Digital Democracy and Data Commons pilot:

kick off workshop notes

Data

Place & Date: Fabra i Coats, 18th October

Time: 1:30pm-2:45pm

Participants (registered/attended): 50/35

Facilitators: Tecnopolítica IN3/UOC & Dimmons IN3/UOC

Table experts: Ideas for Change (Governance track); Nexa/POLITO (Legal track); CNRS (Economic track).

1. AIMS AND DESCRIPTION OF THE SESSION

The workshop consisted in a **collaborative diagnosis session within** the **Digital Democracy and Data Commons pilot**. It served as an **initial discovery and diagnosis phase** for an online-offline process that will last until April 1st, as well as for related sessions at the **Sharing Cities Summit** and beyond.

The main aim was to elaborate a collaborative diagnostic around problematics in three specific areas (which also will help to articulate debates in the DDDC website): data governance, data economics, and data regulations. This diagnostic will be the first element of a transdisciplinary and collaborative research process that will result (among other things) in a **DECODE participatory white paper.**

For this, the setting of the session consisted in an open space with **three main tracks or areas of interest on dedicated tables**. For each topic, the state of the art was reflected on topic cards, summarised in a way that DECODE experts guided participants through it. For example, in the case of the economic track, DECODE experts provided a summary of the existing paradigms and problems around the data economy, from the corporate data extractivism typical of Facebook to the public open data or the data commons paradigms. Then, participants were able to **first identify additional issues or missing areas in the structural/paradigmatic map** presented by the DECODE experts.
Then, the main interaction of the session was for participants to identify (and cluster around each of those paradigms) both **challenges and opportunities** they considered relevant (via sticky notes of different colours). In this way, at the end of the session we had a preliminary **map of the state of the art and some relevant issues** to work on later in the participatory process, online or offline.

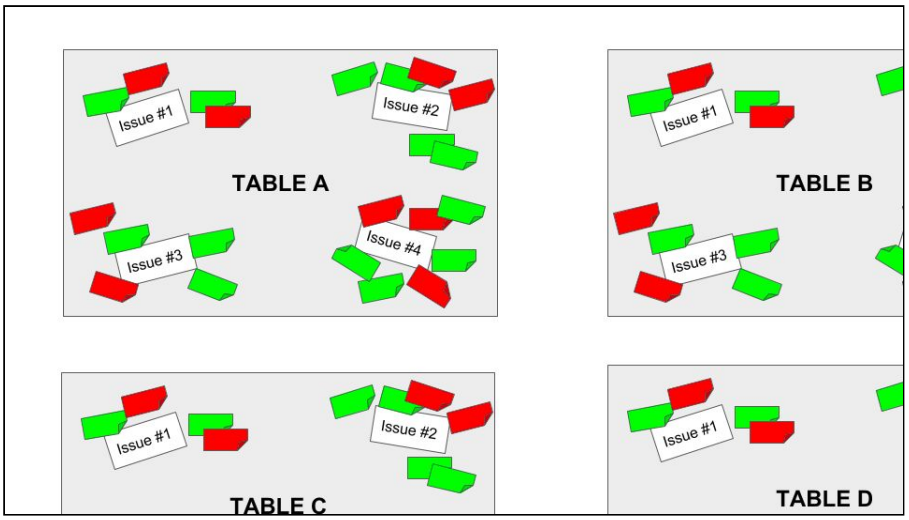


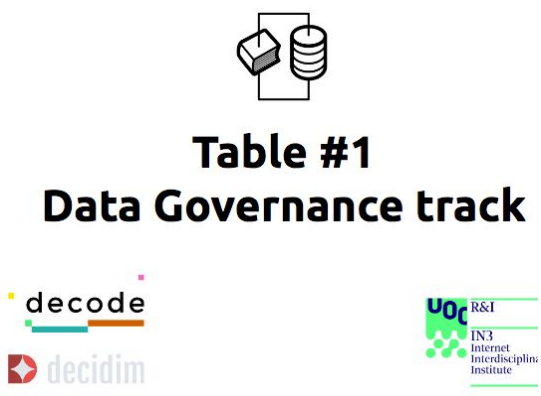
Diagram of the tables at the end of the session

Participants are invited to **follow up the discussions and process via the DDDC online platform** joining the designated survey and participation process defined there. Additionally, the concrete schedule of **specific sessions for each of the 4 topics during the Sharing Cities event** (12-15 November) will be presented as follow up session with interested participants, but also open to visitors of the Smart City Expo during those days.

