2020 12th International Conference on Cyber Conflict
20/20 Vision: The Next Decade
T. Jančárková, L. Lindström,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2020 © NATO CCDCOE Publications, Tallinn

Up in the Air: Ensuring Government Data Sovereignty in the Cloud

Neal Kushwaha
Founder and Advisor
IMPENDO Inc.
Ottawa, Canada
neal@impendo.com

Bruce W. Watson
Chief Scientist and Advisor
IP Blox and IMPENDO Inc.
Eindhoven, Netherlands
Ottawa, Canada
bruce@ip-blox.com
bruce@impendo.com

Przemysław Roguski
Lecturer
Chair for Public International Law
Jagiellonian University
Kraków, Poland
przemyslaw.roguski@uj.edu.pl

Abstract: Governments around the world commonly use Cloud Service Providers (CSPs) that are headquartered in other nations. How do they ensure data sovereignty when these CSPs, storing a nation's data within that nation's borders, are subject to long-arm statutes on data stored abroad? And what if, in turn, the governmental data is stored abroad, would access to that data constitute a violation of the nation's sovereignty?

This paper examines how selected governments have protected their CSP-hosted data from foreign law enforcement access and suggests methods that other governments might employ to ensure data sovereignty. It addresses these issues in three steps. First, we describe the problem of long-arm jurisdiction with respect to the US Clarifying Lawful Overseas Use of Data (CLOUD) Act and the proposed EU *e-evidence* regulation (EU COM/2018/225 final). Given the extraterritorial reach of these regulations, foreign CSPs looking to maintain good standing with their respective governments and laws may consider storing active copies of their customers' data

and metadata in their home country. For CSPs offering services to the EU, having to comply with an emergency Production Order within 6 hours may not be possible without duplication and active parsing of customer data in a CSP centralised location, foreign to the data owner.

Secondly, we evaluate the recently signed US and UK Executive Agreement under the US CLOUD Act to see if and how the UK protects its own Government Cloud from US law enforcement. We also evaluate France's position, the German model which prohibits storing of government data with US CSPs, and the Polish model recently signed with the US CSP Google, to better understand their positions and approach to managing data sovereignty.

Finally, we offer an assessment on how to balance sovereignty over government data stored in the cloud with the needs of law enforcement for States exercising jurisdiction over CSPs.

Keywords: *cloud, data sovereignty, international law*

1. INTRODUCTION

The classical notion of sovereignty, dating back to the 16th century, signifies the highest authority of a State and the right to exercise its own judgment within a territory.[1] Internally, it denotes the State's exclusive competence to enact and enforce laws binding on its territory and to decide freely in all internal matters not regulated by international law, including the right to control access to its territory.[2] Consequently, violations of sovereignty under international law include violation of territorial integrity and impacting inherently governmental functions. Breaches of sovereignty via cyber means may not be as clear. In July 2015, the UN Group of Governmental Experts (GGE) reached consensus confirming that sovereignty applies to the conduct by States of Information and Communications Technology (ICT) related activities and to their jurisdiction over ICT infrastructure within their territory.[3]

Another aspect of sovereignty is jurisdiction, i.e. the State's right under international law to regulate conduct in matters not exclusively of domestic concern.[4] The GGE

1 PCIJ, *Customs Régime between Germany and Austria (Protocol of March 19th, 1931)*, Advisory Opinion, 1931 PCIJ Series A/B No 41, Sep. opinion Judge Anzilotti, para 13.
2 Samantha Besson, 'Sovereignty' in Rüdiger Wolfrum (ed), *Max Planck Encyclopaedia of Public International Law* (Oxford University Press 2011) para 118ff.
3 UN Doc. A/70/174 paras 26, 27, and 28(b), 'How International Law applies to the use of ICTs'.
4 F.A. Mann, 'The Doctrine of Jurisdiction in International Law', Recueil des Cours de l'Académie de Droit Internationale, 111 (1964), 2.

confirmed in its 2015 Report that 'States have jurisdiction over the ICT infrastructure located within their territory'.[5] However, the GGE did not form a consensus view as to jurisdiction over data stored within that ICT infrastructure. This unresolved question causes significant practical problems.

Consider the following example: a governmental department in State A extends a contract to a Cloud Service Provider (CSP) headquartered in State B. The State A department consumes various cloud services, storing transactional data (emails, calendars, etc.) and master data (names, addresses, social insurance numbers, income, etc.) in the CSP's data centres located in State A and replicated in other data centres under the CSP's control, specifically those in State B. Consider further that State B may authorise its law enforcement agencies to access all data stored by CSPs registered in State B and oblige those CSPs to preserve and hand over the data on production of a warrant. Alternatively, the data in the State B data centre is breached by foreign non-state actors and copied to data centres located in State C. The non-state actors then publicly share the content from the State C data centres for anyone to consume, exposing conversations, contacts and State A citizen data, risking identity theft, cybercrimes and more.

In both examples, State A loses control over its data, at the same time enabling another sovereign (in variant 1) to exercise control over that data by virtue of it being stored in that State's territory. This article explores the concept of data sovereignty and asks whether unconsented access to government data stored abroad would constitute a violation of a State's sovereignty; and what States can do to ensure continued control over their data.

This is not only a theoretical problem. At the time of writing, the Government of Canada[6] (GC) has been consuming cloud services for over 7 years.[7] Services such as those provided by Google, Microsoft, Amazon, ServiceNow, and Salesforce are currently being used for production workloads. Various Canadian departments, agencies, crown corporations, tribunals, etc. (herein collectively called departments) use cloud capacities in a variety of ways. Some have email services fully hosted in the cloud, while others use unique services in conjunction with existing internal services.[8]

5 UN Doc. A/70/174 para 28(a).

6 By virtue of the origin and experience of two of the authors, Canada is used throughout the text as an example of a government that may benefit from reviewing its approach to the cloud through the lens of international law and its applicability to governmental data stored domestically or abroad.

