Towards new models of information sharing

Camille Dubedout[1] and Manuel Munier[2][0000−0003−0282−4508]

[1] ANSSI
Université Grenoble Alpes
Grenoble, France
camille.dubedout@univ-grenoble-alpes.fr
[2] LIUPPA
Université de Pau et des Pays de l'Adour, E2S UPPA
Mont-de-Marsan, France
Manuel.Munier@univ-pau.fr

Abstract. The proliferation of data exchange within cities in recent years has raised a number of challenges for the various stakeholders involved at local level, such as private digital service providers and local authorities. These challenges, which arise at every stage of data processing, from sharing to storage, call for the creation of new rules governing the transparency, quality and traceability of exchanged data. Commonly shared, these new rules are likely to foster trust between different types of stakeholders with regard to exchanged data, and encourage the equitable sharing of digital resources, particularly between public and private stakeholders.

Keywords: Data governance · Commons · Accountability · Traceability.

1 The rise of data exchange

Since the development of the Internet and the rise of the World Wide Web in 1989, data exchanges have increased exponentially. In just a decade, we have moved from the era of exchanging exabytes of data to that of zettabytes (10^{21} bytes).

This evolution is particularly evident with the advent of "smart cities", known in France as "Smart cities and territories." These urban areas utilize data processing technologies to promote the circulation of data between public and private actors. According to the French Data Protection Authority (CNIL), a smart city is defined as *"a new concept of urban development. It involves improving the quality of life of city dwellers by making the city more adaptive and efficient, using new technologies which rely on an ecosystem of objects and services"*. Data exchanges within these cities and territories are facilitated by multiple communication networks, data capture tools, and actuators (like connected devices). These technologies not only collect various types of data but also increasingly enable actions on the environment. The proliferation of data exchange through connected devices has led to the creation of new services in diverse areas such as transport, energy, waste management, water management,

and traffic flow. However, most of these data capture and processing technologies are designed and managed by private entities. Consequently, these private actors set the rules for data sharing—and non-sharing—often under the guise of business secrecy. This can limit access to and use of data by external parties, particularly citizens and local authorities. As a result, unless there is a specific, formal contract between a local authority and a private manager covering the reuse of data, many data flows are exploited for private purposes, potentially disregarding the public interest in dissemination.

This article, which may seem atypical in form, is the result of a four-way collaboration between a legal expert and a computer scientist, with the aim of tackling the issue of the risks induced by information sharing, both from the angle of the need for appropriate regulation, and from the point of view of the technical elements that would enable such governance to be implemented. This reflection is perfectly in line with current legal developments, particularly at European Commission level, one of whose major concerns is the notion of data governance, which has resulted in the entry into force of various texts and regulations in recent months.

2 The fundamental challenges of data exchange

The exchange of data, not limited to personal data, presents a significant challenge: how can we control and protect the data circulating among numerous stakeholders ? This question extends beyond the technical security of various networks, such as 4G or 5G, and encompasses the broader issue of governance[3]. The core issues revolve around citizen access to data, its distribution, traceability, and integrity guarantees. These concerns are paramount as data exchanges become increasingly integral to the functioning of cities in France and worldwide.

Today, various legal and regulatory texts aim to guide data usage by promoting its dissemination or restricting certain types of data. For example, in France, the Law for a Digital Republic (In french: "Loi pour une République Numérique" - LRN) of October 7, 2016, encourages administrations to open and share public data, in order to facilitate its reuse by businesses and citizens. This law mandates that all state administrations, local authorities with more than 3,500 inhabitants, public establishments, and private organizations in charge of public services publish their source codes and public databases online. The Law for a Digital Republic must be reconciled with the European General Data Protection Regulation (GDPR) of May 25, 2018. The GDPR requires all entities processing personal data, whether private companies or public authorities, to

[3] Governance can be defined as: « the forms of steering, coordinating and directing individuals, groups, sectors, territories and society, beyond the classical organs of government. [...] It has three central points: the idea of giving direction to society, mobilizing a coalition and exercising constraint – three essential dimensions of politics ». V. Patrick Le GALÈS, « Gouvernance », Dictionnaire des politiques publiques, Laurie BOUSSAGUET, Sophie JACQUOT et Pauline RAVINET, 5e édition., Paris: Presses de Sciences Po, 2018, p. 299–308

minimize the use of personal data, clearly define its purposes, and respect the consent of individuals.

