Design for Agency *vs.* Vulnerability by Design – The Case of Swiss Agriculture

Léa Stiefel, Alain Sandoz

A. Introduction

Should the sensitive data that is shared in an information infrastructure be centralized or distributed? The question appeared openly on the scene of Swiss agriculture in the years 2017-2019. Farmers were producing large volumes of heterogeneous sensitive data for a few hundred private and public organizations that independently collected and used it to provide services. Farmers were increasingly dissatisfied with a situation that was getting out of control. Would it not be better to put all the data in a central database and to delegate control to a unique actor, rather than to distribute control piecewise to organizations that managed subsets of data in many heterogeneous databases? The issue sparked debate and triggered the opposition of two projects, each attempting to establish the foundations of an information infrastructure for agriculture through one of two alternatives: centralization *vs.* distribution.

The question concerns information infrastructures (*II*s) in sectors of activity where digital systems play a significant role.[1] Data is involved in every *operation* executed by a digital system and the transmission of data is involved in every *inter-operation* between any pair of digital systems connected by a network. What if the data represents information *of interest* to a social actor, a person, or an organisation? In all generality, the two digital systems might be *controlled* by different actors, and the actor concerned by the data might be a *third* party. In this situation, information that is possibly sensitive about the third actor is shared by two other actors through their digital information systems. If sensitive information about many actors (possibly tens of thousands or millions) is shared by a small number of

1 Bowker *et al.,* 'Toward information infrastructure studies: ways of knowing in a networked environment' in *International Handbook of Internet Research* (Springer 2009), 97; Monteiro *et al.*, 'Innovation in Information Infrastructures: Introduction to the Special Issue' (2014) JAIS Vol 15; Poppe *et al.*, 'Architecting in Large and Complex Information Infrastructures' (2014) in SCIS, 90.

actors (possibly a few dozens or thousands, each operating a *database*), then questions emerge about who controls and who shares what data, how sensitive data is used and by whom, how it is transformed after having been shared, and how it is re-shared after having been transformed, etc.

The question is not just rhetorical. Digital healthcare, for example, is concerned with the design and implementation of Electronic Patient Records.[2] Standardisation of data in the systems where it originates and it is used have been proposed to stabilize complexity and costs, and improve the effectivity of information management in healthcare *II*s. It is difficult to achieve and faces challenges, *e.g.*, in relation to the usage of patient data by public and/or private healthcare actors.[3]

We examine this question in the *II* of agriculture in Switzerland from the perspective of digital vulnerability, accountability, and trust between actors: data-*owners* (*i.e.*, persons for whom the data is sensitive) and data-*users* (*i.e.*, actors who use and possibly share the data).

The project to centralize data was called Barto and started in 2015. By 2017 an alternative proposition to *manage* data distribution rather than centralize data had emerged and was called ADA. The two projects had radically opposed conceptions of data sharing: a centralized platform with third-party modules for smart-farming in Barto, and a peer-to-peer distributed platform for authorized data-transmission between database operators in ADA. Based on the materials collected during fieldwork in 2018 and 2019, and on subsequent research on software-based platforms, we explore how the vulnerability of farmers, the accountability of organizations, and the trust relationship between the two groups translate in each approach. This brings us to examine trust in relation to digital platforms. To do this, we use a model of organizational trust.[4]

This work is the result of a multidisciplinary collaboration. In January 2018, the first author, then a PhD student in STS (Science & Technology Studies), had just started her thesis and was interested in tracking the dynamics of digitization in Swiss agriculture. She had attended public presentations of both projects and had introduced herself to ADA's archi-

2 Hanseth & Bygstad 'Managing IT in Large Organizations as Platform-Oriented Infrastructures' (2021) <www.researchgate.net/profile/Ole-Hanseth/publication/354435940> accessed 5 June 2024.

3 www.researchgate.net/profile/Ole-Hanseth/publication/35443594

4 Mayer *et al.*, 'An integrative model of organizational trust: past, present, and future' (1995) AMR, Vol 20, 709.

tect (the second author), asking to (ethnographically) follow the project's development.

In September 2018, the terms of a collaboration were defined. In parallel to other enquiries in the sector, the ethnographer would go behind the scenes of ADA to follow and document all of its developments. In return for full access, she would provide the architect with feedback on her observations, according to the rules of her discipline and her progressive understanding of digitization, via anonymized reports of her interviews. The architect would benefit from this informed perspective to drive ADA in its socio-technical environment.