7 See Jean-Martin Thibeault, 'This just in! Canadian Broadcasting Corporation moves 12,000 accounts to Google Apps in 90 days' (Google Cloud Official Blog, 14 May 2013), https://cloud.googleblog.com/2013/05/this-just-in-canadian-broadcasting.html [14.04.2020]. Canadian Broadcasting Corporation (CBC) is a Canadian Crown Corporation and is accountable to the Canadian Parliament.

8 Naming these departments and describing the respective services they consume is not the purpose of this paper.

Large US CSPs such as Microsoft and Amazon Web Services commonly operate and offer their services in Canada under a Canadian corporation. Both Microsoft Canada and Amazon Web Services Canada now offer their Canadian customers the option to host their data in Canadian data centres. Although a Canadian citizen, corporation or the GC may consider this adequate, with the enacting into law of the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act),[9] these Canadian entities may not only be exposing their data to various law enforcement agencies within the US, but also to other States holding executive agreements with the US.

The problems described above are universal, though, and other countries are also grappling with them. How do nations consuming (or intending to consume) CSP services ensure data sovereignty while the nations where the CSPs are headquartered enact new laws?

This paper begins by introducing the concept of 'data sovereignty' and describing some of the implications of long-arm jurisdictions for Internet Service Providers (ISPs) and CSPs and how they will likely manage the tight timelines for evidence requests. It then performs a high-level evaluation of the US and UK Executive Agreement,[10] France's position, the Domestic Cloud Provider (DCP) agreement of Chmura Krajowa (under the Polish Development Fund and PKO Bank Polski) to manage and resell Google's cloud offering,[11] and Germany's GAIA-X project.[12]

We close the paper with suggestions for nations to move forward with consuming cloud services while ensuring data sovereignty.

2. THE CONCEPT OF DATA SOVEREIGNTY

The concept of data sovereignty has been the topic of scholarly debate for some time,[13] but has recently gained traction within States as well.[14] It is not yet a fully

9 Consolidated Appropriations Act of 2018, Pub. L. No. 115-141, 132 Stat. 348, div. 5 (2018).

10 Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime [CS USA No.6/2019], https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019 [14.04.2020], hereinafter '*US-UK Agreement*'.

11 Operator Chmury Krajowej, *Press release of 27 September 2019*, https://chmurakrajowa.pl/partnership.html [14.04.2020].

12 Bundesministerium für Wirtschaft und Energie, *Das Projekt GAIA-X, Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems*, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.html, also available in English: https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.html [14.04.2020].

13 Jing de Jong-Chen, 'Data Sovereignty, Cybersecurity and Challenges for Globalization', Georgetown Journal of International Affairs, (Fall 2015), 112-122; Patrik Hummel, Matthias Braun et al., 'Sovereignty and Data Sharing', ITU Journal: ICT Discoveries, Special Issue No. 2; Andrew Keane Woods, 'Litigating Data Sovereignty' (2018) 128 Yale Law Journal 328.

14 Bundesministerium für Wirtschaft und Energie, *Das Projekt GAIA-X, Eine vernetzte Dateninfrastruktur*, 6.

settled term and States use it in conjunction with other notions such as technological sovereignty[15] or digital sovereignty.[16] For the purposes of this paper, it is best to look at these concepts as akin to a Russian doll, where the broadest concept, technological sovereignty, encompasses the narrower digital sovereignty, which in turn encompasses data sovereignty. Technological sovereignty has been described by European Commission President Ursula von der Leyen as Europe's capability 'to make its own choices, based on its own values, respecting its own rules' in the field of tech.[17] It includes, amongst others, the integrity and resilience of data infrastructure, networks and communications[18] and the development of autonomous capacities in the field of artificial intelligence.[19] The slightly narrower term of 'digital sovereignty' (or '*souveraineté numérique*') has been gaining popularity mainly in France, where it was first introduced by Pierre Bellanger, president of Skyrock,[20] and since then taken up by State organs such as the French Senate,[21] but has been also used by other States such as Germany. In the German view, 'digital sovereignty' (or '*digitale Souveränität*') denotes the 'capability to take autonomous actions and decisions in the digital environment'.[22] The French view is similar and refers to the application of the principle of sovereignty to cyberspace and includes, amongst other aspects relating to the ability to detect and react to threats in cyberspace,[23] control over data in cyberspace.[24]

15 European Commission, *Shaping Europe's Digital Future*, February 2020, 3, doi:10.2759/091014 [14.04.2020]; for a discussion of the term 'technological sovereignty' see also Tim Maurer et al., 'Technological Sovereignty: Missing the Point?', in: M.Maybaum, A.-M.Osula, L.Lindström (Eds.), *2015 7th International Conference on Cyber Conflict:Architectures in Cyberspace*, (NATO CCDCoE Publications 2015), 53ff.

16 French Ministry for Europe and Foreign Affairs, *Intervention de Jean-Yves Le Drian, ministre de l'Europe et des Affaires étrangères, au colloque 'Au-delà de 1989 Espoirs et désillusions après les révolutions*', Speech by Minister Jean-Yves Le Drian in Prague on 6 December 2019, https://www.diplomatie.gouv.fr/fr/dossiers-pays/republique-tcheque/evenements/article/intervention-de-jean-yves-le-drian-ministre-de-l-europe-et-des-affaires [14.04.2020] (referring to the need to construct 'European digital sovereignty' (*souveraineté numérique européenne*)).