In addition of these two important legal texts, in late 2023, the European Commission, Parliament, and Council agreed on a proposal for a European regulation on artificial intelligence, which was approved by the Member States on February 2, 2024, and has come into effect in August 2024. This text aims to establish a framework for the use of data in artificial intelligence models. Specifically, it mandates a range of obligations for organizations that provide, distribute, or deploy AI systems, based on different levels of risk.

Moreover, since February 17, 2024, the Digital Services Act ("DSA"), which has been adopted the October 19, 2022, requires that a wide range of internet entities — including online platforms, cloud providers, and digital service providers — offer tools for users to report illegal content. Upon receiving a report, these entities are required to promptly remove or block access to the offending material. Additionally, they must establish robust content moderation systems and maintain transparency about their moderation policies, ensuring that users have the ability to challenge decisions. Major platforms like Amazon, Google, and Apple are further obligated to conduct an annual assessment of the societal risks their activities may pose, such as impacts on public health, online violence, or electoral integrity. They must then implement appropriate measures, such as eliminating fake accounts, to mitigate these risks. The overarching goal is to curb the spread of misinformation online. In the event of non-compliance, these large platforms could face fines of up to 6% of their global revenue. For severe or repeated violations, they may even be barred from operating in the European market.

Additionally, since 2023, the European Data Governance Regulation (or "Data Governance Act") brings new rules for data sharing within the internal market. This "DGA" aims to promote free data sharing across the Union by encouraging the establishment of common data-sharing spaces and data intermediaries, particularly in health, mobility, energy, and agriculture. The regulation seeks to enhance data access, portability, and interoperability within the Union while balancing business secrecy, personal data confidentiality, and free data reuse. Public organizations must publicly state the conditions for authorizing the reuse of certain data, such as data related to statistical confidentiality or third-party intellectual property rights. However, they must ensure confidential data is anonymized and shared in a secure environment.

While the European Regulation on data governance advances data sharing and availability through data intermediaries, it falls short in specifying the concrete forms of data sharing between public and private stakeholders within member states. Consequently, there tends to be a lack of management rules and organizational responsibilities that adequately balance data openness, protection, and sharing.

This article explores various ways in which data-sharing rules can be further developed.

1. **Stakeholder identification**: Today's smart cities projects involve a diverse range of stakeholders, including local authorities (such as municipalities or metropolitan governments), private economic players (digital service providers, telecom operators, or new players like GAFAM), traditional sectors (building, energy, or transport) and civil society players (like associations). Each stakeholder is likely to produce and share different types of data that need to be identified.
2. **Governance and participation rules**: Once stakeholders are identified, their roles concerning data sharing must be clarified, as well as the types of data involved. For example, determining if a stakeholder is a data producer, the nature of the data (sensitive, confidential, personal), its purpose, and if the stakeholder is also a data user. Depending on the data's nature, sensitivity, duration of use, and purpose, stakeholders could be subject to varying obligations:
   - **quality obligation**: ensuring a certain degree of accuracy and updating;
   - **traceability obligation**: setting up metadata to identify the various uses of data;
   - **transparency obligation**: informing about the measures in place around the data to ensure awareness of data quality levels.
3. **Identifying the type of commitment**: The type of commitment between stakeholders regarding data sharing needs to be specified. Should data exchange be governed by a free or "Creative Commons" license ? Should it be managed by a public contract, such as a public service delegation or a public procurement contract with transparent rules ? Can it be formalized through a Public data charter, as observed in Montreal, in Nantes, or in Occitanie region of France ? These forms of commitment can be combined, similar to a Data Charter proposing different data-sharing license formats.
4. **Material formalization**: From a physical perspective, these data exchanges could be governed by an API model. This public infrastructure would provide everyone access to the sharing rules and the principles of the Charter or contract.
5. **Determining responsibilities and penalties**: The responsibility of stakeholders is crucial for the smooth operation of data sharing. Liability can be administrative, civil, or criminal, and may sanction individuals or legal entities. Potential penalties could include financial sanctions for non-compliance with commitments or payment of damages, as stipulated in the GDPR (Articles 82 and 83).
   Sanctions can be imposed by external authorities, such as administrative authorities or civil courts. They can also be decided by the stakeholders involved in the data-sharing project themselves, acting as a collegial body to decide on appropriate sanctions on a case-by-case basis. Various direct or indirect measures can be considered, such as a negative rating for stakeholders who share significantly erroneous data.