2. RESULTS

Now, we present some of the results of the sessions, divided in the three tracks.

Data Governance track - Table moderated by Mara Balestrini (Ideas for Change) & Antonio Calleja (Tecnopolítica)



Introduction

Today, the issue of who controls data (specially, personal data) is a crucial one in the digital society and economy. The current answer is: primarily, big corporations. People have little to say on what data is gathered, for how long or for what purposes. This disempowerment of citizens opens the gates to situations that go from surveillance (people being tracked throughout the day) and data exploitation (people providing free data that, after aggregation, may be worth more than the free services they receive in return) to social influence or even engineering (data used to shape what people see or do on the internet).

Data is power, and the debate around governance concerns how to control it, specially, the control over its production, management and use, including their conditions and their consequences. In this track the approach focuses on institutions and collective practices, before or beyond the economic models that make them sustainable (touched upon in the economic track) or the regulations that define some of their boundaries (touched upon in the legal track).

Different governance paradigms can be found today. The preeminent model within the private sector is that of “data extractivism” or “exploitation”, in which corporations (led by its owners and represented by their workers) define, through legal, social and technological tools, the terms of extraction, management and use of data. People have little say about it. In a still nascent legal environment, the situation frequently is one of “take it or leave it”. They set up the rules of the game. Facebook is a prime example of this.

A second paradigm within the private sector is that of digital services. Companies offer data storage services. Third parties can access data only with Maria’s consent. The storing company serves as a legally and technologically safe environment where third parties can offer services or ask for data and where people can receive such offers and allow access. Made of Gene is an example of this.

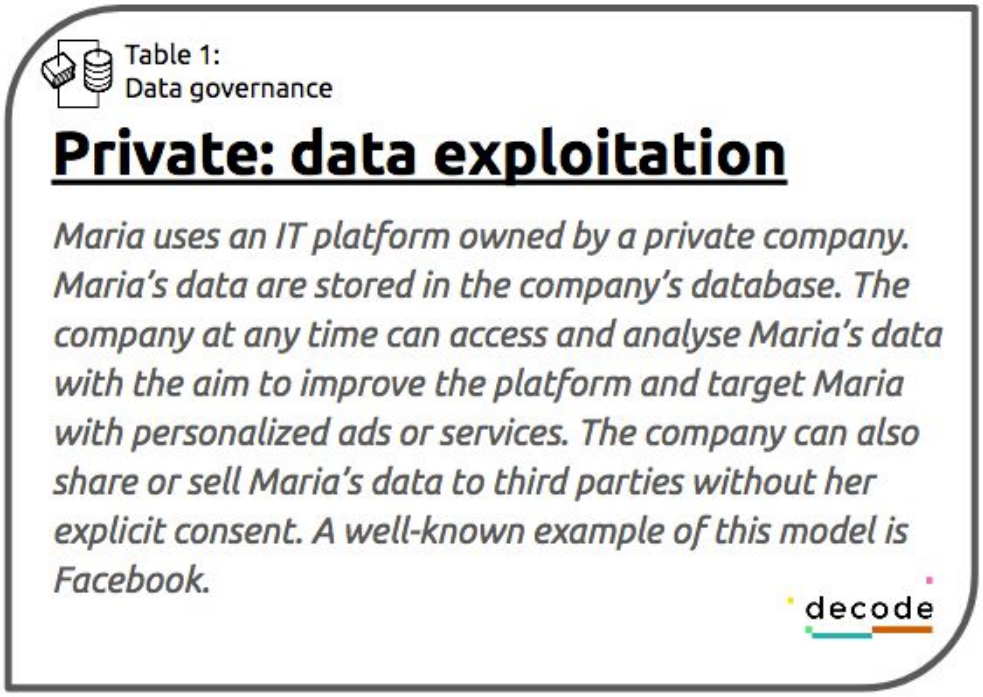
A third paradigm within the private sector is brokering. Here the two key actors are individuals and data brokers. The individual gains control over their data in various apps and services and can decide to sell them (or give some form of control) to brokers that help to find actors that will to pay for those data. DataCoup is an example of this model.

