" in the mistaken belief that increasing data in a data mining operation can defeat the "base rate fallacy").[30]

But that is probably the most that can be achieved: **it is unlikely that the EDPB will be able to come up with "supplementary measures" that can realistically be adopted by EU data**

[30] For a discussion, see Douwe Korff and Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, Council of Europe, June 2015, section I.iii, under the heading, "*The baserate fallacy*", available at: https://rm.coe.int/16806a601b

exporters (or firms that may be exposed to undue access by EU Member States' intelligence agencies) that can achieve more than just making access to the data more difficult.

There are also significant legal dilemmas for controllers and processors who are subject to the GDPR – both in relation to exports of data to the USA (and other third countries with serious intelligence capabilities) and in relation to the possibility of undue access by EU Member States' intelligence agencies.

Companies in the EU that are subject to the US CLOUD Act – such as European subsidiaries of US parent companies – face the dilemma that they may, under that Act, be ordered to transfer personal data (or provide direct access to the personal data they hold, e.g., by allowing the building of "back doors" into their systems) to the US agencies, while under Article 48 GDPR they are forbidden to comply with such orders (unless they are issued under and through a Mutual Legal Assistance Treaty [MLAT]).[31]

Companies in the EU that are served with an order from their own Member State's intelligence agencies to provide certain personal data (or certain classes of personal data), or to allow the building of "back doors" into their system for the benefit of such agencies – i.e., companies in the EU that are ordered to provide "indirect access" or to allow "direct access" to their data by those agencies – face the dilemma that such orders may well be fully in accordance with the relevant national national security law, but with that law not meeting the CJEU/EEGs tests, and the order therefore not being in accordance with the GDPR. They either comply with such orders but may then be acting in breach of the GDPR, or they could refuse to comply with such orders, which would carry its own significant sanctions.

These dilemmas relate to the question of the extent to which private entities such as companies should seek to uphold human rights. It is increasingly accepted that companies (corporations) have serious responsibilities in this regard.[32]

As it is put in the GNI Principles:[33]

> Privacy is a human right and guarantor of human dignity. Privacy is important to maintaining personal security, protecting identity and promoting freedom of expression in the digital age.
> Everyone should be free from illegal or arbitrary interference with the right to privacy

---

[31] Article 48 GDPR (often referred to as "the anti-NSA clause") reads as follows:
"*Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.*"

[32] See Ian Brown & Douwe Korff, Digital Freedoms in International Law, June 2012, prepared for the Global Network Initiative, available at:
https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf
Executive Summary at:
https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20Exec%20Summary.pdf

[33] As explained on the Global Network Initiative (GNI) website, "*GNI Participants [i.e., companies that sign up to the principles] commit to implement the organization's Principles on Freedom of Expression and Privacy ('the GNI Principles'), which provide direction and guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment of these human rights globally.*" The report mentioned in the previous footnote fed into the drafting of the principles.

> and should have the right to the protection of the law against such interference or attacks.[34]
>
> The right to privacy should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws and standards. These restrictions should be consistent with international human rights laws or standards, the rule of law and be necessary and proportionate for the relevant purpose.
>
> - Participating companies will employ protections with respect to personal information in all countries where they operate in order to work to protect the privacy rights of users.
> - **Participating companies will respect and work to protect the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards.**
>
> (emphasis added)

The last bullet-point points to what companies should do when confronted with demands for undue access to personal data they process, from third countries' or from EU Member States' agencies: they should **challenge** such demands, if needs be in the courts.

In fact, even before being actually served with such orders, companies should exercise **due diligence** and **assess** whether, in their home country or in any other country to which they may wish to transfer personal data, they could be exposed to such demands for undue access.

In relation to transfers of personal data to third countries, this is already reflected in both the Standard Contractual Clauses issued by the European Commission[35] and in the EDPB's recommendations on supplementary measures for data transfers.[36]

The SCC decision stresses that any third country data importer should inform the EU data exporter of any laws that could "affect compliance with the clauses" and more specifically of any laws that do not "respect the essence of the [relevant] fundamental rights and freedoms" and that "exceed what is necessary and proportionate in a democratic society".[37] The EDPB recommendations expand on this in considerable detail.[38] Specifically:

> You should in any case pay specific attention to any relevant laws, in particular laws laying down requirements to disclose personal data to public authorities or granting such public authorities powers of access to personal data (for instance for criminal law enforcement, regulatory supervision or national security purposes). If these requirements or powers restrict the fundamental rights of data subjects while respecting their essence and being necessary and proportionate measures in a

---

[34] Taken from Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. [original footnote]

[35] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, OJ L 199, 7.6.2021, p. 31–61, paras. 17 – 19, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.199.01.0031.01.ENG&toc=OJ%3AL%3A2021%3A199%3ATOC

[36] EDPB, Recommendations 01/2020 (footnote 6, above).