After ADA was put in production in 2019 and the project ended, the authors crossed the boundaries of their respective disciplines (STS and Computer science) to better understand the relationships between architecture and governance in digital platforms. By exploring dependencies, autonomy, symmetry and control, architecture and governance, we have acquired knowledge on digital platforms and produced several small theoretical contributions in STS. In this paper, we intend to explore the platforms ADA and Barto under the perspectives of digital vulnerability, accountability, and trust (noted *dVAT*), three social concepts that were implemented in different ways at the technical level in each solution.

At the end of the nineties, the government needed a system to implement new agricultural policies.[5] There was a political consensus among Swiss cantons and federal authorities on the urgency to build a *database* that would implement the requirements of new international trade treaties.[6] Weak resistance to change by cantonal administrations was more a stance than effective, sometimes justified by technical or organizational reasons. At that time, farmers sent paper forms to their local administrations who employed typists to transcribe the written declarations with digital computers. Controllers would visit farms bringing printouts with values to be checked on site. The Internet and mobile technologies were not yet available. With time, the situation evolved and got out of control. The topic of data sharing then became acute. Section B. describes the context where Barto and ADA emerged. Section C. makes a distinction between the [actor-interaction] and [system-interoperation] relationships that are

5 Sandoz, 'Meeting the Requirements of Agricultural Policy Management on Information Technology' (1999) *EFITA*.

6 <www.parlament.ch/blog/Pages/politique-fait-la-vie-dure-au-lait.aspx?lang=1040> accessed 23 March 2023.

fundamental to understanding digital dependencies, and incidentally of *VAT* in the digital context. Section D. describes methodology and the field materials. Section E. is devoted to the case studies. Subsection E.I. concerns Barto and how it was perceived. Subsection E.II. concerns ADA and describes chosen aspects of its design, how the platform functioned, and how it *intended* to counter what was perceived as a threat, including the loss of accountability perceived by public organizations. Its architecture is more detailed than subsection E.I.. What we know of Barto's design (the project declined an interview by the ethnographer) is classical and documented in the literature generally under the term of *software-based platform*.[7] Section F. discusses how digital vulnerability, trust, and accountability translated in both projects and is followed by a conclusion.

B. Context

In Switzerland, *ca*. 48'000 farms[8] (*i.e.,* - 40% less than in 1996[9]) supply food and services such as landscape and biodiversity preservation. Farms interact with other farms, suppliers, buyers, controllers, regulators, professional or label organizations, research, schools, and extension services, IT and other service providers, and cooperatives. Public administrations supervise the implementation of regulation. Some private organizations execute specific regulatory tasks under public supervision (*e.g*., the operation of the national animal control database, BDTA, by *Identitas* – see below). All these actors use digital systems. Farmers supply information about their farm to service providers and other organizations. Information concerning *e.g*., prices, revenues, livestock health, or crop productivity can be sensitive for the farmer and is provided under contract or license agreement. In return receivers of the information provide subsidies, premiums, or other services based on the data they process. Each organization digitizes the information it gets and records it in a database that it operates. Data management comes at a cost for organisations, so the data they collect is tailored to fit their needs. It is redundant, and can be inconsistent, among these independent systems. Redundancies in turn come at a cost in data management for

7 Tiwana *et al*., 'Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics' (2010) ISR Vol 21.

8 <www.bfs.admin.ch/bfs/en/home/news/whats-new.assetdetail.24605850.html> as of 31 May 2023.

9 Sandoz (1999), ibid.

farmers. Some organizations control the data they receive for accuracy, and errors can carry the *risk* of penalties for farmers.

Since the late 1800s, the collection of data on farms had mainly been done by the Union of Swiss Farmers, which used it for statistical, extension, and political purposes. As long as pen and paper were the backbone of information management, the effort required to collect and manage data refrained institutional actors in the sector from developing market or management practices in agriculture that would require the collection of detailed information on farms. Within a few years-time, database technologies, personal computers, and web-based applications made it possible for public administrations and private organisations to collect information directly from every farm and extract value out of large amounts of digital data. But at the other end of the process, *i.e.*, at the source of the data, the farmers could not follow up. The information infrastructure of agriculture had become a mille-feuille of institutional platforms, some loosely connected through APIs, some standing alone, each with their own clientele and caring primarily for their own needs. The multitude, heterogeneity, and complexity of data requirements from too many actors resulted in administrative burden, risks, and a growing dissatisfaction.[10] The deployment of information technologies since the mid-1990s had led by the early 2010s to a *reverse salient*, a situation where change is hindered by practices which, for some reason, prevent innovation.[11] [12] At least the situation was presented in that way by a consortium of private actors, indirectly supported by political interests close to the economy, who proposed to build a *unique* (*centralized*) *database* for the management of *all the data in the sector*. Unicity was the main argument in favour of the proposal and centralization was presented implicitly as a consequence. The database would be complemented with smart-farming *modules*. The resulting platform promised to be a simple means to solve the data problem and to lead farmers into a new age of digital profitability. The Barto project was born.