The fourth paradigm is that of public control. Here public administrations may use a person’s data to develop public policies, improve service provision or conduct research. The individual is informed and can opt-out. The benefit is public. Care.data is an example of this.

Within the cooperative or commons sector, we find two paradigms. The first is the cooperative one. Here members share their data with a cooperative under specified conditions. They control the cooperative at various levels, and take collective decisions around aspects such as the use of the aggregated data (f.i.: whether they are shared with a given company), and share the benefits resulting from their exploitation. Salus.coop is an example of this.

The second paradigm is that of community commons. In this case, members share their data with a community organization under specified conditions. They control the organization at all levels, take collective decisions around the use of the aggregated data and use it for generating collective goods for the community itself (f.i.: moving forward a given political agenda). Making sense is an example of this.
Each of these models have various potential benefits and risks. In the session, we collectively mapped them.

Expert cards and debate points



Opportunities. Competitive marketplace; big good results; customized recommendation; polished UX.
A number of opportunities where listed for the data exploitation paradigm. The first is the creation of a marketplace for other businesses using the aggregated data that, precisely for the size (this model is most frequently deployed by big corporations), gains value. In line with this, if good purposes were designed for these big

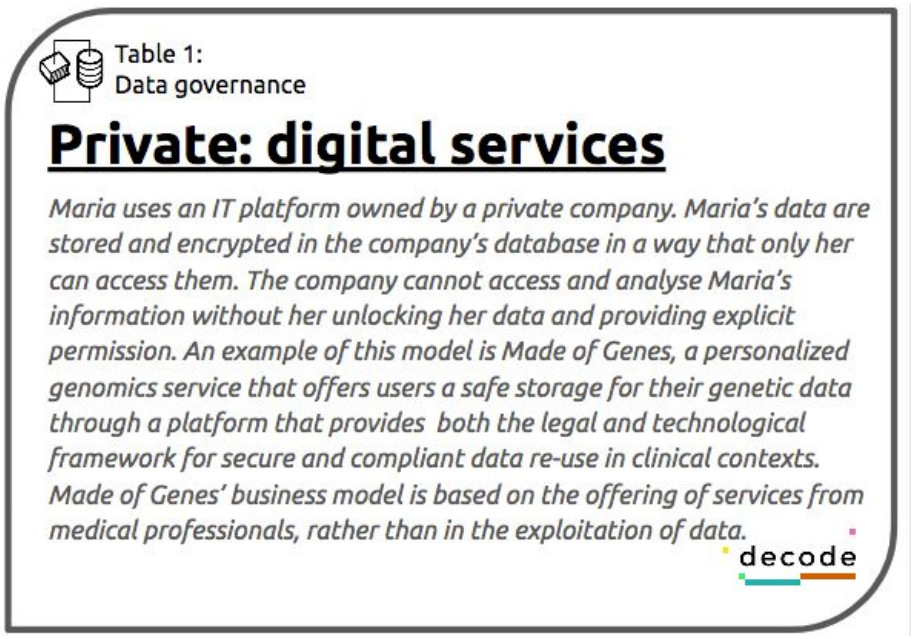
databases, big goods may result, since they provide more capacity for action. A mentioned example of this are customized recommendations on digital platforms. Furthermore, big platforms have a polished UX, which allows a smoother service based on data, or even data extraction.

Risks, Behavior modification, slided information, loss of control, capital concentration and exploitation, surveillance.

On the side of risks, one of the key ones noticed was behavior modification using audience segmentation. Related to this, the issue of slided information, as seen in the recent debates on fake news, generated by close information circuits resulting from data mining use. Loss of control of data to the hands of corporations was a mentioned risk. Capital and power concentration into big monopolies, hand in hand with user dispossession was included as a risk. This concentration relies and reinforces real o potential surveillance.