[37] See paras. 17 – 19.

[38] See the sections on "*Identifying laws and practices relevant in light of all circumstances of the transfer*", "*Possible sources of information*" and "*Results of your assessment*", paras. 32 – 49, on pp. 14 – 21.

> democratic society to safeguard important objectives as also recognised in Union or EU Member States' law, they may not impinge on the commitments contained in the Article 46 GDPR transfer tool you are relying on.
>
> (para. 35)

In other words, if in a third country there are laws that "*lay[] down requirements to disclose personal data to public authorities or granting such public authorities powers of access to personal data*" *inter alia* for national security purposes, and those "*requirements or powers*" (that of course inherently "*restrict the fundamental rights of data subjects*") do not "*respect[] their essence*" and are not limited to what are "*necessary and proportionate measures in a democratic society to safeguard important objectives as also recognised in Union or EU Member States' law*", then those powers will "*impinge on the commitments contained in the Article 46 GDPR transfer tool you are relying on*" – and "*supplementary measures*" will have to be adopted to protect the data against such undue access. And the data should not be transferred to the third country in question if there are no such "supplementary measures" available that would effectively offer such protection.

In this, the EDPB expressly references the standards contained in its own European Essential Guarantees for surveillance which, the Board says:[39]

> stem from EU law and the jurisprudence of the CJEU and the ECtHR, which is binding on EU Member States.
>
> (para. 42)

Consequently:

> The lack of an essentially equivalent level of protection will be especially evident where the legislation and/or practices of the third country relevant to your transfer do not meet the requirements of the European Essential Guarantees.
>
> (*idem*)

The assessment of a third country's laws is demanding. It should cover:

- the general rule of law situation in the third country (para. 37);
- any relevant rules and practices of a general nature (para. 36);
- whether the legislation governing the access to data by public authorities is ambiguous or not publicly available: "*The first requirement of the European Essential Guarantees is that there should be a legal framework providing for such access, when it is envisaged, that is publicly available and sufficiently clear*." (para. 41);
- whether that legislation meets the other requirements of the EEGs (see above) (para. 42);
- whether any data subject rights are thwarted by the special rules relating to intelligence agencies' access to the data (para. 39) and whether data subjects have "effective redress" against undue access (para. 40).

---

[39] See also footnote 45 to para. 35 of the EDPB Recommendations. Of course, "EU law and the jurisprudence of the CJEU" are not "binding on EU Member States" in relation to their national security activities. See the text after the discussion of the assessments that are required.

It is not sufficient to merely look at "law on paper":

> Relevant legislation in the third country may formally meet EU standards on fundamental rights and freedoms and the necessity and proportionality of restrictions thereto. However, the practices of its public authorities (e.g., accessing personal data held by the private sector or when enforcing -or not- legislation as supervisory or judicial bodies) may clearly indicate that they do not normally apply/comply with the legislation that governs, in principle, their activities. In this case, you must take these practices into account in your assessment and consider that the Article 46 GDPR tool will not be able to effectively ensure, by itself (i.e. without supplementary measures), an essentially equivalent level of protection. In such case, if you wish to proceed with the transfer, you will have to implement adequate supplementary measures.
>
> (para. 43.1, emphasis removed)

The assessment should not be based on state information alone. Rather, all available sources should be consulted; it should be "relevant", "objective", "reliable", "verifiable" and preferably "publicly available or accessible".[40] In an Annex, the EDPB provides the following examples of sources that could be relied upon, listed by order of preference:[41]

- Case-law of the Court of Justice of the European Union (CJEU) and of the European Court of Human Rights (ECtHR) as referred to in the European Essential Guarantees recommendations;
- Adequacy decisions in the country of destination if the transfer relies on a different legal basis;
- Resolutions and reports from intergovernmental organisations, such as the Council of Europe, other regional bodies, and UN bodies and agencies (e.g. UN Human Rights Council, Human Rights Committee);
- Reports and analysis from competent regulatory networks, such as the Global Privacy Assembly (GPA);
- National case-law or decisions taken by independent judicial or administrative authorities competent on data privacy and data protection of third countries;
- Reports of independent oversight or parliamentary bodies;
- Reports based on practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, from entities active in the same sector as the importer;
- Warrant canaries of other entities processing data in the same field as the importer;
- Reports produced or commissioned by Chambers of commerce, business, professional and trade associations, governmental diplomatic, trade and investment agencies of the exporter or other third countries exporting to the third country to which the transfer is made;
- Reports from academic institutions, and civil society organizations (e.g. NGOs);
- Reports from private providers of business intelligence on financial, regulatory and reputational risks for companies;