17 Ursula von der Leyen, 'Tech Sovereignty Key for EU's Future Goals', *The Irish Examiner* (Cork, 18 February 2020), https://www.irishexaminer.com/breakingnews/views/analysis/ursula-von-der-leyen-tech-sovereignty-key-for-eus-future-goals-982505.html [14.04.2020].

18 European Commission, *Shaping Europe's Digital Future*, February 2020, 3, DOI:10.2759/091014 [14.04.2020].

19 European Commission, *Press remarks by President von der Leyen on the Commission's new strategy: Shaping Europe's Digital Future*, 19 February 2020, https://ec.europa.eu/commission/presscorner/detail/en/speech_20_294 [14.04.2020].

20 Pierre Bellanger, 'De la souveraineté en général et de la souveraineté numérique en particulier', *Les Echos* (30 August 2011), http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm [14.04.2020]; Pierre Bellanger, La Souveraineté Numérique (Stock 2014).

21 Commission d'enquête sur la souveraineté numérique, *Rapport de Gérard LONGUET sur la souveraineté numérique, fait au nom de la commission d'enquête*, Rapport n° 7 (2019-2020), (Report, 1 October 2019), http://www.senat.fr/rap/r19-007-1/r19-007-1.html [14.04.2020], hereinafter Rapport n° 7.

22 Bundesministerium für Wirtschaft und Energie, 'Digitale Souveränität im Kontext plattformbasierter Ökosysteme', 6, https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digitale-souveraenitaet.pdf [14.04.2020].

23 French Ministry of the Armies, 'International Law Applied to Operations in Cyberspace', https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [14.04.2020].

24 Rapport n° 7, 17.

Therefore, the issue of control is the heart of the concept of data sovereignty.[25] In its classical form, sovereignty denotes supreme authority over territory to the exclusion of other sovereigns.[26] Within the specified territory, the sovereign has the exclusive power to exercise its own judgment.[27] It can control access to its territory and enact and enforce laws with respect to persons and objects within this territory. This traditional understanding is challenged by data in cyberspace. As it is only bits and bytes, which can be moved instantaneously across borders, copied, stored in multiple locations and split into parts, while remaining accessible from within the territory, data becomes 'un-territorial'.[28] Given that territoriality loses its importance with respect to data in cyberspace, the main aspect of sovereignty over data becomes the exclusive authority or control: 'sovereign data subjects are those who are in a position to articulate and enforce claims to power about their data'.[29] Consequently, the concept of data sovereignty denotes exclusive control over stored and processed data and the ability to decide who is granted access to that data.[30]

With respect to the topic of this paper, data sovereignty is particularly relevant in the context of cloud computing. Given that governments are increasingly moving their services and data, including both governmental and citizens' data, to the cloud, *who* exercises control over it is a question of sovereignty. As many of the largest CSPs are located in the United States and CSPs are currently free to store data in offshore data centres, governmental data could be stored on servers within the territories of several States and be subject to the jurisdiction, and thus sovereign control, of each of those States. Thus, competing jurisdictions and control over network infrastructure (data centres) and CSPs directly challenge the exclusive control a government may expect over its data, and States' sovereignty over their data in general.[31]

In the next two sections, we will discuss how States gain control over data through long-arm jurisdiction over CSPs residing or operating within the territory of those States and how other States react to meet this challenge and protect their data sovereignty.

25 See, e.g. Bundesministerium für Wirtschaft und Energie, *Das Projekt Gaia-X: Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems*, 15, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.pdf [14.04.2020], defining 'data sovereignty' as 'guarantee of control over the use of data' ('*Garantie der Datennutzungskontrolle*').

26 Samantha Besson, 'Sovereignty' in Rüdiger Wolfrum (ed.), *Max Planck Encyclopaedia of Public International Law* (Oxford University Press 2011) para 118ff.

27 PCIJ, *Customs Régime between Germany and Austria (Protocol of March 19th, 1931)*, Advisory Opinion, 1931 PCIJ Series A/B No 41, sep. opinion Judge Anzilotti at para 13.

28 Jennifer Daskal, 'Borders and Bits' (2018) 17 Vanderbilt Law Review 179, 181; see also Jennifer Daskal, 'The Un-Territoriality of Data' (2015) 125 Yale Law Journal 326.

29 Patrik Hummel, Matthias Braun et al., 'Sovereignty and Data Sharing', ITU Journal: ICT Discoveries, Special Issue No. 2, 2.

30 Bundesministerium für Wirtschaft und Energie, *Digitale Souveränität im Kontext plattformbasierter Ökosysteme*, .6, https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/p2-digitale-souveraenitaet-plattformbasierter-oekosysteme.pdf [14.04.2020].

31 For a broader discussion of this argument, see Andrew Keane Woods, 'Litigating Data Sovereignty' (2018) 128 Yale Law Journal 328, 360 ff.

3. LONG-ARM JURISDICTIONS

Both the US CLOUD Act and the draft EU Regulation on European Production and Preservation Orders for electronic evidence[32] allow for the preservation and production of data stored by a service provider in another jurisdiction as evidence in criminal investigations.

The US CLOUD Act (title 18 U.S.C. §2713) allows for extraterritorial reach of all US CSP data. Under 'Required preservation and disclosure of communications and records', it specifically states:

> 'A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States'.

Specific in its timelines, the EU COM/2018/225 final proposal requires Member States to respond to requests within 10 days for standard requests and 6 hours in an emergency.[33] The previous response times were on average 10 months for Mutual Legal Assistance and 120 days for European Investigation Orders.[34] The Production Orders and Preservation Orders relate to four data types listed in the proposal and apply to any service provider, regardless of where the parent company is located or where the data is held.[35]

1. **Subscriber data:** personal information used to identify an individual, commonly considered Protected B[36] information at the GC level, including

32 Proposal for a Regulation of the European Parliament and the Council on European Production and Preservation Orders for electronic evidence in criminal matters, EU COM/2018/225 final - 2018/0108 (COD).

