Federated learning as a solution for problems related to intergovernmental data sharing

Sprenkamp, Kilian ; Delgado Fernandez, Joaquin ; Eckhardt, Sven ; Zavolokina, Liudmila

Federated Learning as a Solution for Problems Related to Intergovernmental Data Sharing

Kilian Sprenkamp
University of Zurich
kilian.sprenkamp@uzh.ch

Joaquín Delgado Fernández
University of Luxembourg
joaquin.delgadofernandez@uni.lu

Sven Eckhardt
University of Zurich
eckhardt@ifi.uzh.ch

Liudmila Zavolokina
University of Zurich
zavolokina@ifi.uzh.ch

Abstract

To address global problems, intergovernmental collaboration is needed. Modern solutions to these problems often include data-driven methods like artificial intelligence (AI), which require large amounts of data to perform well. However, data sharing between governments is limited. A possible solution is federated learning (FL), a decentralised AI method created to utilise personal information on edge devices. Instead of sharing data, governments can build their own models and just share the model parameters with a centralised server aggregating all parameters, resulting in a superior overall model. By conducting a structured literature review, we show how major intergovernmental data sharing challenges like disincentives, legal and ethical issues as well as technical constraints can be solved through FL. Enhanced AI while maintaining privacy through FL thus allows governments to collaboratively address global problems, which will positively impact governments and citizens.

Keywords: federated learning, artificial intelligence, eGovernment, data sharing challenges

1. Introduction

Even though there are approaches to allying with other countries, objectively, sovereign nation-states exercise power over a population of citizens within their territorial borders. With the increasing impact of digital technology and the rise of the internet as a "borderless space", the role of traditional borders in the digital realm is questioned more and more often. Although the very essence of the internet is to connect users and devices beyond borders, countries attempt to preserve their sovereignty by subjecting cyberspace to their own national rules.

An area where sovereignty is widely pursued among different countries is data sharing. While sharing data allows enhanced analytics and value generation, the 2022 World Economic Forum underlined the problem that data sharing is impractical as data is stored in different legacy system silos (Antonio, 2022). Further, legitimate reasons making data sharing complicated are disincentives due to the collective action theory (Olson, 1965) and data sharing being unethical (Ward & Sipior, 2010), especially when personal information is involved. In addition, legal uncertainties exist when data is shared between nations created through legislation like the General Data Protection Regulation (2018).

Still, technological advances do not stop, and governments need to keep up with the waves of innovation for economic, social and political reasons. While industry 4.0 is a very common term for the technological advancement in industry, eGovernment 3.0 (eGOV3.0) is the term used to describe the ever-increasing use of disruptive information and communication technology (ICT), such as artificial intelligence (AI) in governments. The term eGovernment 1.0 describes the use of ICT for the realisation of public services (Lachana et al., 2018). In addition, eGovernment 2.0, focuses on the ICT-enabled participation of citizens, while eGOV3.0 uses more advanced and data-driven technologies to solve societal problems through collected data (Lachana et al., 2018).

In order to fulfil the aspiration of AI to solve societal problems vast amounts of data are needed (Duan et al., 2019), which can be acquired through intergovernmental data sharing. From a global perspective, this need for data immediately creates tension between governments' interests and incentives, i.e., one government might want to pursue open data sharing, and another might seek to maintain their data private. This tension is illustrated by the statement of Germany's former health minister regarding the World Health Organisation's (WHO's) potential to place sanctions on countries that do not share their data during disease outbreaks (Wheaton & Martuscelli, 2021). While such a pandemic treaty exists, it is only actively supported by 25 countries (WHO, 2021), making the creation of accurate AI models in regard to Epidemiology difficult. Therefore, the question arises of how to access data without sharing it in order to collaboratively solve global problems. It can be argued that we can still build AI methods on private data. However, to advance the newly created eGOV3.0, we need to ensure that AI models operate as well as possible, as the performance of these systems has a far-reaching influence on governments and directly on citizens' lives.

One recent approach that promises to solve these problems is federated learning (FL) (McMahan et al., 2017). The core idea of FL is that individual entities build their own AI models and share them at a centralised point. Another AI model is built that aggregates the individual models. At no point in time is the data of any individual entity shared. In general, FL shows that the *federated model* performs better than *individual models*, which are built solely on the data of a single entity. However, federated models generally perform worse than the *oracle model*, a model built with all available data stored in a single silo. Nonetheless, it is often impractical to build an oracle model due to the limitations of data sharing (Jordan & Mitchell, 2015), leaving open the question of which technological approach would be the most fitting.

In our paper, we propose to use FL to enable better intergovernmental collaborations. We, therefore, investigate the research gap regarding how FL can be used for international eGOV3.0 in use cases where data cannot be shared. The following research question (RQ) is formulated:

RQ *How can federated learning address the problem of data sharing in intergovernmental collaboration?*

To answer this RQ, we investigate how challenges in data sharing listed by the Organisation for Economic Co-operation and Development (OECD) in OECD (2019) can be mitigated through FL. We choose the challenges named by OECD (2019) as a scientific framework listing intergovernmental data sharing challenges in the context of AI does not exist to our knowledge. We analyse these challenges through a structured literature review, aiming to propose FL as a solution to the challenges of intergovernmental data sharing.