Other. People, more data means more aggregated value and more attraction for hackers.

As ambiguous effects, two were mentioned. More people into one platform means stronger network effects. In relation to this, here data gains more aggregated value too, while also becoming more attractive to hackers.



Opportunities. Data for clinical and medical analysis for health services; personalized and collective health services; community data and diagnosis for complex diagnoses.

Participants registered a number of opportunities deriving from this paradigm. The first is to have these data used in clinical and medical analysis for health services. A related one, the possibility of benefiting from personalized health services, going beyond the current model of generic medicine, preeminent both in the public and the private sector. Simultaneously, sharing would allow to improve collective treatments too. Aggregated community data would further help with complex diagnoses. Safety and personal control over data was stressed too. The existence of a marketplace and its impact in service improvement was also mentioned.

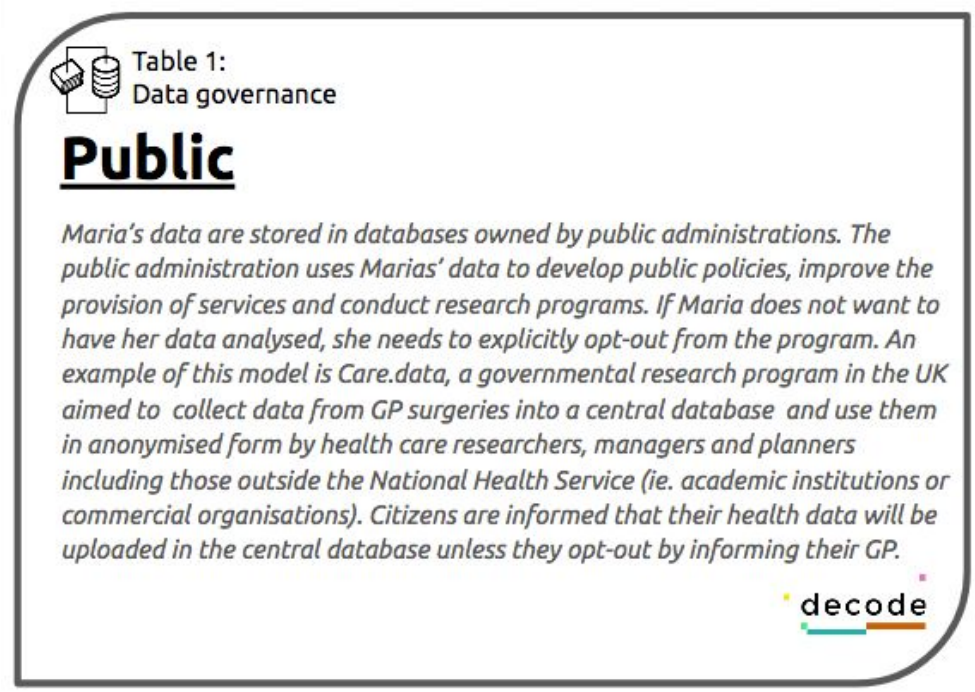
Risks: preeminence of profit in medicine; unauthorized research; privacy violations; data security breaches.

Among the risks, several were noticed. The first was that of the preeminence of the profit motive in the provision of health insurances and services. Another point raised was the potential use of data for unauthorized research, profit driven or not.

Similarly, concerns regarding privacy violations and data security breaches were listed.

Other: integration with international databases for mapping risks.

In other considerations, participants pointed to the potential integration of international public and private databases for mapping and identifying risk conditions.



Opportunities. Data public analysis; Big Sample; Prediction; Smart City well managed.