33 Ibid. Article 9 'Execution of an EPOC', all paragraphs describe the deadlines and how to respond.

34 'What will the new rules change?' in the European Commission's *Frequently Asked Questions: New EU rules to obtain electronic evidence*, 17 April 2018, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345 [14.04.2020].

35 EU COM/2018/225 final. Article 2 'Definitions', paragraphs 6-10 define and describe electronic evidence as four data types.

36 In Canada, the compromise of 'Protected' information or assets could cause various levels of injury to a non-national interest. The Protected levels are described as A, B, and C. The compromise of 'Classified' information or assets could cause various levels of injury to national interests. The Classified levels are Confidential, Secret and Top Secret. See Treasury Board of Canada Secretariat, *Directive on Security Management - Appendix J: Standard on Security Categorization*, 01 July 2019, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32614 [14.04.2020]. It should be noted that certain Canadian Crown Corporations (e.g. Bank of Canada) create their own security categorisations which do not align with those described in Appendix J. See Treasury Board of Canada Secretariat, *List of Crown corporations*, 02 February 2019, https://www.canada.ca/en/treasury-board-secretariat/services/guidance-crown-corporations/list-crown-corporations.html [14.04.2020].

name, address, billing information, date of birth, email address, telephone number, etc.

2. **Access data:** a component of metadata, including the logon and log-off dates and times, IP addresses assigned by service providers, etc. It is common to all internet users and generally available from ISPs, and includes IP addresses assigned to the user and the connection times.
3. **Transactional data:** a component of metadata, including geolocation of the source and destination of the data, size of data, route, communication protocol, etc., available from the ISP and CSP. The ISP is able to describe the route and the internet services the user has consumed (examples: access to websites, use of encryption, download of data streams, etc.) while the CSP is able to describe the opening and closing times of a document stored at the CSP, the length of time spent composing an email over the CSP infrastructure, the recipients of the email, and more, but not the content of the document or email.[37]
4. **Content data:** the digital data consumed by the user in voice, video, audio, text, images, etc.

From the perspective of managing criminal proceedings, the US CLOUD Act and EU proposal make it easier to quickly request and gather electronic evidence, however, this places a burden on CSPs. Being prepared to respond to a potential 6-hour or 10-day response for a Production Order likely means the CSP will invest in resources (including staff, equipment and software) to help manage these quick turn-around requests. This investment is unlikely to be in each country in which it operates and will probably be in a central location, at least for the smaller CSPs.

CSPs and ISPs are often not the same company and that likely means the request must go to at least two different parties. Furthermore, users often store information at more than one CSP; for example, data may be stored on Google Drive and in Amazon containers while using email services from Microsoft Office 365. It is thus possible that a Production Order may reach multiple companies.

By way of an example, Canadian ISPs already have the responsibility to provide basic metadata data to law enforcement agencies when lawfully requested.[38] Besides their customers' online activity, ISPs maintain records of user logon and log-off dates and times along with associated IP addresses. This log data is very simple to parse, join with customer account datasets and use for reporting.

On the other hand, due to the volume and velocity of log data, CSPs looking to remain in good standing with their respective governments and laws may consider keeping active copies of their customers' metadata (activity logs) and possibly their customers'

37 Content data (data type #4) may be encrypted and inaccessible to the CSP.
38 See Canada's Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 7(3)(c).

data in their headquarters country for easy and centralised parsing. For those offering services to the EU, having to comply with an emergency Production Order in 6 hours may not be possible without duplication and active parsing of customer data and/or metadata.

The duplication of data into a CSP's data centre located in another country may result in a breach of sovereignty, while the constant parsing of customer data and metadata may be considered a breach of privacy. CSPs will need to remain aware of laws in the various States they operate in, and international law, all at the same time. This complicated legal knowledge coupled with the required technical knowledge may be economically unreasonable for smaller CSPs and start-ups.

4. INTERNATIONAL POSITIONS

A. US-UK Executive Agreement

The first international cooperation agreement (Agreement) under the US CLOUD Act was signed on 3 October 2019 between the United States and the United Kingdom.[39] Its aim is to create a mechanism for cooperation in allowing law enforcement agencies access to data stored outside their territory and held by service providers registered in a State party to the agreement. In this regard, it will be most beneficial to the UK, allowing it to make direct requests to American CSPs and therefore overcoming the blocking provisions of the US Stored Communications Act, which had previously prevented American CSPs from handing over data stored in the US to foreign law enforcement agencies.[40] In short, the Agreement allows the parties to directly request from CSPs stored content data, traffic data or metadata, subscriber information and intercept wire electronic communications related to a serious crime investigation (Article 1(3)).

Production Orders may be addressed directly to the Covered Providers (i.e. any private entity which provides to the public the ability to communicate or to process or store computer data, by means of a Computer System or a telecommunications system; or processes or stores Covered Data, Article 1(7)) and the Providers have to produce the information directly to designated authorities of each Party (Article 10).