10 Droz *et al.*, *Malaise en agriculture. Une approche interdisciplinaire des politiques agricoles France-Québec-Suisse* (Karthala Editions 2014); Stiefel, 'Les données du problème. Une plateforme numérique inadaptée à l'agriculture suisse' (2022) Etudes Rurales, 209.

11 Hughes, 'The evolution of large technological systems' (1987) in Bijker, Hughes, & Pinch (eds) *The social construction of technological systems* MIT Press, 51.

12 Slota & Bowker, 'How infrastructures matter' (2017) in Felt, Fouche, Miller, & Smith-Doerr (eds.) *The handbook of science and technology studies*, MIT Press.

Many farmers, administrations, and private organizations however agreed neither to the proposed centralization of ("*their*") data nor with the ensuing private control of all of the sector's data by a self-promoted benefactor.[13] This led to the counter-initiative called ADA to develop a solution to data-sharing that could be used to relieve the pressure on farmers *and* to curtail the deployment of Barto. It was supported by organizations in the integrated, organic, and plant production sectors and represented 50% of Swiss farmers.

C. Definitions and conceptual framework

We explore *dVAT* in this socio-technical context from the perspectives of 1) farmers who supply sensitive information to organisations that make some usage of the corresponding data in their digital information systems, possibly returning a tangible benefit to the originator of the data (*e.g.*, a subsidy, a premium, or market access for their product); and of 2) the abovementioned organisations when their digital systems exchange sensitive data.

Farmers and organisations belong to the *analogical* world. We need to be able to qualify the notions above in that context (exchange of *information* to obtain/deliver tangible benefits) in order to understand how they can be declined in the digital context (production, exchange, and usage of *digital data* for the computation and traceability of the benefit). To study *trust* in this context, we use the ABI framework. Although agriculture is evidently not an enterprise, nor an organization in the classical sense, its organizational characteristics justify the framework which was designed initially in the context of organization studies.

The definition of trust proposed by Mayer, Davis and Schoorman is "the willingness of a party to be *vulnerable* to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the *ability to monitor or control* that other party". [14] This abundantly referenced definition (the paper has been cited over 30'000 times) also encompasses both the notions of vulnerability and of accountability. The model has been used to study trust in contexts

13 Stiefel (2022), ibid.
14 Mayer *et al.*, ibid.

that go beyond organizations.[15] [16] [17] We use it here to study vulnerability, accountability, and trust in the digital context.

Mayer *et al*., emphasize the *risk* that a trustor is willing to take in order to benefit from the outcome of an action executed by a trustee whom the former potentially does not *control*. *Ability*, assessed by the trustor, refers to the capacity of the trustee to execute precisely that action, independently of any other actions the latter might or might not be able to undertake. *Benevolence* is the belief by trustors that trustees are not acting on their own profit-driven motives, but genuinely want the trustor's good.[18] *Integrity* is how much the trustor perceives that the trustee is attached to principles that the former finds acceptable. Based on their review of the literature on trust, Mayer *et al*. select these three factors to represent what trustors might generally *take into account* when evaluating the risk of an action that they have trusted another party to execute.

Relatively to data sharing, we consider vulnerabilities, risks, and benefits between farmers and organisations, and between organisations. We start from a situation where: 1) farmers have a relationship with selected organisations whom they provide sensitive information to. A contract or a software license agreement exist between the parties and regulate the production and the usage of the corresponding data, as well as the possibility to transmit the data to third parties. Organisations are accountable to farmers under the provisions of these private or public contracts; and 2) organisations are autonomous entities that operate under legal constraints. They are liable for their actions under their own responsibility. Specific contracts *between organisations* concerning the exchange of data might exist. In this case, *both* entities must conform to regulation on the access to sensitive data of third parties.

At this point Barto and ADA come into the picture. Neither one aims at changing the relationship between farmers and organisations as described in 1) and 2). However, they strongly modify the reasons, the way, and the means by which data are to be shared in agriculture. Do *new* vulnerabilities,

15 Ward *et al*., 'Trust building and the European Reference Network for Critical Infrastructure Protection community' (2014) IJCIP Vol 7, 193.

16 Bodó, 'Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators' (2021) *New Media & Society* Vol *23*, 2668.

17 Sasse & Kirlappos, 'Design for Trusted and Trustworthy Services: Why We Must Do Better' (2014) in *Trust, Computing, and Society* CUP, Part 3, 229.