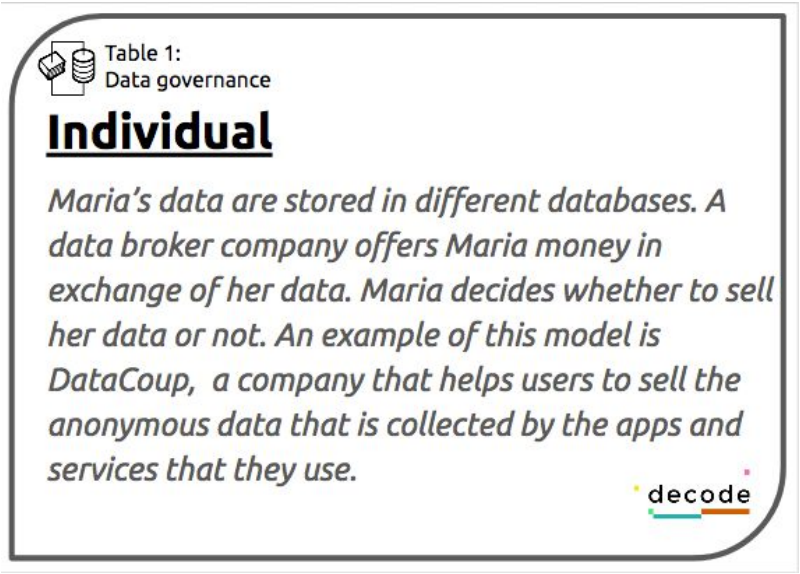
Several opportunities were noticed. The first was the elaboration of open, public analyses based on open data, serving as a ground for more research and outputs. A related benefit was the constitution of a big database that would provide more aggregated value. On the basis of this big database, prediction also comes closer as a possibility. Finally, all of these factors combined can bring about a well managed smart city.

Risks. Loss of data; Opt-out as dark pattern; Private companies in control of results and central database; non-usable data.

As a counterpoint, various risks were listed. The first is the risk of data losses, either by breaches, by inappropriate data formats (non-usable), or by lack of information. On this last point, the possible emergence of an “opt-out” culture may bring about dark patterns in databases and associated research, biasing the samples. Fears were also raised that corporations may be the actors controlling these databases, especially the ones benefiting the most from their exploitation and results; they may also become so by playing the role of providers maintaining the infrastructure. The existence of a central database, if that is the model, may have its own problems, including security.

Other. Encryption needed; no central database; use blockchain; open data are usually non usable.

Among the other considerations raised around this paradigm. There was an stress on the need of strongly encrypting the data controlled by public administrations. Similarly, there was a fear around central databases, that could expose the data of many people if hacked by external actors or misused by the administration. A point was also raised about the possibilities of using blockchain for turning various aspects of data management transparent.



Opportunities. Data monetization; data marketplace; user control; decentralization.

Among the opportunities, data monetization was the first pointed. Against the exploitation model, preeminent today, under a brokering model people will be able to extract an explicit economic benefit from their data. This may bring about a data marketplace where multiple actors can operate with data, potentially improving the way data is valued and, perhaps, used, against the exploitation model. Another opportunity noticed concerned the decentralization of data management, preventing the centralization and concentration of power over (and through) personal and, more broadly, social data. This paradigm was also associated with a greater user control. People can decide what to do with their data, both in negative terms (preventing other actors to gather and exploit it) and in positive ones (defining to what actors they give their data).

Risks. Governance problems; business driven choices; individual data sent to many companies; little value; little bargaining power.

Several were the risks noticed around this paradigm. The first is governance problems resulting from decentralization. More actors means, potentially, less accountability and trackability of data transactions. Individual data sent to many companies may also multiply the number of actors being able to surveil and operate over individuals. It also multiplies potential security breaches, as ensuring security is expensive. Another risk noticed was a potential business-turn in people's consideration of data, obliterating other values and purposes such as collective benefits. Fragmentation of databases may also imply a reduction in the value of data, as much of it comes out of its aggregation and the processing based on this. Furthermore, a potential loss of bargaining power for actors was pointed out as a potential risk. An individual trying to sell her data may have few ways to negotiate either price or rights.

Opportunities. People can collectively bargain and profit (individual data has little value); smaller = more control; access; + private and collective gain.