3 An information risk management approach

To put this kind of responsibility management into practice, it will obviously be necessary to have "technological tools" on which we can rely. This is a more technical vision of the subject, presented in terms of security policy (sharing rules: contracts, usage control rules, etc.) and metadata (traceability, etc.).

If we approach this issue from the angle of information security and risk management (e.g. ISO/IEC 27005:2022 standard[4], french EBIOS Risk Manager method[5]), the aim is to propose and implement mechanisms for supervising information exchanges between a multitude of organizations (the stakeholders). These entities are independent of each other, i.e. they are free to set up their own (information) security policies; there is no central authority a priori. Moreover, they each have their own objectives and evaluation criteria, and may even be in competition on certain points: economic stakes, security criteria and levels, regulatory constraints, etc.

This interconnection of information systems is sometimes referred to as "systems of systems", to distinguish them from traditional "monolithic" systems, and to emphasize the operational independence of the elements (the individual systems), their managerial independence (there is no authority providing global, centralized, federated or other supervision), and emerging behaviors, in the sense that these interactions between elementary systems will inevitably give rise to new behaviors at the global level, behaviors that no one, a priori, will have specified. It should also be remembered that in this approach, it's not the security of information systems as such that takes precedence, but the security of the information itself.

A number of technologies and models already exist to guarantee the security properties of data exchanges between different interconnected information systems: cryptography (encryption, signature, watermarking, etc.), logging, blockchain [21], access control [20] and usage control [16], and so on. And, to be sufficiently precise, we need to come back to the distinction between the terms "data" and "information". (Digital) data is made up of a sequence of bytes: an integer, a real number, a character string, an image, etc. Unlike information, data is simply the representation of a value of a certain type in computing. For example, the value "15" only represents an integer. Does it correspond to a person's age ? A temperature ? The price of an item ? What information does this data convey ? Returning to existing technologies for ensuring the security of data exchanges, these will enable us to authenticate the system issuing the data (electronic signature), that the data is not altered (accidentally or deliberately) during transport, that only the recipient of a message can read the data (encryption), that no message is lost, that access restrictions are respected, that all stakeholders see the same events in the same order (blockchain), and so on. But when it comes to the information conveyed by this data, what about trust in

[4] ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection – Guidance on managing information security risks

[5] EBIOS: Expression des Besoins et Identification des Objectifs de Sécurité (ANSSI)

the system that issued it, the conformity of the use that will be made of it, the adequacy of the "quality" of the information produced to the "requirements" in relation to its use, etc. ?

In the context of setting up data governance to control information sharing on the one hand, and with the aim of reassuring data holders and encouraging them to make their data available to the community on the other, our problematic will naturally focus on aspects such as provenance, usage control, quality, sharing strategy, etc., which will be the focus of our research.

4 Relying on formal tools

As we indicated at the beginning of the previous section, from an Information Technology (IT) point of view, the challenge is to provide the "technological tools" to put into practice a data governance policy and the management of the resulting responsibilities. As current digital ecosystems have developed, they have mainly focused on the processing and storage of information at the level of individual players. As a result, communication infrastructures are generally limited to routing data from point A to point B, i.e. the data produced by one process is "simply" sent to serve as input for another. But NICTs could be capable of much more !

A number of research projects focus on communication infrastructures, proposing the implementation of data governance mechanisms to supervise information sharing. The idea is that these mechanisms should be able to check automatically whether the defined sharing rules have been respected, or that they should be able to reason to identify the causes of any violation, and to deduce, for example, the responsibilities of the various players involved. This requires a formal specification of the sharing rules, followed by the use of inference techniques for reasoning.