The paper is structured as follows. In the subsequent chapter, we present related work and the background to the study. In Chapter 3, we explain our methodology. We present our results in Chapter 4. In Chapter 5, we discuss the implications of our results. We then conclude the study with an outlook in Chapter 6.

2. Related Work and Background

2.1. Intergovernmental Data Sharing

Data sharing is an ever-increasing factor for intergovernmental collaboration and success (Wiseman, 2020). Examples of successfully created AI applications trained on intergovernmental data include health, mobility and the social sector (Wiseman, 2020). Yet, there are legitimate national, public and private interests (OECD, 2019), making data sharing between administrations disincentive, unethical, legally uncertain or impractical due to technology constraints. We focus specifically on these four issues as they are well researched within the scientific literature. Thus, OECD (2019) functions as an extension focusing on practical intergovernmental challenges.

First, for intergovernmental collaboration, it is of great importance to take into account governments' counterincentives to share data, as sharing data might conflict with other policy goals (OECD, 2019). This can be due to information asymmetry that arises between information-poor and information-rich countries and can result in negative consequences for each type of country (Clarkson et al., 2007). Information-poor countries are often in a weaker position to negotiate data sharing agreements (Clarkson et al., 2007) and are thus inclined to make less advantageous concessions. In contrast, information-rich countries might have a counterincetive to share their data as they want to maintain their strong economic position. This reluctance to share data emerges from what is known as the "free rider" problem, where data is a non-exclusive public good and information-rich countries have to accept the risk of information-poor countries utilising their good free of charge (OECD, 2019). Due to "free riding" on the goods provided between organisation the allocation of public goods becomes ineffective, which is known as the collective action theory (Olson, 1965). Collective action thus results in difficulties for inter-organisational cooperation. While Olson (1965) focuses on inter organisational cooperation the theory has been expanded to problems regarding intergovernmental cooperation, e.g., Aspinwall and Greenwood (2013) for cooperation within the European Union (EU) allowing "free riding" of public goods provided by sovereign nation-states.

Second, some data has special privacy rights, such as personal information. Sharing this data can create ethical concerns. Data breaches from the private sector, like Facebook or Meta (Isaak & Hanna, 2018), and the public sector, like the disclosure of the records of 191 million voters in the United States (Bennett, 2016), decreases user trust, and data subjects are less likely to share data again (Pingitore et al., 2017). Therefore, countries need to ensure transparency, disclosure, control and notification in case of the maltreatment of citizens' data (Isaak & Hanna, 2018).

Third, the fear of legal consequences in a fragmented regulatory landscape limits the ability of data sharing. This is amplified by legal uncertainties over who controls the data and under which legislation and jurisdiction it falls (Ward & Sipior, 2010). Especially complicated is the distribution of data among multiple administrations with conflicting bilateral agreements. An example could be the cross-border transfer of data between EU countries, Japan and the United States, which is not currently possible. Right now, the EU only recognises nine non-EU countries as providing adequate protection for saving data. Japan is among them, but the United States is not (General Data Protection Regulation, 2018). Moreover, the EU can issue fines to any organisation not complying with General Data Protection Regulation (2018), creating a further monetary disincentive to share data based on EU law binding to nations inside and outside the EU.

Last, while data should be distributed in according to the FAIR (findability, accessibility, interoperability, reusability) principle (Wilkinson et al., 2016) several technological challenges and threats for governments can occur in data sharing. While in the age of cloud computing the cost of storing, copying and analysing data has shrunk, open data provision still involves significant costs for collecting, preparing, sharing, scaling, maintaining and updating data (C. P. Chen & Zhang, 2014; Johnson, 2016). Another challenge is the varying quality of data due to inconsistency and incompleteness and the resulting need for standardisation when data is stored in multiple locations (C. P. Chen & Zhang, 2014; Mikhaylov et al., 2018). Data sharing further creates multiple entry points into a system, decreasing data security (C. P. Chen & Zhang, 2014; D. Chen & Zhao, 2012).

These challenges, arising from national, public and private interests, are especially relevant as they hinder the sharing of data and thus the creation of AI trained on data recorded in multiple countries. This, in turn, impacts the advance of eGOV3.0 and the realisation of its benefits to society as a whole.