Small and medium sized organizations such as cooperatives, which also count with democratic governance mechanisms, mean people retain more personal and collective control over their data. As data is aggregated, value rises in comparison to the brokering individual model. Furthermore, people can collectively bargain with other actors, increasing the personal and collective benefits (both profit and common good) resulting from data production. The cooperative also helps with issues of access, also to discourses and practices of data management.

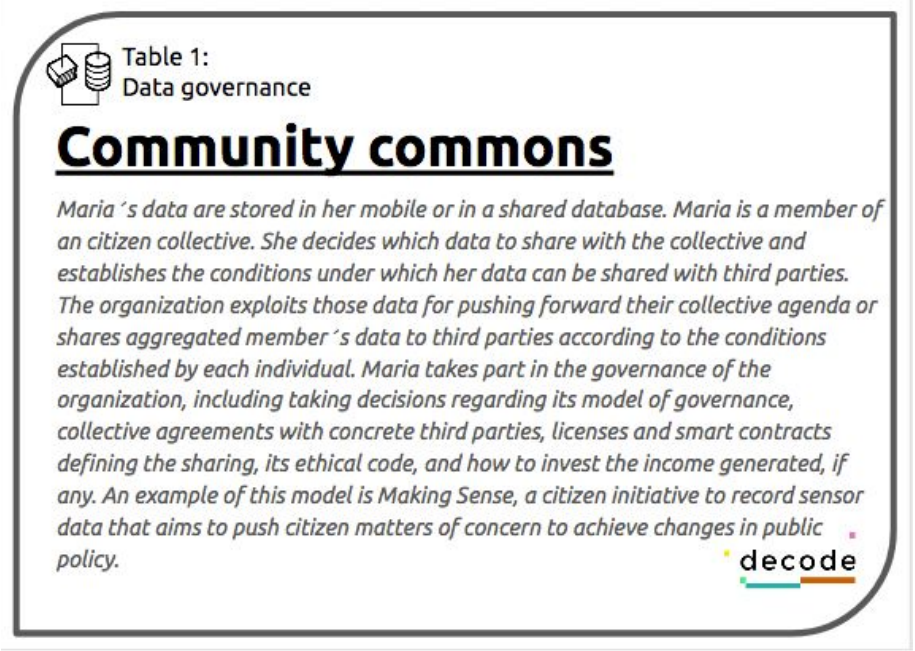
Risk. CEO power; risk of hacking; governance and collectives; humans can be corrupted; Privacy.

One risk noticed by various actors was the risk to privacy resulting from the smaller data samples and the possibility of de-anonymization. In a similar line, risks of hacking resulting from smaller organizations with smaller security measures. Risks were also raised concerning the potential accumulation of power by CEOs or cooperative directives positional power resulting from their role and justified by technical expertise, economic and efficient/fast performance, unless there are strong mechanisms of power redistribution. Humans can be corrupted, so strong

mechanisms of accountability and bottom up control will b required. This, however, is complex, horizontal forms of governance of collectives frequently require more resources to make decisions, are less efficient and fast.

Other. Smaller and less attractive for hackers.

As other considerations, the debate focused on how smaller databases have both less value but also less attractive for hackers.



Opportunities: citizen empowerment.

Having citizen organizations on this field is a good way of mobilizing people and promote them taking an active role in public life, around data and beyond. In this case, benefits revert on the communities themselves. Strong democratic control over the organization and perhaps the infrastructures is also a gain.

Risks: effort; governance problems.

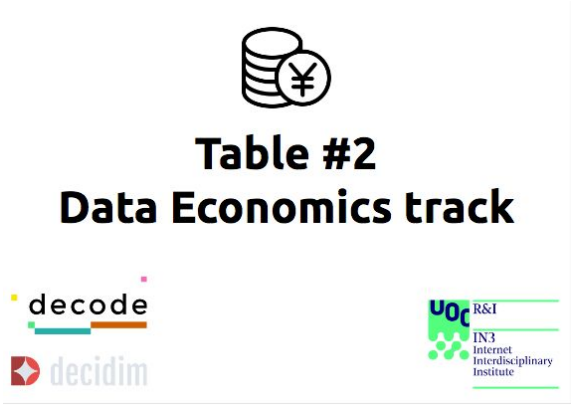
Its complicated and a lot of effort from the end user is needed. It is difficult to define ethical code and specifical contracts.