18 Hardin, R., *Trust and trustworthiness* (RSF 2002).

risks, and benefits emerge from these projects? Might *old* vulnerabilities, risks, and benefits be altered by them?

Farmers, students, and patients are physical *persons*. They use *computer systems* (mobile devices, laptops, personal computers) in their daily activities. Some of these digital systems might be large, or seem to be, like the computer system that operates a modern farm. But they are small relatively to the information *systems* of private or public organizations like the ones we consider in this paper. Those systems are operated by professional IT staff. They are built and maintained according to strategies and guidelines that relate to the discipline of *enterprise architecture*.[19] They support complex functionalities at the core of an organization's business. They comprise databases and applications, run on private networks, and their connexion to the Internet is very sensitive. They might have evolved over long periods of time and parts of this infrastructure might be *legacy*, which means, basically, outdated but too important to throw out and too expensive to adapt. Some functional components (*e.g.*, enterprise resource planning, ERP) might be licensed from third party software providers and operated remotely *out of the cloud*. These large enterprise *information systems* are owned and controlled by organisations under their individual legal responsibility, and for their own profit if the owner is a private actor.

People and organizations *interact*. When digital systems mediate interactions, those systems *interoperate*. Interoperability is a coordinated exchange of data between systems over a digital *platform*. At the lowest level the platform is TCP/IP. At higher levels it might be *e.g.*, FTP, HTTP, a webservice or e-mail, Amazon, Facebook, or Uber, or SWIFT.[20]

We use a definition of "software-based platform" to anchor the notion of *platform*: "the extensible codebase of a software-based system that provides *core functionality shared* by the modules that interoperate with it and the interfaces through which they interoperate".[21] The terms "core", "shared", and "functionality", will come back into focus when we discuss trust in relation to platforms. Most platforms considered in the literature are *centrally controlled and proprietary*.[22] Although it is more restrictive than the

19 Ross *et al.*, *Enterprise Architecture as Strategy. Creating a Foundation for Business Execution* (HBS Press 2006).

20 Scott & Zachariadis, 'Origins and development of SWIFT, 1973–2009' (2012) *BH* Vol *54*, 462

21 Tiwana *et al.*, ibid.

22 Hanseth & Bygstad, ibid.

definition, this is actually the model considered in the research note on platform evolution.[23] It also applies to large social media. This type of configuration tends to be problematic, as the literature has shown for platforms like Twitter or Facebook.[24] *Service* platforms like the latter or like Barto are controlled by their owner over application programming interfaces (APIs) that give access to functionality and data shared by the system. The sharing of functionality goes from the core (the platform owner's information system) to the periphery (modules) and the sharing of data basically goes in the other direction.

However, digital platforms in the sense of the definition need not be centrally controlled nor proprietary. *Interoperability* platforms like in particular, TCP/IP, FTP, and HTTP are not, and neither was ADA by design. These different characteristics of platforms are described in and are relevant to understand platform trustworthiness.[25]

D. Methods and materials

Our appreciation of Barto relies on the fieldwork of the first author.[26] Interviews were conducted between January 2018 and September 2019 with *ca.* 40 actors in the sector. These included farmers (5) and representatives of agricultural organizations: agents of public administrations (11) and of professional defence (2), representatives of control bodies (6), certification bodies (2), professional associations and companies in the animal and dairy sectors (6), IT service providers for agriculture (4), and system operators of these same organizations (7). Interviews were recorded, transcribed, and coded using Nvivo. Section 5 gives a summary of this work in relation to our concerns here.

23 Tiwana *et al.*, ibid.

24 Bucher, 'Objects of intense feeling: The case of the Twitter API' (2013) Issue 3 *Computational Culture* <http://computationalculture.net/objects-of-intense-feeling-the-case-of-the-twitter-api/> accessed 5 June 2024; Puschmann, 'The politics of Twitter data' (2013) *HIIG Discussion Paper Series*; Helmond, 'The platformization of the web: making web data platform ready' (2015) *Social Media+Society.*

25 Sandoz & Stiefel, 'Untying the knot between software-based platforms and information infrastructures' (2022) <www.researchgate.net/publication/363582508> accessed 5 June 2024.

26 Stiefel (2022), ibid.

In parallel, the second author held meetings in ADA with over 50 representatives of public and private organizations, and with farmers and researchers, covering in particular the German-speaking part of Switzerland, that he reported back to the ethnographer who held a field diary on ADA (725 pages and 223 entries). The details are presented in her thesis.[27]

The appreciation of ADA is rooted in conceptual considerations. It was designed in view of stopping Barto by proving that data-centralization, if at all possible, was not necessary to solve the reverse salient in data management to the satisfaction of the actors in place. The approach explicitly left the choice to organisations whether or not to participate. The design would rely on a model of *actors exchanging information* over their information systems (*e.g.*, where notions such as liberty of association, autonomy, or trust apply), and not only of technical systems that interoperate over APIs.