2.2. Federated Learning

A possible solution to the challenges of data sharing for the creation of AI models was proposed by McMahan et al. (2017), who, while leveraging data utility, maintained a clear separation between data owners. This solution, namely FL, relies on the distribution of models across different databases instead of the classical machine learning (ML) example, where all the data is stored in a single silo. By distributing the models, the authors separated the model and the data, keeping the latter isolated and at the data owners' selected location without revealing it. Since then, applications in health (Xu et al., 2021), banking (Q. Yang et al., 2019) or smart cities (Jiang et al., 2020) have been subject to research. FL thus provides incentives in terms of privacy, security, legal and economic benefits for users (Q. Yang et al., 2019). To the extent of our knowledge, one framework on how to apply FL in eGOV3.0 use cases (Guberović et al., 2022) has been created, which includes the specification of client, server, model and application programming interface requirements at the start of a project. Further, the accountability of FL in government to overcome legislative constraints has been researched, pointing out engineering requirements, i.e., architecture design and management requirements, i.e., trust among actors (Balta et al., 2021).

Originally, McMahan et al. (2017) proposed FL while working at Google, utilising decentralised data stored on multiple edge devices for tasks like image or voice recognition. Now, the original technique is also termed "horizontal FL" as the data of each client shares the same feature space. We visualise FL incorporated into eGOV3.0 in cross-silo (Wiseman, 2020) use cases (see Figure 1). The term cross-silo refers to different data storages on a national or sub national level, which due to the challenges of intergovernmental data sharing, explained in Section 2.1 cannot be exchanged between nations.

The algorithm is initialised with a base model sent to all clients (i.e., nation-states) by the server (i.e., an intergovernmental organisation or intergovernmental collaboration project). This step is not part of the repeatedly performed steps and is therefore named step 0. In step 1, each client starts the training process from the base model using their own data. In step 2, the difference between the base model parameters and the client model parameters is sent to the server, but each client's data is not shared. While sharing model weights is also a form of information sharing, security techniques like *secure aggregation* and *differential privacy* keep data secure and private. The communication channel between client and server is ciphered via *secure aggregation* (Bonawitz et al., 2017) and thus made secure. *Secure aggegration* thus allows for the transfer of model parameters between parties which do not trust each other, other clients or the server are not capable of obtaining the model weights other clients send through the federated system. During step

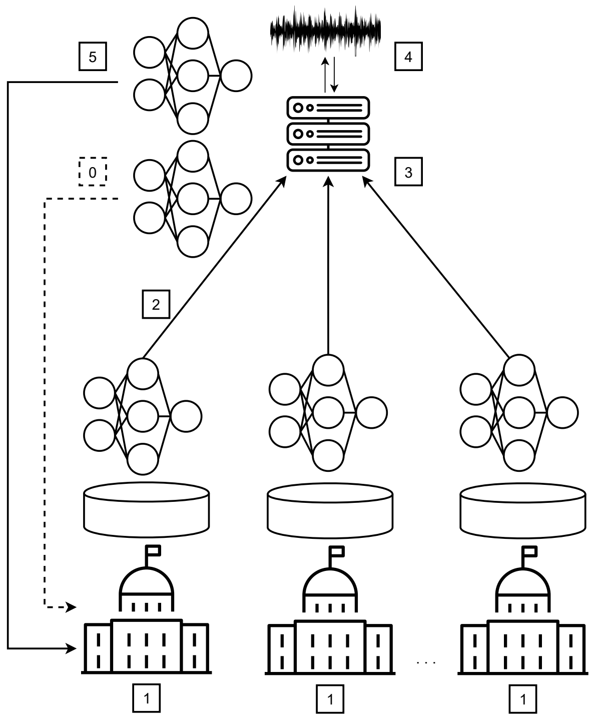

Figure 1. Federated Learning in eGOV3.0

3, the server utilises *federated averaging* to calculate a weighted mean of all differences. The weight of each client is determined by the amount of data used to train the model. Then, in step 4, the server adds random noise to the aggregated model. By adding random noise, privacy is ensured, meaning that the prior steps cannot be reverse-engineered. This procedure is known as *differential privacy* (Agarwal et al., 2018) and is also used in standard ML algorithms. Differentially private models are defined by the tuple (ϵ,δ), where ϵ defines the impact of each individual piece of information on the results of the analysis. In other words, low ϵ indicates a robust system where the outcome is not represented by any particular client data. Additionally, δ regulates the likelihood of a data breach occurring. Step 4 is optional, but if chosen, the model becomes a secure federated model, allowing governments to keep their data private. Finally, in step 5, the private aggregated model is sent to the clients. Steps 1 to 5 represent one round of federated training, which is repeated until the federated model converges.

For the paper we focus how FL can solve problems related to external intergovernmental data sharing meaning collaboration happening between multiple sovereign nation-states. However, partly we consider that individuals, as well as companies, give their data to the respective nation-state they are located in, e.g., multiple states creating a model for the prediction of the effect of climate change based on CO_2 data collected from companies or households.

While FL has been proposed by McMahan et al. (2017) to solve the problem of data sharing on edge devices, there have been limited attempts to adapt this technique to the public sector. It is especially unclear how the specific challenges of data sharing among governments can be solved.