Other: It is also required to define methods and governance rules to guarantee rights.

Shared view

There is no absolute right choice, however, there is a feeling that sovereingty and the collective dimension (and benefits) are important to move beyond the exploitation model. People must be able to make informed decisions and is necessary to build ways to facilitate such choice. Risk minimization is also something to look after. Different models for value creation have their role.

Data Economics track - Table moderated by Giulia Rocchi (CNRS) & Ricard Espelt (Dimmons)



Introduction

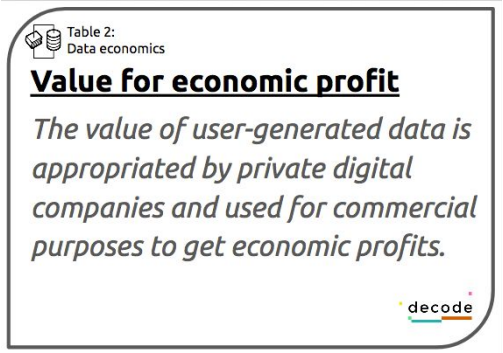
Regarding economy, we can distinguish three major current economic models around data:

1. **Profit-driven models**, namely those of private digital companies (e.g. Google, Facebook, Uber, Airbnb, Amazon) that appropriate user-generated data and exploit it for commercial purposes (such as targeted advertising or improvement of the service offered), and those of companies known as 'data brokers', that collect (and then cluster and sell) data from other sources rather than from consumers first hand.

2. **Public value-driven models**, based on a 'data open for all' logic promoted either by governments to strengthen innovation and transparency (e.g. Open Data BCN), or by private or public entities either to pool previously unrelated dataset and get unprecedented insights out of it (e.g. PRIDE, whose goal is the implementation of a

platform for gathering, handling and visualising energy data from diverse sources) or to contribute to a cause of public interest (e.g. Inside Airbnb).

3. **Common-driven models**, where data is considered as a not merchantable resource that is produced, governed and used by a given community to feed either the commons itself or nurture commons-oriented networks and models (e.g. OpenStreetMap).



Opportunities: constantly updated, fastest and well-configured digital services

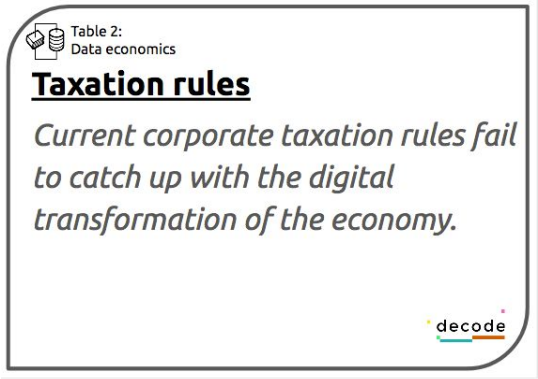
Applications and services offered by dominant tech companies are usually full-optional, customizable and regularly improved thanks precisely to the regular enrichment of the information the users give them by interacting with their services, as well as to substantial Research and Development investments.

Risks: privacy, data protection, and antitrust violation

All the most well-known tech giants have been involved in data misuse/breach scandals and anti-competitive proceedings. However, being globally the leading companies in terms of market value (which results in great lobbying powers), the inference that monetary sanctions or regulative interventions are able to correct monopoly and privacy protection issues is questionable.

Other: Tech giants' design is inherently aimed at making profit rather than directed to pursue public/citizens' good

Small but promising competitors with innovative, social value-oriented models frequently end up getting acquired.