The Agreement includes limitations on the use and transfer of data (Article 8) and privacy and data protection safeguards (Article 9). Both parties certify that their legal

39 US-UK Agreement [CS USA No.6/2019].

40 Theodore Christakis, *21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)*, https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/ [14.04.2020]; see also Jennifer Daskal, Peter Swire, 'The UK-US CLOUD Act Agreement is Finally Here, Containing New Safeguards', (*Just Security*, 08 October 2019), https://www.justsecurity.org/66507/the-uk-us-cloud-act-agreement-is-finally-here-containing-new-safeguards/ [14.04.2020].

systems have adequate protections for privacy and civil liberties (which is required by the CLOUD Act for the US to enter into such an agreement) and the Agreement establishes procedural requirements and oversight mechanisms to comply with privacy requirements.[41] Under Article 5(10) of the Agreement, the party issuing a Production Order is obliged to notify the authorities of a third country, where an 'Order subject to this Agreement is issued for data in respect of an individual who is reasonably believed to be located outside the territory of the Issuing Party and is not a national of the Issuing Party'. This is with the exception of cases where notification would endanger national security or the notification would imperil human rights.

Three inherent limitations of the US-UK Agreement need to be stressed. *Firstly*, pursuant to Article 6(3) of the Agreement, it 'does not in any way restrict or eliminate any legal obligation Covered Providers have to produce data in response to Legal Process issued pursuant to the law of the Issuing Party'. Consequently, Article 6(3) does not exclude the parallel application of national provisions such as the CLOUD Act to data of persons covered by the Agreement. Thus, US law enforcement can request the production of data of UK (or EU) persons held by CSPs falling under the CLOUD Act, without necessarily having to fulfil other obligations under the Agreement, such as the notification of third parties.[42] Therefore, it is not clear under which incentives US law enforcement would choose to use the Agreement, rather than the CLOUD Act.[43]

Secondly, the Agreement authorises both parties to request from CSPs data of persons residing in a third country (such as Canada or the European Union Member States, for example), provided it is stored in the territory of the parties.[44] In effect, this might create conflicts with third States, which would presumably not take kindly to such practices or might also resort to applying such measures themselves.

Thirdly, the Agreement does not address the question of governmental data or data of government employees which might be connected with the exercise of their official duties and thus affect not only the interests of those individuals, but also the sovereign interests of the State. Thus, if an American CSP holds data under a contract with a British governmental agency, the CLOUD Act remains potentially applicable and the CSP might still be required to hand over such data to American law enforcement if duly ordered to do so.

41 Nathan Swire, 'Applying the CLOUD Act to the U.S.-UK Bilateral Data Access Agreement', (*Lawfare*, 28 October 2019), https://www.lawfareblog.com/applying-cloud-act-us-uk-bilateral-data-access-agreement [14.04.2020].

42 Theodore Christakis, '21 Thoughts and Questions about the UK-US CLOUD Act' (*European Law Blog*, 17 October 2019), https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/ [14.04.2020].

43 Ibid.

44 Ibid.

In sum, the US-UK Executive Agreement on access to electronic data to combat serious crime is a welcome step to address issues of extraterritorial data Production Orders with a dedicated international legal instrument. Nevertheless, the subjection of the Agreement to domestic provisions such as the CLOUD Act raises certain questions as to its status under international law.[45] For the purposes of this analysis, it is important to note that the main issue with governmental cloud systems depending on the services of foreign CSPs is not addressed. The Agreement governs only Production Orders for data of individuals that is needed to combat serious crimes, not industrial or governmental data. Neither does it give the UK government a way to address potential Production Orders for governmental data by American law enforcement, be it under the CLOUD Act or other provisions of domestic law, within an agreed international framework. This issue therefore remains unresolved by the Agreement.

B. France

France was one of the pioneers of the notion of digital sovereignty (*souveraineté numérique*) in Europe.[46] In 2019, the French Senate convened an Inquiry Committee (*Commission d'Enquête*) on the topic of digital sovereignty with the aim of studying the issue and formulating policy recommendations. Its final report, presented by Rapporteur Gérard Longuet, critically examined, among others, the question of cloud storage and extraterritorial jurisdiction.[47] It held that in the modern world, data has become an economic strategic issue (*enjeu économique stratégique*) of immense importance to the activities of the major actors of the digital economy.[48] The report discussed the question of data localisation as one of the modes of protecting data, but found it an imperfect solution.[49] It found that data localisation rules might be important with respect to securing digital sovereignty in three instances: in cases of strategic or particularly sensible data such as data pertaining to public finances (*traitements publics souverains*), private financial data or commercial secrets, to guarantee access to essential services and to support the industrial ecosystem of cloud providers.[50]

The report noted, however, that data localisation clauses do not ameliorate the risks posed both by extraterritorial legislation such as the CLOUD Act and the dependence of certain technology companies on their States, as with certain Chinese companies.[51] It criticised the CLOUD Act as being too broad with respect to the affected entities,

45 Ibid.
46 For an overview of French scholarly literature on this matter Pierre Bellanger, *La souveraineté numérique*, (Paris, Stock 2014); Marin Brenac, Pierre-Luc Déziel, *La souveraineté numérique sur les données personnelles : étude du règlement européen no 2016/679 sur la protection des données personnelles à l'aune du concept émergent de souveraineté numérique*, (Québec, Université Laval 2017); Pauline Türk, Christian Vallar, *La souveraineté numérique: le concept, les enjeux*, (Paris, Editions Mare & Martin 2018).
47 Rapport n° 7.
48 Ibid, 54.
49 Ibid, 68.
50 Ibid.
51 Ibid, 69.
52 Ibid, 71.

the infractions covered and the type and amount of data collected[52] and found the CLOUD Act to pose a risk of access by American law enforcement to strategic data of legal persons and to be incompatible with the GDPR with regard to the protection of personal data.[53]

The report discusses three options to mitigate those risks: *firstly*, the legal separation of subsidiary companies for each region and geographical location of services;[54] *secondly*, mobilising companies on a case-by-case basis to contest excessive law enforcement demands in court; and, *thirdly*, the extensive use of robust data encryption technologies.[55] Similar to the report of 26 June 2019, prepared for the French Prime Minister by Raphaël Gauvain,[56] the Longuet Report advises the strengthening of the 1968 law on blocking measures,[57] extending the protections of the GDPR to non-personal data of legal persons and sanctioning their 'improper transmission' (*transmission indue*) and encouraging the fast conclusion of a cooperation agreement between the European Union, its Member States and the US.[58]

While none of these measures has been implemented at the time of writing, what becomes clear from the Gauvain and Longuet reports is that France is deeply concerned about American (and Chinese) extraterritorial reach, brought about by their dominance in the software and hardware sectors, respectively. The French view is that it has to take robust action, both legislative and in terms of industrial policy, to protect French data and French strategic interests against the reach of foreign States, even like-minded States such as the US.