E. Case studies

During 2018 and 2019, interviews revealed a range of concerns and risks of organizations and farmers regarding data management by Barto. Data-owners (farmers) and representatives of data-users (organizations) were concerned by the project's stakeholders, by the dependencies the system would create, and by the possible consequences. We start by describing how data is used by farmers and organisations, before reporting on their respective concerns.

Farmers use digital systems in *production* and in *management*. In *production*, systems are used for *functionality* (*e.g.*, to control the gate to an automatic milking machine, depending on how long a cow has been feeding) and for *decision-support* (*e.g.*, to suggest when to irrigate or to treat a crop, depending on environmental factors). Systems use data that is generated locally (*e.g.*, by machines, sensors, robots) or remotely (*e.g.*, by weather stations or global navigation satellite systems). These systems produce new data. They are developed by the agroindustry which supplies machines and inputs. Suppliers usually keep under tight control the data that their systems produce and use.

In *management*, digital systems are used for *resource planning*. For this type of system, data is related to resources, to products, to the market, and

27 Stiefel Léa, *Politiques des architectures numériques. Cheminements ethnographiques dans la conception d'alternatives à la centralisation des données* (University of Lausanne 2023).

to financial, regulatory, or other factors. Farmers themselves supply some of the data used for resource planning, *e.g.*, dates and places of sowing, types of crops or treatment, produce and income, costs, etc. The rest of the data is supplied or sourced by the software provider who develops, operates, and maintains the system.

Increasingly, data used and produced by these systems is stored in remote databases operated by their service providers. The latter compete to increase the number of farms that use their software, which collects, computes, and accumulates data. Data can be used to improve a system, but it can also be a valuable source of information on the market. So, data is precious to service providers. It is also sensitive for farmers, because it describes quantities, quality and maturity of products, customers, costs and prices, as well as modes of production that can be strictly contracted or regulated.

The evolution of digital technology *as a service* has brought advantages to farmers as it often simplifies management, and enhances the quality and availability of information. It has also benefited database operators by giving them free access to large quantities of valuable data (all the while enabling the cost of software maintenance and of customer relationship management to decrease).

Organizations use data to manage information on individual farms and transversally through the sector depending on their mission. Public administrations supervise the implementation of regulation, notably of subsidies; producers organizations define requirements for labels (*e.g.*, organic, integrated, traditional, etc.) and distribute individual quotas, which, if both are respected by the farmer, bring a premium on the market; professional organizations compute statistics to define their policies and lobbying strategies; some private organizations are supported by the regulator, *e.g.*, to prevent inbreeding in livestock by controlling the distribution of genes to farms and to improve breeds by increasing the resistance of animals to pathogens; etc. All of these activities require sensitive data from farmers who must deliver if they want a shot at the benefits. For each organisation, its data is homogeneous and might have a broader coverage than the market share of any service provider (see above). Organizations store the data in their own database and develop in depth knowledge, both transversal and specific to individual farms, on sensitive questions.

To summarize: data concerning farms is maintained in dispersed databases operated by independent organizations, *i.e.*, data-*users*. Each organization defines procedures (*i.e.*, in particular *when* the data is collected)

and data formats (*i.e.*, how information is digitized) according to its needs. To prevent sanctions and other negative consequences of false interpretations, farmers (*i.e.*, the data-*owners*) need to control what information goes where, when and in what form.

I. Barto: a service platform on top of a centralized database

Project Barto proposed to collect all farm data in a unique central database and, on this basis, to develop smart services for farms (decision support modules). Farmers explained their concerns to the ethnographer:

- among the project's stakeholders were the largest agricultural cooperative in Switzerland *Fenaco*, both the main supplier and a major buyer of products for farms; a European software development company *365-FarmNet*, linked to the cooperative by a German machinery manufacturer *Claas*; and two important publicly owned, *resp.* supported, Swiss organizations *Identitas* and *Agridea*. Farmers were concerned that the project was backed by a conglomerate of powerful private players. The centralized database would be able to provide full visibility into what was happening on all farms, on a daily basis. Combined with their own private decision-support tools, the database would enable the cooperative and its foreign partners to drive the demand for inputs and the supply of agricultural products, and to influence market and supply prices. Farmers perceived a high risk of "vertical integration", bringing commercial vulnerability because a third party would control all their data. Meanwhile they would retain the burdens of debt and production risks (such as losses due to weather or disease). They would *pay* to use "services" developed on the basis of *their* data and would be held *liable* by contract for its quality, while all the profits would go to the database owners;
- it was unclear how data would flow between organisations associated with the centralized database. Without control over the flow of their data, they were at risk. For example, if data inadvertently reached a government agency, indicating high nitrogen levels in one field, the farm could lose subsidies, even if they were compensated in another (which happens daily on many farms). If data from a government inspection showing a health problem of an animal was inadvertently passed on to a dealer, the farm and its neighbours could be side-lined (what actually