---

40 See the box on p. 19 of the EDPB Recommendations.

41 Annex 3, footnote references omitted.

- Warrant canaries of the importer itself;
- Transparency reports, on the condition that they expressly mention the fact that no access requests were received. Transparency reports merely silent on this point would not qualify as sufficient evidence as these reports most often focus on access requests received from law enforcement authorities and provide figures only on this aspect while remaining silent on access requests for national security purposes received. This does not mean that no access requests were received but rather that this information cannot be shared;
- Internal statements or records of the importer expressly indicating that no access requests were received for a sufficiently long period; and with a preference for statements and records engaging the liability of the importer and/or issued by internal positions with some autonomy such as internal auditors, DPOs, etc.

The assessment should be written up in a **formal report**. As the EDPB puts it, with reference to Article 5(2) GDPR that spells out the important "accountability" principle:

> You should conduct this overall assessment of the law and practice of the third country of your importer applicable to your transfer with due diligence and document it thoroughly. Your competent supervisory and/or judicial authorities may request it and hold you accountable for any decision you take on that basis.

There is no reason why the above due diligence/legal assessment requirements should not apply in relation to the obtaining (be that by means of [indirect] "pushing"-on-demand or [direct] "pulling") of personal data by any EU Member States intelligence agencies from companies in those states. After all, in both cases – the transfer of personal data to third countries that do not provide "adequate"/"essentially equivalent" protection to the GDPR, or the "pushing" or "pulling" of personal data to an EU Member State intelligence agency – the data leave, and loose, the protection of the GDPR. As noted earlier: "*EU law and the jurisprudence of the CJEU*" are not "*binding on EU Member States*" in relation to their national security activities.[42]

And as the previously mentioned WWWF report makes clear, it cannot be assumed that the laws of the EU Member States that (often vaguely) regulate the actions of the Member States' intelligence agencies "*respect the essence of the [relevant] fundamental rights and freedoms*" and do not "*exceed what is necessary and proportionate in a democratic society*".[43]

In sum: In my opinion, companies that are subject to the GDPR have a due diligence duty to assess whether any personal data they process are at risk of being unduly accessed by intelligence agencies, both in relation to any transfers of those data to "inadequate" third countries and in relation to any possible undue access by EU Member States' agencies including those of their own country of establishment. If they fail to perform this duty, they could be liable for breaches of the GDPR data transfer rules (in relation to the third countries) and for personal breaches (in relation to data being obtained by the EU Member States' agencies).

---

42 See footnote 39, above.

43 See again Douwe Korff, Ben Wagner, Julia Powles, Renata Avila and Ulf Buermeyer, Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes (footnote 12, above).

5. How to address the dilemmas

Above, I believe I have shown the dilemma that can be posed to companies by, on the one hand, there being a risk of being forced to hand over (or allow access to) personal data to a country's intelligence agencies under surveillance laws that do not meet the EEGs standards and, on the other hand, a duty under the GDPR to not disclose the data (in cases of third country transfers, because that would be in breach of the "anti-NSA clause", Article 48; and in cases of demands from EU Member States' intelligence agencies, because that would not be "lawful" or "authorised" and would thus constitute a personal data breach).

Under emerging principles requiring companies to respect and promote human rights including privacy and data protection, the companies should at least **challenge** any such demands including in judicial proceedings; wherever possible, **make their opposition public**; and **publish information on such demands and on the outcome of any challenges**. Moreover, just as in relation to third countries, under the GDPR "accountability" principle, they should **carefully assess the laws of both third countries and EU Member States** to see if they do not allow for undue access to the personal data they process, and they should make a **careful record** of those assessments – and **publish** the results of those assessments.

If private companies would take their duty to protect human rights seriously (a duty that is increasingly recognised at UN and regional levels including at EU level), this could result in a coalition of civil society groups and private companies to guard against undue state surveillance – provided of course that the private companies also themselves abandon surveillance capitalism. Just as many companies are beginning to learn that being environmentally friendly serves both a moral and societal purpose and is in their long-term enlightened self-interest, the same should happen in relation to mass surveillance: neither companies nor states should indulge in it, and decent companies should join civil society groups in fighting it rather than indulging in it. Some major global (US and other) companies may never follow this path, but that should be all the more reason for human rights-conscious European (and American) ones to embark on it.

Of course, such developments would not in themselves remove the dilemma. It remains the case that (as Ian Brown and I have forcefully argued) the only solution to the conundrum is for the intelligence agencies, at least those of the Western democracies, to be brought into a proper international legal framework. But if companies and NGOs were able to make common cause on this issue, that could provide impetus towards that move.

- o – O – o -

Douwe Korff (Prof.)
Cambridge, August 2021