The first step is to formally represent (in a "mathematical logic") the main semantic elements of our domain, along with their relationships, in order to remove any ambiguity of interpretation linked to one domain or another: a piece of data, a data manager (sometimes referred to as the "holder" of the data, or even, erroneously, as the "owner" of the data), a data user (or "consumer", i.e. the person carrying out a processing operation), a sharing "rule", "properties" on the shared data, etc. The most significant part of this work obviously concerns the last two points. The "rules" are generally expressed in the form of logical predicates on which it will be possible to "reason", i.e. to deduce (notion of inference in logic) new knowledge (facts) on the basis of knowledge already expressed. Intuitively, these rules are written in the form of "if... then...". In a nutshell, such rules can be used, for example, to decide whether an action is authorized or not, or to add a new fact to the knowledge base (e.g. a new "property" of data or metadata, an "obligation" i.e. an action that must be performed before anything else can be done, etc.). These are known as access control rules (for information) or usage control rules (for information). Expressing these rules

in a formal language then enables them to be processed automatically by tools such as reasoners or inference engines.

But an essential part of expressing these rules is agreeing on the terminology to be used, just as when drawing up "paper" contracts. As early as 2001, Tim Berners-Lee and his colleagues [1] highlighted particular cases in which the existing World Wide Web had not maximized its potential, and further developed the fundamental principles of the then-emerging Semantic Web. Building on this research trajectory, Shadbolt and his team [12] examined the notion of ontologies, which are sets of concepts used to describe relationships between entities in a machine-understandable format known as RDF[6]. This enables knowledge modeling, the aggregation of different information systems and computational reasoning. To this end, SWRL[7] [6] is a rule specification language for the Semantic Web expressed in OWL[8]. By integrating such SWRL rules into a knowledge base, it is then possible to deduce new facts using automated reasoning engines.

In practice, it would be very interesting for this first stage to use semantic web techniques based on descriptive logics to represent ontologies (e.g. OWL) and rule specification languages (e.g. SWRL) for reasoning. It would then be possible to express an information-sharing policy, both in terms of "general" rules and specific license clauses, rather like a framework license within a community that can be refined with usage rules specified by the initial data holder, or the person who "produced" (or "made available") the data. Note that other models exist for representing usage control policies in higher-level formalisms. This is the case, for example, with the UCON [17] and OrBAC [8] models, which support the concepts of permissions, prohibitions and obligations. OrBAC's expressiveness is also enhanced by the ability to activate or deactivate certain rules depending on the context at the time they are evaluated. These are known as dynamic usage control rules.

This vision is perfectly realistic given today's IT tools. In [9, 10] the authors present such an architecture for ontology-based information sharing. In an informational self-determination approach, data producers can express the usage control rules they wish to see applied, in the form of licenses (entities represented in OWL, rules expressed in SWRL). They have also developed a prototype implementing this architecture using current tools available for the Semantic Web (notably the OWLAPI and SWRLAPI programming APIs). In [11] they also propose a method for translating OrBAC rules (including contexts) into SWRL rules usable with semantic web reasoners (e.g. Drools, HermiT, Pellet).

As we have presented them, usage control rules enable us to express that a certain action performed by a certain actor on a given resource will be permitted or rejected. The formalisms generally used are mainly based on the "producer" of the data, the "consumer" of this data and the action requested. As part of the implementation of data governance, it could be interesting to capture other aspects of information sharing, such as the various intermediaries between the

[6] RDF: Resource Description Framework
[7] SWRL: Semantic Web Rule Language
[8] OWL: Web Ontology Language

"producer" and the "consumer", any transformations applied to the information, the intrinsic properties of the information (e.g. quality criteria), and so on.

The second step in the formalization process is to specify the metadata that will be added to supervise the sharing of information. This applies in particular to traceability metadata, using provenance models such as PROV [13], both for upward traceability (the "where does the data come from ?") and for downward traceability (the "who uses my data ?"). By enabling traceability, metadata can help improve data quality. For example, metadata can provide contextual information on the date the data was updated, on the various modifications made to the data during its lifecycle, on its origin or its purpose, thus making it possible to assess the "quality" of the data studied. What differentiates data (known as raw data) from information is precisely the contextualization of this data (known as enriched data). This metadata can then be used in usage control policies to trigger certain rules via logic inference mechanisms, and so on in cascades.

These various mechanisms should enable us, through metadata ("who certifies that…") and licenses ("you have to respect the rules that…"), to determine and identify the "responsibilities" of the various players in this ecosystem, either in real time as data is used, or a posteriori by analyzing the traces in the event of an investigation.

From an IT point of view, the notion of responsibility refers, for example, to the presence (in the event history) of an erroneous event, or of a sequence of events that does not conform to the established rules (e.g.: an obligation not respected, i.e., an action that must be carried out before another has not been logged). More generally, it involves using traceability mechanisms to associate a given event with a specific actor. In fact, the term "*accountability*" can sometimes be more precise, designating "*imputability*" rather than "*responsibility*".