happened to an entire village because of a single sick animal) for fear that disease might spread from a shipment to the slaughterhouse;

Barto also proposed to redistribute the data out of its central database to data-users (*i.e.*, organizations) according to their needs. For the latter, centralization also posed problems:

- organizations would have to "log in" to the central database to access the data they needed and that had been previously supplied to them directly by the farmers. There was no guarantee that they would actually be allowed to access the data in contents and formats, and at times necessary to carry out their duties, nor was there any indication of the price to be paid. Centralization promised to jeopardize the autonomy of the organizations, to the point of threatening their very existence;
- project Barto planned to store farm data in a cloud in Germany[28], under the control of its software partner. This posed a problem of data sovereignty, which was unacceptable to public administrations. It also posed problems as to how to resolve conflicts between farmers and organizations arising from data management, with data residing in the legal realm of a foreign authority;
- the centralized database would introduce a distortion of competition: faced with foreign stakeholders who would concentrate all the farmers' data, small Swiss organizations, e.g., high quality local insemination cooperatives, would not stand a chance to compete and were at risk to disappear;
- Barto promised that organizations could propose functional modules connected to the central database, but it was not clear to organizations if this openness would be observed in reality beyond the rhetoric. Its owners could act single-handedly, as long as they controlled the platform's APIs and the data.

II. ADA: a peer-to-peer platform for authorized data transmission

ADA emerged in reaction to Barto and to the problems and threats that were perceived by the sector's actors. The opposition between the two

28 Swissmilk, <https://api.swissmilk.ch/wp-content/uploads/2019/06/praesentationen-vorstellung-ada-barto-hotel-bern-2018-02-28-de-fr.pdf> accessed 5 June 2024.

projects is clearly assumed in this paper and was public.[29] Our purpose is not Manichean: ADA was not a commercial competitor, nor was the project an attempt to *take over* the information infrastructure of Swiss agriculture. ADA's *proposed* alternative to Barto's approach was to provide a transversal component in agriculture, that farmers and organisations could freely use to improve data management where it was meaningful, and possibly reduce costs, inconsistencies, and redundancies. The section describes the rationale and functioning of ADA. It does not intend to be rightful or prove correctness, but rather to show the complexity of sensitive data sharing and to sketch its technical limits by connecting the concerns of the actors with the constraints, design features, and technical mechanisms that were embedded in ADA. The proposition consisted in providing the digital ecosystem of agriculture with a means 1) to authorize and trace the exchange of sensitive data between the information systems of data-users 2) without altering the practices (of actors) or the operations (of systems) in place. The technical solution would be a peer-to-peer platform where the peers would be organizations, each operating a *node* of the platform to which it would connect its information system over an API that it controlled alone. The platform, composed at any time of all the operational nodes, would be neither proprietary nor centrally controlled. Its only (core shared) functionalities would be:

a) for the data owner (*i.e.*, the farmer) to grant and manage authorizations; and
b) for the data users (*i.e.*, the organizations that operated sensitive data) to exchange data if the authorization had been granted by the owner, and if and when both users agreed to do so.

Nodes would manage and make data persistent only when it was related to these two functionalities and only when their peer was directly concerned. Sensitive data of farmers would be sent and received by nodes, in order to be stored and accessed in their respective systems, only by the users of that data, under the separate contracts or software licenses they had previously established with the data owner (see section 3), and on the respective system. Transmission would be bilateral and direct between the two nodes of the peers concerned. Authorization would be tripartite. How a data-owner was identified by a data-user would not be shared (the contrary

29 Swissmilk, ibid.

would imply a dependency between operators and violate the principle of autonomy). Traces necessary for a peer to positively prove *correct* behaviour would be stored locally in its node after each sensitive operation and kept under the control of that peer only. Traces might be *removed* from a node by its peer, because of the latter's full local control over its node. So, there could be *no proof of misconduct*, only *an absence of proof of correct behaviour*, that could lead to the suspicion of a rule violation. These considerations follow the technical line of what is possible or not in an asynchronous (general) distributed system. They determine the scope and the limits of accountability for data sharing between organizations. The platform would be *fully* distributed. All roles would be *symmetrical* (what a peer could, every peer could, with the same constraints). Within its scope, the platform's architecture would preserve the autonomy of each peer and guarantee the freedom of association, an equal treatment, and symmetry among peers.[30]