C. Germany

Similar considerations underpin the German position with respect to American cloud services. Ever since the Snowden revelations, Germany has been deeply worried about the access of the US National Security Agency and US law enforcement to German data. The German government has repeatedly stressed that while it recognises the importance of facing up to novel challenges to law enforcement posed by the proliferation of transnational cloud services, any solution needs to respect fundamental

53 Ibid, 72.

54 The report refers as an example to the French company OVH, which has set up a dedicated company for its activities in the United States, presumably to separate the parent company's data from American law enforcement requests.

55 Ibid, 74.

56 Raphael Gauvain, *Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale, Rapport à la demande de Monsieur Édouard Philippe, Premier Ministre*, (Report, 26 June 2019), https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000532.pdf [14.04.2020].

57 Referring here to a 1968 Statute prohibiting, subject to international treaties, the passing on to foreign governments of documents or information of an economic, commercial, industrial, financial or technical nature, the communication of which is likely to undermine France's sovereignty, security, essential economic interests or public order. 'Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères', https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000501326&categorieLien=cid [14.04.2020].

58 Rapport n° 7, 75.

human rights and facilitate cooperation between States. To this end, it advocates rapid negotiations between the European Commission and the US government to conclude a cooperation agreement on data sharing, as envisaged by the CLOUD Act.[59]

Germany also seeks to secure its digital sovereignty (*digitale Souveränität*), limiting US law enforcement access to German data. This is done via two routes: *firstly*, by limiting the type of data that can be stored on US cloud services; and *secondly*, by developing an autonomous cloud storage solution. It is interesting to note that the first route is driven not only (or even predominately) by the government, but by regional data protection agencies. For instance, the Hessian Commissioner for Data Protection and Freedom of Information (*Der Hessische Beauftragte für Datenschutz und Informationsfreiheit*) has forbidden schools in the Land of Hesse to use Microsoft Office 365 services or to store students' personal data in the cloud if the providers are subject to US law. He said that 'public institutions in Germany have a special responsibility regarding the permissibility and traceability of the processing of personal data [and that] the digital sovereignty of State data processing must also be guaranteed'.[60] The main reason for this statement is that Microsoft, like other CSPs, does not reveal what kind of data is being transmitted to the US and whether US law enforcement would be able to access this data.

To address these concerns, on 29 October 2019, the German government launched the GAIA-X project.[61] The stated motivation for this project is to preserve European 'data sovereignty' (*Datensouveränität*) against increasing dependence on foreign digital technologies.[62] The report defines digital sovereignty as the 'possibility of independent self-determination of State and organisations' with regard to the 'use and design of digital systems themselves, the data generated and stored therein and the processes represented by them'[63] and data sovereignty as 'guarantee of control over the use of data' (*Garantie der Datennutzungskontrolle*).[64]

Germany wants to create a data infrastructure that would guarantee European control over the data of European citizens and reduce dependence on foreign CSPs.[65] This is to be done by linking centralised and decentralised infrastructures (cloud and

59 Bundesregierung, *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE*, BT-Drs. 19/3392, 2.

60 The Hessian Commissioner's statements are not limited to Microsoft, but also apply to other US CSPs. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, *Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen*, 09 July 2019, https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-für-datenschutz-und [14.04.2020].

61 Bundesministerium für Wirtschaft und Energie, *Das Projekt GAIA-X: Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems*, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.pdf [14.04.2020].

62 Ibid, 6.

63 Ibid, 7.

64 Ibid, 15.

65 Ibid, 9.

edge services) into one coherent system, based on open technologies and providing interfaces for the facilitation of data exchange and use of applications.[66] Crucially, this is to be done based on existing and yet-to-be-built European services and infrastructure, thereby limiting the exposure to US law enforcement by cutting out US headquartered CSPs. It is not surprising that these US companies, feeling the threat of a loss of market share in the important European market, are intensively lobbying against such autarky, rather singing the praises of the benefits of cooperation and investing in data centres located in key European States to alleviate concerns about data localisation.[67]

D. Poland

However, not every European State follows the path of achieving digital sovereignty through the exclusion of US CSPs from access to key data. In 2018, the Polish government launched the programme 'Common Information Infrastructure of the State' (*Wspólna Infrastruktura Informatyczna Państwa*, WIIP), which aims at creating two public cloud services: Public Computational Clouds (*Publiczne Chmury Obliczeniowe*) and a Governmental Computational Cloud (*Rządowa Chmura Obliczeniowa*).[68] With this, the Polish government does not exclude foreign CSPs, but rather applies different security and access standards to different types of data. For instance, the Public Computational Cloud (or simply 'National Cloud', *Chmura Krajowa*) will be set up in partnership with Google, which will build a Google Cloud hub in Warsaw.[69]

Currently, the largest and most strategically important client of the National Cloud is the largest bank in Poland, PKO BP and the National Cloud is aimed predominately at the private sector. Public and local administration will be able to use the Governmental Computational Cloud, which is currently in the phase of planning and in November 2019 issued a call for expressions of interest by those entities that would like to take part in a tender for setting up such a cloud service.[70] For this public cloud, the government will set up security requirements and a Governmental Security Cluster (*Rządowy Klaster Bezpieczeństwa*), presumably for the most sensitive data.[71]

66 Ibid, 12.

67 See Sabine Bendiek, 'Digitale Souveränität durch Partnerschaft: Wie Deutschland und Europa ihre Cloud-Zukunft selbstbestimmt gestalten können', (*Microsoft Blog*, 28 October 2019), https://www.microsoft.com/de-de/berlin/artikel/digitale-souveraenitaet-durch-partnerschaft.aspx [14.04.2020].