To conclude this section on IT tools for information security risk management, it should be noted that the use of formal tools (models based on descriptive logics, inference engines, etc.) offers us additional possibilities, thanks to their ability to justify the decisions inferred. The inference engines used are in fact capable of providing explanations for the knowledge they have inferred: which facts were involved in the decision, which rules were triggered, etc. This possibility is therefore extremely interesting in terms of the way it can be used in a decision. This possibility is therefore extremely interesting with regard to current trends concerning the explicability of decisions, trust and transparency in automatic decision-making systems (in the context of IA[9] [10], but not only), responsible digital, etc. In relation to the problematic of this article, the notion of explicability is perfectly in line with that kind of responsibility, and will undoubtedly be at the heart of much future work, in particular for the construction of a legally

[9] Artificial Intelligence in the European Commission – A strategic vision to foster the development and use of lawful, safe and trustworthy Artificial Intelligence systems in the European Commission (2024)

[10] Regulation (EU) 2024/1689 of the European Parliament and of the Council – laying down harmonised rules on artificial intelligence (June 2024)

valid model of digital evidence in the event of investigations following litigation, for example.

5 Technical tools in the service of the law: towards obligations for the quality of shared data ?

These various technical tools could be used by the law to clarify data-sharing rules, particularly those related to data quality and traceability.

5.1 From metadata to the obligation of data quality

To enhance the quality of shared data, the law could mandate that data producers and intermediaries publish their metadata. This would allow users to access more precise information, such as the production date of the data, any modifications made, and the identity of the organization or individual responsible for these changes. Metadata could also play a role in a certification process, where an external body reviews the data and decides whether to grant a quality certificate. In cases where companies lack metadata, the law could require them to implement a data quality management system.

Moreover, the law could set standards requiring that only data meeting specific quality criteria be shared. For example, it could stipulate that data producers must provide information that is less than a year old, with metadata used to verify the currency of the data. In this way, metadata serves as a critical tool for ensuring compliance with data-sharing rules, particularly regarding data quality.

5.2 From metadata to traceability and liability concerns

When a breach of data-sharing rules is discovered — such as the sharing of outdated or inaccurate data — technical tools like metadata can be also used to determine legal responsibility ("liability"). These tools can aid in gathering evidence and identifying the organization accountable for the violation.

In French, "responsibility" has a broader meaning compared to technical contexts, where it refers more to liability, or legally enforceable responsibility. There are various forms of liability: administrative (relating to public order violations), civil (relating to damages to individuals or property), and criminal (relating to unlawful acts). Liability differs from imputability, which involves attributing an action or fault to a person based on their conscious, voluntary decisions.

In civil law, liability can be either contractual or extra-contractual. Contractual liability arises from the obligation of one party to compensate the other for damages caused by failure to perform or improper performance of a contract. Extra-contractual liability generally hinges on fault—defined as intentional action, carelessness, or negligence that causes harm to another party. This form of liability requires establishing a causal link between the fault and the damage, and it can also result from a failure to act. Fault may be presumed, particularly

when a legal or regulatory obligation is violated. For example, breaching the European Data Protection Regulation could result in the liable organization being held accountable for any moral harm caused to an individual.

In this context, if a data user identifies a violation of data-sharing rules — such as the sharing of outdated or incorrect data — technical tools like metadata can help attribute the breach to the liable organization. For instance, log data can reveal which users may have altered the data, serving as a key method for tracing data exchanges. This enables a more precise understanding of the nature of the breach, facilitating evidence collection and helping to clarify the liabilities between data producers and intermediaries.

However, while these technical methods can address specific legal challenges, they fall short of resolving broader issues related to the distribution of liabilities among the numerous stakeholders involved in data exchanges. How can we manage situations where there are dozens, or even hundreds, of stakeholders ? What legal frameworks are most appropriate for enforcing data quality and relevance standards ?

6 Paradigm shift to management by the Commons

Even though technical tools help improve certain data-sharing rules, such as data quality or traceability, in law, the application of traditional rules in the broader context of data sharing among public and private organizations and citizens raises several issues.