3. Method

We conducted a structured literature review to investigate how FL can solve data sharing problems identified by OECD (2019). We utilised the challenges provided by the OECD as a single scientific framework for intergovernmental data sharing does not exist to our knowledge. However, the OECD study results from workshops attended by data professionals and policy leaders from various countries and industries, ensuring a diverse and holistic view. The challenges of data sharing identified by OECD (2019) are grouped into three categories and various subcategories (see table 1) and formulated with regards to the growing importance of AI. During the literature search process, we focused on information systems and computer science literature, and we applied forward as well as backward searches (Webster & Watson, 2002). We utilised the search string `{"Federated Learning" AND "Data" AND "Challenge*"}` in the disciplines of Information Systems, Computer, Decision, Manangement and Social Science, yielding a total of 879 results. We searched through the scopus, IEEE, ACM and the AIS library database. As pre-selection criteria, we analysed if the given article discusses the challenges named by OECD (2019) based on the abstract, 43 articles were thus chosen for further analysis. We mapped 14 articles to the challenges of the OECD (2019), a forward and backward found further 7 articles resulting in 21 articles selected.

4. Results

We identified solutions to the sub-challenges (OECD, 2019) by conducting a structured literature review. We found solutions for eight of the 12 sub-challenges defined, while two of the sub-challenges were partially solved and two of the sub-challenges remained unsolved (see Table 1).

[1] Balancing the benefits of data openness with legitimate interests, policy objectives and risks.

With FL, the security and confidentiality breaches in data sharing [1.1] can be avoided, as FL alleviates the need to share data. FL does so through the range of

Table 1. FL solutions to data sharing challenges (OECD, 2019)

Challenge	Sub Challenge	Solved by FL	Proposed Solution
[1] Balancing the benefits of data openness with legitimate interests, policy objectives and risks	[1.1] Security risks and confidentiality breaches	solved	• Security and privacy techniques (Agarwal et al., 2018; Bonawitz et al., 2017; Mothukuri et al., 2021) • Hierarchical federated learning (Abad et al., 2020)
	[1.2] Violation of privacy and intellectual property	solved	• Workaround for contractual agreements (L. Li et al., 2020; Q. Li et al., 2021)
	[1.3] Difficulty of risk management approaches	not solved	• N/A
	[1.4] Cross-border data access and sharing	solved	• Unnecessity of cross-border data sharing (Truong et al., 2021; D. Yang et al., 2021; Q. Yang et al., 2019)
[2] Trust and empowerment for the effective re-use of data across society	[2.1] Supporting and engaging communities	not solved	• N/A
	[2.2] Fostering data-related infrastructures and skill	partially solved	• Communication cost (T. Li et al., 2020; McMahan et al., 2017) • FL toolkits (Ziller et al., 2021)
	[2.3] Lack of common standards for data sharing and re-use	solved	• System heterogeneity (Mitra et al., 2021) • Vertical federated learning (Q. Yang et al., 2019) • Federated transfer Learning (Y. Chen et al., 2020)
	[2.4] Data quality	solved	• FL on noisy data (Passerat-Palmbach et al., 2020; Tuor et al., 2021)
[3] Misaligned incentives, and limitations of current business models and markets	[3.1] Externalities of data sharing, re-use and misaligned incentives	solved	• Incentives of FL (Kang et al., 2019; Yu et al., 2020)
	[3.2] Limitations of current business models and data markets	solved	• FL as a business model (Balta et al., 2021; Manoj et al., 2022; Q. Yang et al., 2019)
	[3.3] The risks of mandatory access to data	partially solved	• Evaluation of samples (Ziller et al., 2021)
	[3.4] Uncertainties about data ownership	solved	• Data ownership is explicit (Y. Liu et al., 2020; Shae & Tsai, 2018) • Model ownership is explicit on technical level (X. Liu et al., 2021)

security and privacy techniques (Mothukuri et al., 2021). We like to point out two core approaches *differential privacy* (Agarwal et al., 2018) and *secure aggregation* (Bonawitz et al., 2017). While *differential privacy* secures the system from being reverse-engineered, *secure aggregation* secures the system by ciphering the communication channel between the clients and the server. Moreover, concerning the importance of personal information, hierarchical FL settings (Abad et al., 2020) enable FL to be applied on multiple levels. A country could thus give citizens or companies control over their data while still profiting from AI being trained by international projects.

The violation of privacy and property rights [1.2] is, according to OECD (2019), based on contractual agreements. The violation of these agreements can lead to fines. Moreover, sharing data prematurely can reduce the chance of creating intellectual property. FL offers a technological pathway for entities to comply with these contractual agreements (L. Li et al., 2020; Q. Li et al., 2021), thus preventing them from violating contractual clauses and being exposed to ensuing fines or the premature revelation of intellectual property.

Regarding mitigating the difficulty of applying risk management approaches [1.3], we currently see limited potential in FL to solve this challenge.