Technically, the project faced two challenges: *i*) *asynchrony* in distributed systems (which is usually overcome by using the master-slave paradigm underlying internet protocols based on APIs controlled by the master); and *ii*) *matching the different meanings attributed to information* by a sender, a receiver, and a farmer *using digital data* (which is usually overcome by using data standards and fixed formats agreed by or imposed to data-users).[31] Problem *i)* is inherent to communication in distributed systems and requires its own toolset to be correctly mastered, notably to maintain shared states in asynchronous configurations. Problem *ii)* is trickier and is usually solved by using data standardization, an invasive mechanism that can provoke side effects.[32] It would imply a change in system processes and organization practices, neither of which was acceptable for ADA's sponsors. A mechanism called *segmentation* was designed to bridge the gaps in time and meaning that could arise between organizations that would exchange data over ADA. The same mechanism underlay the touch-screen app used by farmers to manage authorizations. Organizations would know how to associate information that they managed for farmers to digital data using segmentation. So, organisations whom farmers trusted (*i.e.*, *from* which they accepted to *send their data* to other organisations) could help them

30 Stiefel & Sandoz, 'Une plateforme en pair-à-pair pour l'échange de données: l'émergence d'un commun numérique' (2021) *Terminal.*

31 Hardstone *et al.*, 'Standardization, trust, and dependability' in *Trust in Technology: A Socio-Technical Perspective* (Springer 2006).

32 Hanseth *et al.*, ibid.

manage authorizations by providing guidelines and templates (see the discussion below).

The platform was designed as a permissioned, fully distributed and symmetrical network of identical nodes, each operated under the control of one peer. The node was designed as a structured set of *services*, organized in functional layers as in the OSI model of ISO.[33] Each service *instance* in one node *logically* interoperated only with the instances of the same service of other nodes.[34] The platform's technical architecture, its node implementation, and the connexion of legacy systems to nodes, were based on the Kubernetes (K8s) microservice architecture. The gRPC standard interface framework (for APIs) and the Hyperledger Fabric distributed ledger (for the publication of source datatypes and usages) were available at the time of the project on top of K8s. All three technologies were standalone and freely available in open-source code.

F. Discussion

In the previous sections, we examined the two projects that aimed at solving a digital reverse salient caused by uncontrolled digitization *following* a structural transformation in Swiss agriculture, that was *independent* of digitization.

Barto was a service platform with a centralized database and APIs controlled by the platform owner. It proposed to manage all of the farm data in the sector. Its stakeholders were a consortium of private actors with commercial interests in the agri-food sector. These interests could leverage Barto by concentrating exhaustive vertical and transversal information in one system they would control. The business model was a service platform with complementors, like Facebook.[35] Complementors would supply smart-farming modules. Organisations would delegate data management to the platform and access the data they needed over its APIs. The project was capital intensive (over 10MCHF in 5 years), and technically and commercially risky. Feasibility was only sporadically questioned though it represented a significant risk: if the project could not collect all the data or

33 ISO/IEC 'Information technology — Open Systems Interconnection — Basic Reference Model' (1994).

34 Sandoz, 'Inter-operating Co-opeting Entities: A Peer-to-Peer Approach to Cooperation between Competitors' (2020).

35 Helmond, ibid.

implement all the functionalities required, the platform would become just another farm-ERP, possibly with privileged relationships along the business lines represented by specific stakeholders. Development was conducted internally by one of the stakeholders.

ADA was a peer-to-peer platform composed of an evolving and open number of nodes connected each to the information system of one organisation (a peer). The APIs and the services of the platform were distributed in the nodes, each node being technically and legally controlled by the peer it serviced. ADA itself did not manage nor store any data. Farm data remained in operators' databases. The project's stakeholders were associations of farmers and professional organisations. Its business model was collective funding of the initial instance and free open-source community development and maintenance once the platform would be in production. Access was free for farmers and auto-financed by organisations according to their needs. Organisations would continue to operate their own information system infrastructure, legacy systems, and databases, and operate their own node. Farmers would be implicated in data management through the authorisation function for data exchange between operators. The main motivation of stakeholders was to curtail Barto which was seen as an existential threat. Technical *dependability* of the platform was a design goal, but it was never discussed *in detail* with ADA's sponsors. The initial version of the platform cost under 1MCHF. The project was commissioned by the organisations and development was external.