1. **Determining legal subjects**: It is crucial to identify the legal subjects, which may include public administrations, companies, or any organization responsible for data processing. Responsibility can be assessed by defining the "data controller" as the entity determining the objectives of data processing, similar to the GDPR. If data-sharing rules are contractual, the legal subjects are the parties to the contract. Additionally, new legal entities, such as data intermediaries responsible for collecting and controlling data characteristics, could be established as advocated by the DGA.
2. **Defining data types**: It is important to specify the types of data involved, whether personal, non-personal, or metadata. Some data, such as sensitive personal data, may require special protections regarding the risks for privacy. The rules should apply to all stages of data processing, from production to storage.
3. **Establishing legal sources**: It is essential to consider the type of legal framework that outlines the various obligations for data controllers and, in the event of a breach (whether through a positive act, negligence, or omission), could engage their liability. This legal basis might be a law or regulation, such as the Law for a Digital Republic or the GDPR. Alternatively, it could consist of specific contractual rules, which vary across different disciplines. In public law, for example, this might involve public-private partnership agreements. Public administrations can enter into public procurement

contracts with private entities, as well as concession contracts, global performance contracts, experimentation contracts, or innovation partnerships. In private business law, particularly intellectual property law, license agreements are a common framework (see Article L613-9 of the french intellectual property Code). These license agreements allow the owner of a trademark, patent, or software to authorize another party (the licensee) to exploit their product or service within their commercial activities. The license agreement enables an organization to market a product or service without losing ownership and specifies the obligations of both the licensor and licensee, the duration of the contract, and the methods for resolving any disputes. These licenses can also be open access and then allow the licensee to use, re-use, share, modify, and distribute code in other programs or applications. Each open access license specifies the conditions under which source code can be re-used. Among the 80 license variants, two main categories can be identified: copyleft licenses, such as the GNU General Public License ("GPL"), the Affero GPL ("LGPL"), and the Mozilla Public License ("MPL"); and permissive licenses, such as Apache, the MIT license, and the BSD license.
Furthermore, from a broader political perspective, a Charter (a written and signed document detailing principles and commitments of the signatories) can also be established concerning data. Although signed, charters possess only declarative value. However, if a community decides, the principles outlined in a charter can be incorporated into all acts and contracts it enters into with its service providers. Several territorial data charters have been formalized by cities in recent years, such as those in Nantes[11] and Brest (Metropolitan Charter[12]). The latter aims to *"create a framework of trust for the collection, storage, use, and sharing of public or private data for the general interest"*. Its goal is thus *"to initiate cooperations with various public and private actors to enhance the value of all local data for the benefit of residents and public policies"*. Signing the Charter therefore acts as a label and enhances the image of the party voluntarily adhering to it.
More specifically, it entails determining whether current legal frameworks governing data sharing, notably those addressing data openness as outlined in the Law for a Digital Republic and the Data Governance Regulation (DGA), as well as personal data protection under the GDPR, are sufficient with minor enhancements, or if a new legal framework needs to be established.

4. **Specifying obligations**: The obligations for data controllers should be clearly outlined. Non-compliance with quality or integrity criteria for shared data, failure to include necessary metadata, or non-adherence to transparency obligations could constitute faults.
5. **Types of sanctions**: Sanctions for breaches of data-related obligations can vary widely, including warnings, financial penalties, or public notices, as seen

[11] https://metropole.nantes.fr/charte-donnee
[12] https://www.banquedesterritoires.fr/sites/default/files/2023-07/charte éthique de la donnée version signable.pdf

in the GDPR. In the context of a Metropolitan Charter, sanctions might involve the exclusion of stakeholders who fail to comply with its principles. Moreover, identifying responsibilities among various stakeholders in case of non-compliance can be challenging. This necessitates clear rules on metadata, including its retention and control by an external organization, to ensure data quality and traceability. Establishing such protocols helps maintain accountability and fosters trust among all parties involved in data sharing.

Given all these challenges, it is essential to move away from market and property-based logics and adopt a "commons" model for data management, as proposed by economist Elinor Ostrom [15, 14][13]. The notion of Common remains controversial [3]. However, Elinor Ostrom demonstrated that the Commons, under certain conditions, are an effective solution for managing resources. A Common, like a natural resource such as water, involves creating "a community of users collectively assuming responsibility for the long-term conservation of the resource, maintenance of the infrastructure, and distribution of the available resource according to very precise rules balancing the effort made in the service of the community and the benefits derived from it" [2]. This entails establishing collective liability for the resource that data represents, a liability that international law professor René Jean Dupuy (1989) termed "functional ownership". This type of ownership aims to ensure the integrity of the shared resource. Already, many public services in the fields of social action, education, sports, culture, or environmental protection can be considered as common services.