From a legal perspective, cross-border data sharing [1.4] can be complicated due to regulations like the General Data Protection Regulation (2018). FL allows the training of AI without the need to share data across borders. Q. Yang et al. (2019) proposed the training of federated models between Chinese and American companies. Similarly, D. Yang et al. (2021) presented an FL system using data from China, Japan and Italy to predict SARS-CoV-2 from chest computed tomography images. However, Truong et al. (2021) point out that due to to the exchange of model weights and the resulting threat of backward engineering, FL, without any security and privacy techniques is not conform with General Data Protection Regulation (2018) in Europe. Therefore, FL can only be utilised with privacy and security preserving techniques when utilising data from multiple countries.

[2] Trust and empowerment for the effective re-use of data across society

FL cannot help to create more engagement in open data communities [2.1] as it reduces the need to share data. However, we can see that the shared model training creates a community aspect. To our knowledge, this has not yet been researched.

We found that FL cannot solve problems related to data infrastructure or skills [2.2]. Generally, the technique requires a more complicated setup (T. Li et al., 2020). FL profits from dividing the computational cost across multiple clients. Yet, the cost of communication is high in FL, as clients need to communicate continuously. This cost is practically non-existent in normal ML (McMahan et al., 2017). The reduction of costs associated with FL is currently under research, and several solutions have been proposed (T. Li et al., 2020). Further, due to the increased complexity and novelty of FL, tool kits like `TensorFlow Federated` based on McMahan et al. (2017) and `PySyft` (Ziller et al., 2021) have not seen wide adoption compared to other ML frameworks. Nonetheless, we see possibilities for less skilled countries to profit as they prefer to use federated models rather than training models themselves.

The lack of data standardisation [2.3] reflects two core challenges of FL: system and statistical heterogeneity. Solutions to this issue exist already. System heterogeneity is described as different hardware being used among clients, leading to a slower training process. For example, Mitra et al. (2021) propose re-using parts of the model during the training process, such as gradients of the learned network or the specification of concrete learning rates for individual clients depending on the hardware. Statistical heterogeneity refers to different data features being stored or features having non-identical distributions across clients. In this case, vertical FL (Q. Yang et al., 2019) can be used, which allows for the training of models with different feature spaces. Moreover, it is possible to apply transfer FL, meaning that a model is retrained for a different learning task, benefiting from the knowledge of the previously learned task. Y. Chen et al. (2020) employ this technique by first training a model for activity recognition for smartwatches, which is then transferred to the task of predicting Parkinson's disease.

The OECD notes that poor data quality [2.4] will lead to poor analytics. While FL cannot improve the data quality of clients, entities with poor data quality can profit from the federated model. Examples can be found within the medical field of genomics or mental health, where large amounts of noisy data can be found (Passerat-Palmbach et al., 2020). In this case clients with poor data can profit from the federated model and the contribution made by other clients with better quality data. Still, the clients with poor data quality will decrease the overall model quality. A solution to this challenge is proposed by Tuor et al. (2021), each client evaluates their data set with a benchmark model trained on high quality data. For bad quality data the model will be incapable of making a prediction, generating a high loss value. These data points will not be further utilised for training.

[3] Misaligned incentives, and limitations of current business models and markets

A central problem within data sharing is misaligned incentives [3.1] between information-rich and information-poor countries. The problem of incentivising information-rich clients to participate in FL has been well researched (Kang et al., 2019; Yu et al., 2020). These methods typically offer a reward for participating within the federated system. Hence, an entity could earn depending on how much value was brought to the federated model.

Implementing FL could significantly reduce the need for data markets [3.2], as data can be kept by the owner. Moreover, according to the OECD, the ex-ante evaluation of the economic potential of data is challenging. However, given the previously shown incentive schemes of FL, it is possible to track participation in an FL project. Q. Yang et al. (2019) estimate that FL will evolve into a business model where participants in an FL project can profit from the value they contribute to the model. FL thus allows participants to pursue joint business activities (Balta et al., 2021). An example of such a joint business activity is given by Manoj et al. (2022) training a model for predicting the yield of crop. This model can be utilised by multiple stakeholders, e.g., farmers for revenue estimates, banks and insurances for mitigating risks and governments for setting export prices.

In a federated setting, mandatory data access [3.3] can be kept to a minimum. For example, the `PySyft` package (Ziller et al., 2021) within `Python` allows for viewing a limited number of samples of each client's data to optimise the federated model. Accessing all available data points is, in theory, not necessary and, due to the number of data points available, not always feasible while training AI models.

Finally, the OECD notes a loss of data ownership [3.4] as an emerging challenge of sharing data. With FL, the ownership of a data point remains unaffected as it is not shared across multiple sources. For example, Shae and Tsai (2018) propose storing medical information on a blockchain for training federated models. Thus, the ownership of data cannot be falsified. In a similar manner, Y. Liu et al. (2020) proposed a traffic flow prediction model utilising data from government organisations, smart devices, private persons as well as private companies like Uber or Didi. For each of these entities, the data ownership is unambiguous. Moreover, it is possible to verify the ownership over a trained federated model by implementing a watermarking technique, thus, the contribution and resulting ownership of clients is recorded through the watermark (X. Liu et al., 2021). However, the watermarking technique solely clarifies ownership on a technical and not legal level. To our knowledge the legal ownership of federated models remains unsolved.