68 Poland Ministry of Digital Affairs decision on Common Infrastructure of the State: Ministerstwo Cyfryzacji, *Wspólna Infrastruktura Informatyczna Państwa*, https://www.gov.pl/web/cyfryzacja/wspolna-infrastruktura-panstwa-wip-20 (last modified 27.09.2019 12:11) [14.04.2020].

69 Operator Chmury Krajowej, 'Strategiczne partnerstwo Operatora Chmury Krajoweji Google dla cyfryzacji polskiej gospodarki', (Press release, 27 September 2019), https://chmurakrajowa.pl/pdf/informacja_prasowa_27.09.2019.pdf [14.04.2020].

70 Michał Duszczyk, 'W 2020 roku państwo przeniesie się do chmury', (*Rzeczpospolita*, 05 October 2019), https://cyfrowa.rp.pl/it/41069-w-2020-roku-panstwo-przeniesie-sie-do-chmury [14.04.2020].

71 Ibid.

It remains to be seen whether Poland will exclude foreign CSPs from this Governmental Security Cluster or try to secure governmental data contractually and through encryption. It has to be noted, however, that Poland cannot rely on big national CSPs and therefore is dependent on outside expertise for its national cloud and is thus limited in a potential quest for digital sovereignty.

E. Preliminary Conclusions

By way of a preliminary conclusion, we can see that there is no one universal way in which States try to ensure their data sovereignty against the challenge posed by the US CLOUD Act and the potential long-arm jurisdiction over European data stored with US CSPs. The potential reactions range from data localisation laws such as in Russia or China,[72] through treaty-based cooperation with the United States (the US-UK Agreement, for example), contract-based cooperation with US CSPs using software solutions while building a localised data cluster (Poland), to escaping from US long-arm jurisdiction by legislative decoupling (France) and technological independence (Germany). All these examples, however, show that States recognise the need to ensure sovereignty over their own and their citizens' data and limit its exposure to the control and access by other sovereigns, in particular the US.

5. RECOMMENDATIONS: BALANCING SOVEREIGNTY

The preceding analysis has shown that Western States in general and European States in particular are increasingly conscious of challenges to their sovereignty, understood as the capability for autonomous action, that stem from the rapid development of digital technologies. Especially with regard to the rising importance of personal, business and governmental data in digital (data-driven) economies and in view of US technological dominance in the sector of cloud storage, cloud services and data processing, these States frame their sovereignty in terms of exclusive control over data stored in the cloud, to the exclusion of third States acting through their organs, for instance law enforcement agencies. Therefore, it becomes a priority to find solutions which reconcile the continued consumption of services of foreign-headquartered CSPs, the needs of law enforcement and the protection of sensitive data from unauthorised or excessive access by law enforcement agencies of third States.

The preceding analysis also discusses different ways how States such as the UK, France, Germany or Poland address these issues of data sovereignty vis-à-vis US CSPs in view of the US CLOUD Act's long-arm jurisdiction over foreign data stored by these CSPs. In our view, the concerns raised by France and Germany over their data sovereignty are not confined to those States, but describe a universal challenge to and evolution of the understanding of the principle of sovereignty in cyberspace.

72 John Selby, 'Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?', (2017) International Journal of Law and Information Technology, Volume 25, Issue 3, 213–232.

States will increasingly face difficult policy decisions with regard to deciding how best to balance competing sovereign interests. Based on the described policy and legal approaches to 'data sovereignty', we propose seven actions for consideration by States that have not yet specifically addressed the issues discussed in this paper. Actions A, B, C and D are likely to be completed sequentially, followed by actions E, F and G, which could be executed concurrently. Of course, all of these recommendations involve speculation by the authors and will require further debate.

A. Formulate a Domestic Policy for Cloud Storage and Take a Position on 'Data Sovereignty'

Addressing the described challenges of control over data in cyberspace requires a two-step analytical exercise. *Firstly*, the government should formulate a domestic policy for cloud storage, taking into account the problems described above. *Secondly*, the government should analyse the issues regarding the interpretation of the principle of sovereignty and its application in cyberspace, especially with regard to the questions of jurisdiction and data sovereignty. This position should not only address the question of the applicability of international law to cyber operations, as done by various other governments, but also the challenges of jurisdiction, in particular with regard to data, as the Dutch government has done.[73] Such a position is especially important for States which do not have sovereign CSPs or where many companies and government departments are consuming cloud facilities from CSPs headquartered in a foreign State.

B. Enact Rules for the Distribution or Sharing of Sensitive Data

Pass a bill (and enact into law) rendering unlawful the distribution or sharing of the country's sovereign State data without permission from the government, including that which is stored in cloud capacities in other nations. Much like France's legislative[74] and industrial policy to protect French data against the reach of foreign States (including the US) and Germany's Hessian Commissioner's decision to forbid schools in the Land of Hesse to store students' personal data in the cloud if the providers are subject to US law,[75] other States must also move to manage the potential risk to their government and citizens if such data were to escape the State's control.

73 Dutch Ministry of Foreign Affairs, *Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, Appendix*, (Government document, 5 July 2019), https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [14.04.2020].