Information goods, being non-rival and intangible, fit well into this model. Data can indeed be considered as resources of infinite quantity, equally shareable infinitely. Non-rivalry [22] means that one individual's use of the resource does not prevent others from benefiting from it, while anti-rivalry means that individuals will use the resource all the more if it is already in use. Building on Ostrom's work, Benjamin Coriat [4] defines information commons as "resources governed by a system of distributed rights and a governance structure that ensures compliance with rights and obligations". Jeremy Rifkin [18] describes the commons as "a new economic paradigm that prioritizes use value over ownership", as seen in practices like *car-sharing*, *couch surfing,* and *crowdfunding*. Despite Garrett Hardin's 1968 assertion [5] that common ownership leads to resource depletion, the commons model now presents a credible alternative to traditional ownership structures.

To address these issues, we must:

- Overcome the dichotomy between public and market goods: This simplistic opposition fails to account for the diversity of goods and services, many of which fall outside this binary categorization.
- Develop a multi-actor data management model inspired by the Commons: Data, like natural resources, should be managed by a community of users

[13] Authors' note: Although some of these references are a little dated, they are nonetheless relevant in the sense that they form the basis of the concepts presented.

responsible for its long-term conservation, infrastructure maintenance, and equitable distribution based on contributions and benefits.

– Consider that local administrators should work with citizens to translate guiding principles into local rules, ensuring maximum unity and diversity without imposing uniform standards. This decentralized approach transforms the role of local administrators from mere compliance enforcers to active collaborators in governance.

However, the application of Commons to digital technologies remains a challenge [7] and shows many complexities in law [19]. In particular, challenges remain in establishing shared responsibility, avoiding erroneous data, and implementing sanctions. Identifying responsible actors for unreliable data, determining appropriate sanctions, and devising incentive mechanisms for reliable data sharing are critical. The introduction of metadata may play a major role here. The application of sanctions also raises questions. Which members would be legitimate in determining sanctions ? How should collective decisions be reached ? Is a supervisory authority necessary in the event of litigation ?

According to Pierre Calame and Yolanda Ziaka, *"experience shows that setting uniform standards is not the best way to ensure maximum unity and maximum diversity. It is essential to leave room for manoeuvre at the most local level, in application of jointly-developed guidelines. But using this room for manoeuvre transforms the very function of local administrators. With uniform rules, their duty was simply to comply. Now they have the responsibility to work with citizens to find the best way of translating the guiding principles into local rules. These local standards are a new type of common to be established and managed at the finest level".*

Finally, we need to devise incentive mechanisms that encourage the sharing of reliable data. Training stakeholders in the sharing of quality data should also be considered. Behind these questions lies the need to rethink the governance of the new digital services being created in cities today, often by private players reluctant to share data.

7 Conclusion

At a time when new models of data exchange are being developed, we have attempted to demonstrate that sharing rules based on the resources of IT and law offer a glimpse of better exchange practices. These are based on a greater emphasis on metadata and traceability mechanisms, as well as on default common management of data between the various players in the ecosystem. By following the path of commons-based approaches, open data, and open source, it becomes possible to ensure that data is shared more openly and transparently.

Based on these principles, there are still many elements that need to be clarified. For example, it is up to the various players to choose the type of contract, license, or charter that will enable them to agree on these sharing rules and to adapt them on a case-by-case basis according to the use cases and needs

identified. Among these rules, members will be able to define the type of sanction to be applied in the event of non-compliance with the founding principles, such as the impossibility for a sanctioned player to reuse the available databases. These new exchange models are likely to take many forms, depending on the needs of each group of public or private players.

What is certain, however, is that it is essential to assess the new risks induced by these new ways of sharing information. The 21st century is the advent of the information society, but without information, or with unreliable information, the digital revolution will not be as successful as we had hoped.