5. Discussion

This study aimed to address the research gap regarding how FL can be used in international eGOV3.0 use cases where data sharing is complicated or unfeasible. Previous research has shown that data sharing is limited due to being disincentive (Olson, 1965), unethical (Isaak & Hanna, 2018; Pingitore et al., 2017), legally uncertain (Ward & Sipior, 2010) or impractical due to technical challenges (C. P. Chen & Zhang, 2014; D. Chen & Zhao, 2012; Johnson, 2016; Mikhaylov et al., 2018). Since McMahan et al. (2017) first proposed FL, a vast number of publications have appeared in the field, including applications in health, banking and smart cities. However, research in the area of eGOV3.0 is limited. While Guberović et al. (2022) created a framework specifying component requirements for government FL projects and Balta et al. (2021) analysed the accountability of FL in government, we analysed how FL can solve the problem of intergovernmental data sharing. We did so by conducting a structured literature review, which served the purpose of analysing how FL can solve challenges identified by OECD (2019). In doing so, we were able to answer the given RQ: *How can federated learning address the problem of data sharing in intergovernmental collaboration?*

First, FL can help to deal with legal (Ward & Sipior, 2010) and ethical (Isaak & Hanna, 2018; Pingitore et al., 2017) issues around data sharing. We provided evidence regarding how the sub-challenges [1.1], [1.2], [1.4] and [3.4] identified by the OECD can be solved. FL significantly reduces the need for data sharing agreements to build AI (L. Li et al., 2020; Q. Li et al., 2021), which also applies to cross-border data sharing (Truong et al., 2021; D. Yang et al., 2021; Q. Yang et al., 2019). A further consequence is that data ownership cannot be falsified, as the data is stored at the owners' selected location. Moreover, FL, mainly through *differential privacy* (Agarwal et al., 2018) and *secure aggregation* (Bonawitz et al., 2017), allows for secure model training and keeping data private. FL, thus provides a trusted technology that is ideal for intergovernmental use cases.

Second, we showed how technological constraints in data sharing (C. P. Chen & Zhang, 2014; D. Chen & Zhao, 2012; Johnson, 2016; Mikhaylov et al., 2018) can be overcome using FL, especially issues regarding the sub-challenges of standardisation of data [2.3] and data quality [2.4]. Mitra et al. (2021) show methods that allow federated models to be trained in system heterogeneous settings. This is beneficial for FL in intergovernmental settings as countries, companies and citizens can partake in FL projects without the need for special hardware. Vertical FL (Q. Yang et al., 2019) and transfer FL (Y. Chen et al., 2020) allow the training of AI models on non-standardised data sets, and they can even leverage data that was not recorded for the task they have been employed to solve. Intergovernmental collaboration can thus profit from data stored by all types of entities and further re-use data effectively. Additionally, data from both information-poor and information-rich countries can be utilised to contribute to FL projects. Information-poor countries are not limited to their own data sources anymore and can contribute and profit from the federated model. Still, while federated learning shows potential and has been implemented on a scientific basis till now applications of FL in an intergovernmental context in real-world scenarios are not known to us. This could be the case due to technological challenges solely being solved in the literature but not in real-world scenarios.

Last, FL can evolve into a business model (Balta et al., 2021; Q. Yang et al., 2019), which gives entities an incentive to take part in intergovernmental projects. This mitigates disincentives in data sharing caused by "free riding" and the problem of inefficiency due to collective action (Olson, 1965). Consequently, we demonstrated how sub-challenges [3.1] and [3.2] could be solved through FL. With incentive mechanisms developed for FL (Kang et al., 2019; Yu et al., 2020), both information-rich and information-poor entities can be motivated to participate in an FL project by offering a reward. For example, an intergovernmental climate model could be possible where different stakeholders, e.g. countries, companies or single individuals could earn money or CO_2 credits based on the revenue or value that an intergovernmental FL project generates. Still, large contributors would earn the most, but also, less funded entities can profit fairly. We consider the incentives to partake in FL to be superior to the incentives for partaking in data sharing. When using FL, the ownership of the data [3.4] remains intact for each FL project an entity might participate in. In contrast, for standard data sharing, as soon as data is distributed, it becomes unclear who the real owner is. Therefore, "free riding" as described in the collective action theory (Olson, 1965) and the resulting inefficiency can be mitigated on a technical level in theory.

However, not all problems related to data sharing can be solved through FL. Sub-challenges [2.2] and [3.3] are only partially solved, while sub-challenges [1.3] and [2.1] are not solved. There are two key problems. First, implementing FL infrastructure is more complicated, with higher communication costs. Even with a larger adoption, this will cause challenges in eGOV3.0. Second, although ownership of FL is actively researched from a technological point of view (X. Liu et al., 2021), we see problems on the organisational level, in which the geolocation and the controlling entity of the server aggregating the model will play a central role. The entity controlling the federated model could cut off countries in an intergovernmental collaboration project without a democratic process. Especially from a political realism perspective, it is unlikely that nations which do not trust each other will participate in a joint FL project. Future research could consider governments' willingness to participate in projects that benefit various multinational stakeholders. Within this analysis, the difference between incentives of information-rich and information-poor countries is likely to play a key role.