74 Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères', https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000501326&categorieLien=cid [14.04.2020].

75 See Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, *Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen*, 09 July 2019, https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-für-datenschutz-und [14.04.2020].

Possible positions include that the State's data can be accessed only with permission, thereby obliging nations to notify when such data is delivered to or requested by another nation. This action may seem particularly challenging as it requires political support; however, the politicians of the particular nation should be made aware of the challenges their nation faces and that there is a roadmap to make them manageable.

C. Clearly Classify Data

To represent data that is to remain within the State's borders, some States mark the content with limited dissemination control marking.[76] States should consider a similar marking or use of an existing marking that represents data sovereignty to identify information that may reside in a foreign country or not.

Besides technical requirements to transmit or store data abroad which remain the primary focus for some countries, States should consider defining legal requirements for storing data abroad. As an example, some Canadian medical clinics operated as corporate entities store their patient data in the cloud (or in software that is backed up in the cloud), without fully understanding the risks related to such decisions. The legal requirements for storing citizen or government data in the cloud should also extend to corporations and similar entities.

D. Enter into Bilateral Agreements with the US, UK and EU

Negotiate and sign bilateral agreements, where applicable, on legitimate law enforcement access to data stored abroad with States that have adopted a national regulatory framework for cloud computing, such as the US (US CLOUD Act) and the UK (Crime Overseas Production Orders COPO Act 2019[77]). The purpose of such agreements would be to define, based on reciprocity, the scope of legitimate law enforcement access to data of the nation's legal and natural persons stored in data centres on the territory of other States and controlled by those other States' CSPs (e.g. the US, thus putting them within reach of the US CLOUD Act). However, the governments should also consider concluding separate agreements or including special provisions for governmental data, according to its inviolability for law enforcement purposes, similar to the Agreement between Estonia and Luxembourg for the hosting of data and information systems.[78]

76 Such as NOFORN to represent "no foreign dissemination", or CEO to represent "Canadian eyes only," in Canada. Admittedly, CEO marked assets and information are sometimes shared with "Foreign Integrees" who sign non-disclosure agreements. The GC is aware of the challenges this may bring and has requested all departments restrict CEO assets and information access to Canadians only. Canadian Committee On National Security Systems, *CCNSS Bulletin Edition 1*, March 2018, 3, https://www.cyber.gc.ca/sites/default/files/publications/ccssn-1-eng.pdf [14.04.2020].

77 Crime (Overseas Production Orders) Act 2019, c. 5.

78 *Agreement between the Grand Duchy of Luxembourg and the Republic of Estonia on the hosting of data and information of 20 June 2017, as appended to Loi du 1er décembre 2017 portant approbation du « Agreement between the Grand Duchy of Luxembourg and the Republic of Estonia on the hosting of data and information systems »*, http://data.legilux.public.lu/eli/etat/leg/loi/2017/12/01/a1029/jo [14.04.2020].

It may seem too soon to begin negotiations with the EU with regard to the proposed EU e-evidence regulation (EU COM/2018/225 final); however, the US and the EU have already jointly announced that negotiations[79] are underway on the matter. Negotiating with the EU now is important for nations that, like Canada, have arrangements with providers headquartered in the EU.[80]

The agreements offer the opportunity to discuss the challenges and construct an agreement in line with each other's newly enacted laws and best interests.

E. Advise Departments of the Challenge

Considering that various departments are already storing their information in non-sovereign cloud facilities, it is important to advise and educate all departments on the challenges placed on the nation by their actions and the legal and political complications that may arise if a State's data, of both non-national interest and national interest, were to be accessible by another nation or breached.

Consider encouraging departments currently using non-sovereign cloud capacities to migrate their information to sovereign cloud capacities within a reasonable timeline.

F. Mandate International Interaction

Put in place a mandate to interact with other nations to better understand and be aware of their legal positions and changes to them. This action may involve various departments[81] to manage the discussions, digest the effect of international positions and disseminate the information to the rest of the government.

G. Cultivate Sovereign CSPs

Like Germany's GAIA-X project, States should consider creating a national programme to foster and promote nationally headquartered companies to invest in creating and offering CSP services within their country. These services could be coupled with cross-departmental agreement to host government-used services from within a government-owned and -operated data centre, thereby supporting national and non-national interests.

79 US Department of Justice, *Joint US-EU Statement on Electronic Evidence Sharing Negotiations*, 26 September 2019, https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations [14.04.2020].

80 The Shared Services Canada (SSC) department has arrangements with 8 providers; one of them, OVH, is headquartered in France while 6 others are headquartered in the US. See SSC's website to help understand its GC cloud broker responsibility, Shared Services Canada, *Cloud services*, 13 August 2019, https://www.canada.ca/en/shared-services/corporate/cloud-services.html [14.04.2020].

81 Likely examples for Canada: Global Affairs, Justice, Privy Council Office, and/or Treasury Board.

6. INSTEAD OF A CONCLUSION

This article has presented recommendations for States to consider the management of their sovereign data. The enactment of these recommendations could help governments to formulate a comprehensive data sovereignty strategy which balances the need to protect and retain control over sensitive data while at the same time being open to international cooperation in addressing the legitimate needs of law enforcement. The alternative – strict data localisation laws as seen in Russia[82] – might lead to the increasing fragmentation of cyberspace and endanger the goal of promoting an open, secure, stable, accessible and peaceful ICT environment, which the international community endorses.[83] We will see over the coming months and years how and whether more States choose to address the matter of data sovereignty and what their conclusions will be.

82 Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (with Amendments and Additions, official translation available at: https://pd.rkn.gov.ru/authority/p146/p191/ [14.04.2020].

83 See UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, para. 24.