Acknowledgments. We would like to thank the organizers of the « Convergences du Droit et du Numérique » (https://cdn.u-bordeaux.fr/), an event which aims to provide a common framework for reflection for lawyers, computer scientists, sociologists, historians and digital players, by actively encouraging cross-disciplinary work. Indeed, the « digital revolution », resulting from the massive spread of digital technologies throughout society, is overturning organizational and economic models, as well as legal categories.

References

1. Berners-Lee, T., Hendler, J., Lassila, O.: The semantic web. Scientific american **284**(5), 34–43 (2001)
2. Calame, P., Ziaka, Y.: Les biens communs et l'éthique de la responsabilité. Éthique publique **17**(2) (09 2015). https://doi.org/10.4000/ethiquepublique.2306
3. Clément-Fontaine, M., de Rosnay, M.D., Jullien, N., Zimmermann, J.B.: Communs numériques: une nouvelle forme d'action collective ? Terminal (130) (2021). https://doi.org/10.4000/terminal.7509, http://journals.openedition.org/terminal/7509
4. Coriat, B.: Communs fonciers, communs intellectuels. Comment définir un commun ? Paris, Les Liens qui libèrent (2015)
5. Hardin, G.: The Tragedy of the Commons. Science (1968)
6. Horrocks, Ian, Patel-Schneider, F, P., Boley, Harold, Tabet, S., Said, Grossof, Grosof, B., Dean, M., Mike: SWRL: A Semantic Web rule language combining OWL and RuleML. W3C Subm **21** (01 2004)
7. Jarry-Lacombe, B., Bergère, J.M., Euvé, F., Tardieu, H.: For a Digital Technology in the Service of the Common Good, chap. 7 (Digital Commons ?), pp. 161–167. Odile Jacob (2022)
8. Kalam, A., Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C., Trouessin, G.: Organization based access control. In: Proceedings of 4th IEEE POLICY. pp. 120–131 (2003). https://doi.org/10.1109/POLICY.2003.1206966
9. Laamech, N.: Towards a secure data sharing management approach for IoT environments. Ph.D. thesis, UPPA - ED211 Sciences Exactes et leurs Applications (9 2024)
10. Laamech, N., Munier, M., Pham, C.: IdSM-O: An IoT Data Sharing Management Ontology for Data Governance. In: Proceedings of the 14th International Conference on Management of Digital EcoSystems. p. 88–95. MEDES '22, Assoc. for Computing Machinery, NY, USA (2022). https://doi.org/10.1145/3508397.3564825

11. Laamech, N., Munier, M., Pham, C.: Translating Usage Control Policies to Semantic Rules: A Model using OrBAC and SWRL. Procedia Computer Science **225**, 1881–1890 (2023). https://doi.org/https://doi.org/10.1016/j.procs.2023.10.178, kES 2023
12. Middleton, S.E., De Roure, D.C., Shadbolt, N.R.: Capturing knowledge of user preferences: ontologies in recommender systems. In: Proceedings of the 1st international conference on Knowledge capture. pp. 100–107 (2001)
13. Moreau, L., Groth, P.: Provenance: an introduction to PROV. Springer Nature (2022)
14. Ostrom, E.: Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge, Cambridge University Press (1990)
15. Ostrom, V., Ostrom, E.: Public goods and public choices. Alternatives for Delivering Public Services (1977)
16. Park, J., Sandhu, R.: Towards usage control models: beyond traditional access control. In: Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies. p. 57–64. SACMAT '02, Association for Computing Machinery, New York, NY, USA (2002). https://doi.org/10.1145/507711.507722
17. Park, J., Sandhu, R.: The UCONABC usage control model. ACM Trans. Inf. Syst. Secur. **7**(1), 128–174 (feb 2004). https://doi.org/10.1145/984334.984339
18. Rifkin, J.: la Nouvelle Société du coût marginal zéro. Paris, Les Liens qui libèrent (2014)
19. de Rosnay, M.D.: From Open access to digital commons goods. Paris Nanterre University (2021)
20. Samarati, P., de Vimercati, S.C.: Access control: Policies, models, and mechanisms. In: International school on foundations of security analysis and design, pp. 137–196. Springer (2000)
21. Sapra, R., Dhaliwal, P.: Blockchain: The new era of Technology. In: 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC). pp. 495–499 (2018). https://doi.org/10.1109/PDGC.2018.8745811
22. Weber, S.: The success of open source. Cambridge, Cambridge University Press (2004)