6. Conclusion

This study conducts a structured literature review to show how FL can function as a solution to various challenges related to intergovernmental data sharing. FL enables the training of models in a decentralised manner and can thus reduce incentive, legal, ethical and practical challenges in intergovernmental data sharing. Nevertheless, secondary problems of a technical and organisational nature arise.

The contribution of this study is threefold. First, we present a state-of-the-art AI method to overcome the problem of intergovernmental data sharing. This serves as a basis for FL research in international eGOV3.0, which we hope will influence both governments and citizens. Second, we contribute to the existing literature on FL, providing a structured review on how FL should be utilised in eGOV3.0, focusing on the aspect of data sharing. We hope this will enhance the research output of real-life use cases in and outside the eGOV3.0 space. Third, we show a new possibility of how to mitigate inefficiency created by the collective action theory (Olson, 1965).

Moreover, our study has the limitation of solely focusing on the challenges of data sharing provided by the OECD (2019). We estimate that challenges described by other authorities will be similar, but adding challenges from authorities of different cultural or economic origins would create an even more holistic and diverse picture.

Considering the opportunities and challenges highlighted in this study, we find substantial potential for the information systems and related research communities. We suggest creating federated systems on proprietary, potentially unbalanced data from multi-governmental stakeholders. Dedicated qualitative research could be done, drawing insights from workshops or stakeholder interviews to further investigate the potential of FL in eGOV3.0. Moreover, at the organisational level, it is necessary to determine the owner of the server that creates the aggregated model. Finally, the higher infrastructure costs and skill levels of users in FL need to be considered in further research.

Acknowledgement

We thank the University of Zurich and the Digital Society Initiative for (partially) financing this study under the DIZH postdoc fellowship of Liudmila Zavolokina. Further, this work has been supported by the European Union (EU) within its Horizon 2020 programme, project MDOT (Medical Device Obligations Taskforce), Grant agreement 814654 and from PayPal and the Luxembourg National Research Fund FNR (P17/IS/13342933/PayPal-FNR/Chair in DFS/Gilbert Fridgen). Last, we would like to thank Linda Weigl for her insightful comments on the work.

References

Abad, M. S. H., Ozfatura, E., Gunduz, D., & Ercetin, O. (2020). Hierarchical federated learning across heterogeneous cellular networks. *ICASSP*.

Agarwal, N., Suresh, A. T., Yu, F. X. X., Kumar, S., & McMahan, B. (2018). Cpsgd: Communication-efficient and differentially-private distributed sgd. *Advances in Neural Information Processing Systems*.

Antonio, N. (2022). The public sector must accelerate digital transformation – or risk losing sovereignty and trust. Retrieved May 23, 2022, from https : / / www . weforum . org / agenda / 2022 / 05 / the - public - sector - must - accelerate - digital - transformation - or - risk - losing-sovereignty-and-trust/

Aspinwall, M., & Greenwood, J. (2013). *Collective action in the european union: Interests and the new politics of associability*. Routledge.

Balta, D., Sellami, M., Kuhn, P., Schöpp, U., Buchinger, M., Baracaldo, N., Anwar, A., Ludwig, H., Sinn, M., Purcell, M., et al. (2021). Accountable federated machine learning in government: Engineering and management insights. *International Conference on Electronic Participation*.

Bennett, C. J. (2016). Voter databases, micro-targeting, and data protection law: Can political parties campaign in europe as they do in north america? *International Data Privacy Law*.

Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., Ramage, D., Segal, A., & Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. *ACM Conference on Computer & Communications Security*.

Chen, C. P., & Zhang, C.-Y. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on big data. *Information sciences*.

Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. *2012 International Conference on Computer Science and Electronics Engineering*.

Chen, Y., Qin, X., Wang, J., Yu, C., & Gao, W. (2020). Fedhealth: A federated transfer learning framework for wearable healthcare. *IEEE Intelligent Systems*.

Clarkson, G., Jacobsen, T. E., & Batcheller, A. L. (2007). Information asymmetry and information sharing. *Government Information Quarterly*.

Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019). Artificial intelligence for decision making in the era of big data–evolution, challenges and research agenda. *International Journal of Information Management*.

General Data Protection Regulation. (2018, May 25). *European Commission*. https://gdpr.eu/

Guberović, E., Alexopoulos, C., Bosnić, I., & Čavrak, I. (2022). Framework for federated learning open models in e-government applications. *Interdisciplinary Description of Complex Systems*.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, cambridge analytica, and privacy protection. *Computer*.

Jiang, J. C., Kantarci, B., Oktug, S., & Soyata, T. (2020). Federated learning in smart city sensing: Challenges and opportunities. *Sensors*.