The opposition between the two projects along clear functional, organizational, and architectural lines is an opportunity to study the potential and limits of digital technologies in relation to *dVAT*. Before Barto and ADA were launched, farmers' data were distributed throughout a landscape of organisations, each operating its database and accountable under its own technical and legal responsibility: *dVAT* were point to point (farmer to organisation) and determined by contracts. The *data-for-service* relationship was biased in favour of the organisations and created asymmetric dependencies, but the farmers could quit in most cases, exceptions being the enforcement of regulation (like animal control). With Barto, this freedom would be lost, creating a new type of digital vulnerability for farmers: complete visibility, and the economic threat of verticalization. Additionally, every organisation but one (Barto) would become vulnerable to the whims of the latter.

With ADA, the relationship between farmers and organisations remained unchanged. Farmers were provided with a means to control and trace eventual data-flows between organisations, making them less vulnerable to data-leaks through undisclosed back channels. Consequently, the accountability of organisations would be reinforced and trust of the farmers towards organisations would follow where accountability, and hence trustworthiness, could be established. Where this was not the case, the farmer retained the possibility to quit, as previously. With Barto, trust fell out of the equation: the farmer would not *willingly* take a risk (of entrusting their data to the consortium), but would be compelled to do so. Additionally, farmers would be made accountable for errors, not the contrary. For organisations, Barto became a new intermediary cast between them and the farmers. Not only would organizations become vulnerable towards the central actor, as described above, but technically, the centralized platform and API configuration would impair their ability to fulfil their missions.[36] They would remain accountable to farmers for the quality and the timeliness of their services, but would no longer be able to control what they delivered and when. With ADA, each organisation controlled, operated, and was responsible for its own node, preserving accountability to farmers. Mutual liabilities between organisations concerning the transmission of data over ADA would have to be defined, either collectively or bilaterally.[37]

The two approaches were technically different (centralization *vs.* distribution) and the choice of the approach had heavy consequences on the vulnerability of actors, on their accountability, and on their mutual trust relationships.

G. Conclusions

As opposed to platforms with millions or tens of millions of users worldwide like Facebook or Amazaon, in this paper we explored the topic of digital vulnerability, accountability, and trust (*dVAT*) *in the small*, *i.e.*, the design of sensitive data sharing in a small economic sector in a small European country, with homogeneous legislation. A few tens of thousands of persons (farmers) must make decisions concerning which organizations

36 Stiefel & Sandoz, 'Critique de la concentration: une analyse des relations de dépendance sur les plateformes numériques' (2022) *AIMS Conference on Strategic Management.*

37 Stiefel & Sandoz, 2021, ibid.

they can or cannot entrust their sensitive data with. A few hundreds of organizations, private or public, who structure the activities of the sector, traditionally consider the data they use as "*their*" own property. How can accountability and trust be sown into this type of environment? When Barto threatened to take over data management in the sector, ADA attempted to give some control over their data back to farmers. The project designed a peer-to-peer software-based platform that had a key characteristic: it was not controlled (neither owned, nor operated) by a single actor or a small group of actors who might aim to leverage data to sustain their interests. It was operated by *every* actor, within their circle of control and legal responsibility, and worked symmetrically relatively to all the participants.

The platform sent the question of accountability and trustworthiness back to each organization that managed sensitive data of farmers. The farmer could privilege a trusted relationship with one player or another, or delegate the assessment of platform usage to several independently. In this decartelized configuration, the agency of the farmer would encourage trustees to be more accountable.

The peer-to-peer platform was designed to address the concerns of data owners and of data users, and to enhance accountability and mutual trust based on its socio-technical architecture.[38] Farmers demand privacy from the organizations that manage their data. They *trust* them more or less to provide services in accordance with the information they supply about their farms (aptitude). They do not always trust them to use the data to their sole benefit (benevolence). They are sometimes at risk that the data will not be used properly (integrity). An architecture that relies on transparency in how data is collected, circulated, and used by operators could reduce vulnerabilities, strengthen accountability, and enhance trust. In a framework with clearly defined rules, control mechanisms and sanctions, that the user community itself could steer according to changing conditions and needs, possibly under the guidance of external authorities[39], farmers (and organizations) might better accept, and even push for, data sharing. Data management might then become less complex and more efficient, and the digital vulnerability of data-owners might be reduced.

38 Mazzella *et al*., 'How digital trust powers the sharing economy' (2017) IESE Insight, Issue 30, 24.

39 Hess, C. & Ostrom, E. *Understanding Knowledge as a Commons. From Theory to Practice* (MIT Press 2007).