Johnson, P. A. (2016). Reflecting on the success of open data: How municipal government evaluates their open data programs. *International Journal of E-Planning Research*.

Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*.

Kang, J., Xiong, Z., Niyato, D., Xie, S., & Zhang, J. (2019). Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. *IEEE Internet of Things Journal*.

Lachana, Z., Alexopoulos, C., Loukis, E., & Charalabidis, Y. (2018). Identifying the different generations of egovernment: An analysis framework. *The 12th Mediterranean Conference on Information Systems*.

Li, L., Fan, Y., Tse, M., & Lin, K.-Y. (2020). A review of applications in federated learning. *Computers & Industrial Engineering*.

Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., Liu, X., & He, B. (2021). A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*.

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine*.

Liu, X., Shao, S., Yang, Y., Wu, K., Yang, W., & Fang, H. (2021). Secure federated learning model verification: A client-side backdoor triggered watermarking scheme. *IEEE International Conference on Systems, Man, and Cybernetics*.

Liu, Y., James, J., Kang, J., Niyato, D., & Zhang, S. (2020). Privacy-preserving traffic flow prediction: A federated learning approach. *IEEE Internet of Things Journal*.

Manoj, T., Makkithaya, K., & Narendra, V. (2022). A federated learning-based crop yield prediction for agricultural production risk management. *2022 IEEE Delhi Section Conference*.

McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. *Artificial intelligence and statistics*.

Mikhaylov, S. J., Esteve, M., & Campion, A. (2018). Artificial intelligence for the public sector: Opportunities and challenges of cross-sector collaboration. *Philosophical transactions of the royal society a: mathematical, physical and engineering sciences*.

Mitra, A., Jaafar, R., Pappas, G. J., & Hassani, H. (2021). Linear convergence in federated learning: Tackling client heterogeneity and sparse gradients. *Advances in Neural Information Processing Systems*.

Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. *Future Generation Computer Systems*.

OECD. (2019). Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies.

Olson, M. (1965). The logic of collective action harvard university press. *Cambridge, MA*.

Passerat-Palmbach, J., Farnan, T., McCoy, M., Harris, J. D., Manion, S. T., Flannery, H. L., & Gleim, B. (2020). Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. *2020 IEEE International Conference on Blockchain*.

Pingitore, G., Rao, V., Dwivedi, K., & Cavallaro, K. (2017). To share or not to share. https://www2.deloitte.com/content/dam/insights/us/articles/4020_To-share-or-not-to-share/DUP_To-share-or-not-to-share.pdf

Shae, Z., & Tsai, J. (2018). Transform blockchain into distributed parallel computing architecture for precision medicine. *International Conference on Distributed Computing Systems*.

Truong, N., Sun, K., Wang, S., Guitton, F., & Guo, Y. (2021). Privacy preservation in federated learning: An insightful survey from the gdpr perspective. *Computers & Security*.

Tuor, T., Wang, S., Ko, B. J., Liu, C., & Leung, K. K. (2021). Overcoming noisy and irrelevant data in federated learning. *International Conference on Pattern Recognition*.

Ward, B. T., & Sipior, J. C. (2010). The internet jurisdiction risk of cloud computing. *Information systems management*.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*.

Wheaton, S., & Martuscelli. (2021). Who, berlin float sanctions if countries suppress information on pandemics. Retrieved May 20, 2022, from https://www.politico.eu/article/who-berlin-float-sanctions-if-countries-suppress-information-on-pandemics/

WHO. (2021). *Global leaders unite in urgent call for international pandemic treaty*. Retrieved May 19, 2022, from https://www.who.int/news/item/30-03-2021-global-leaders-unite-in-urgent-call-for-international-pandemic-treaty

Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., da Silva Santos, L. B., Bourne, P. E., et al. (2016). The fair guiding principles for scientific data management and stewardship. *Scientific data*.

Wiseman, J. (2020). Silo busting: The challenges and success factors for sharing intergovernmental data. *IBM Center for The Business of Government. Accessed April*, *6*, 2021.

Xu, J., Glicksberg, B. S., Su, C., Walker, P., Bian, J., & Wang, F. (2021). Federated learning for healthcare informatics. *Journal of Healthcare Informatics Research*.

Yang, D., Xu, Z., Li, W., Myronenko, A., Roth, H. R., Harmon, S., Xu, S., Turkbey, B., Turkbey, E., Wang, X., et al. (2021). Federated semi-supervised learning for covid region segmentation in chest ct using multi-national data from china, italy, japan. *Medical image analysis*.

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*.

Yu, H., Liu, Z., Liu, Y., Chen, T., Cong, M., Weng, X., Niyato, D., & Yang, Q. (2020). A fairness-aware incentive scheme for federated learning. *Conference on AI, Ethics, and Society*.

Ziller, A., Trask, A., Lopardo, A., Szymkow, B., Wagner, B., Bluemke, E., Nounahon, J.-M., Passerat-Palmbach, J., Prakash, K., Rose, N., et al. (2021). Pysyft: A library for easy federated learning. *Federated learning systems*.