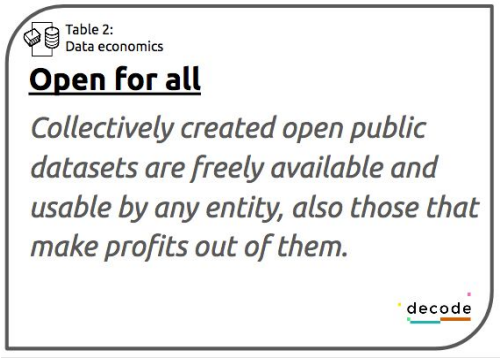
Opportunities: taxes could be collected at local level and the money raised could be used to support alternative initiatives (privacy-aware and oriented to the local collective good)

A possible digital taxation model could be that of a locally collected levy on the share of tech companies' revenue that relies on user-generated data exploitation, re-allocating the funds raised to sustain projects precisely aimed at building alternatives both to capitalist platforms and to the traditional - uncritically focused on technological advancements - smart city's approach.

Risks: lack of power to ensure worldwide policies that ensure that the benefit of information is for all

Any try to implement a global regime as regards the taxation of digital businesses (form the first attempts in the 1990s to the legislative proposals presented in March 2018 by the European Commission) looks set to be opposed, due to conflicting political agendas and national-driven interests.

Other: incremented economic and social inequality

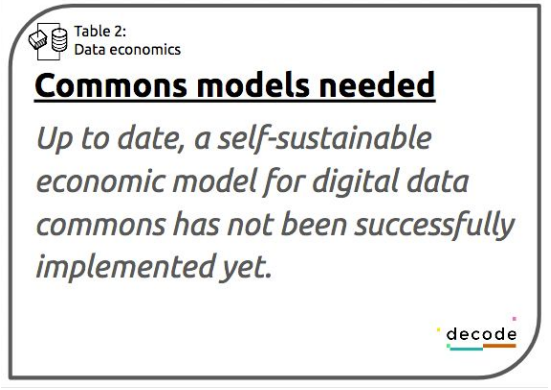


Opportunities: Open data can unlock new social value and enable services that falls out of tech giants' interests

Open data can generate a new stadium of opportunities for public administrations and social organizations in order to provide citizen-centric services. For instance, the Finnish 'Kannattaako kauppa' provides insights on the price development of real estate in the future, making it easy to compare houses and neighbourhoods by price and population. The estimates are available as an interactive visualisation and the model is available on GitHub.

Risks: Bad actors (spammers, Russian trolls, predatory financial & tech companies) can abuse of open data

The fact that data can be accessed, used and redistributed by anyone means that it may be private actors endowed with economic and knowledge capital who appropriate it and benefit the most out of its commercial, rarely transparent, and even risky exploitation, in stark opposition to the Open Data philosophy.



Opportunities:

- Get sources from public administration as an alternative to combine different models of funding

In an ever-increasing digitally soaked society public administrations have the greatest interest in investing for the protection of their autonomy in political decision-making processes, their financial independence and their technological sovereignty against the digital economy oligopolies.

- Take advantage of tokens as an incentive

As in the case of projects such as 'La'Zooz' (a decentralized, community-run, ride-sharing application), common-based models' economic sustainability may be reached using blockchain-based virtual currencies to remunerate people who participate in the project (whether developers or users) in accordance with their contributions' weigh.

Risks:

- Funding from big tech companies and loose independence

Frequently, talented minds are detected, financed and finally recruited by dominant digital companies. As a way of example, over the course of little more than a decade Facebook has acquired 65 companies (inclusive of assets and talents), spending billions of dollars.

- Common data used by tech giants to make profit

As in the case of Open Data models, absent a proper legal instrument forbidding commercial exploitation, also common data suffers the risk of being used for purposes far from those it has been conceived to accomplish.

Other: Hard to have a governing body that reacts fast to problems. The technological advancements' speed is inversely proportional to that characterizing normative actions aimed at tackling and discipline them, especially when a centralized procedure (at State-level) is needed. Following the process of 'regionalization' and consequent strengthening of the principle of subsidiarity that has interested several European countries in response to the crisis of the nation-state, local and regional realities could claim strong forms of autonomy with regard to particular cutting-edge sectors.

Shared view

A shared point among participants in this table was to notice the risk of appropriation of the common´s economic space by private companies and corporations. On the other hand, there was a key point risen: how to scale up the common´s model.

Data Regulations track - Table moderated by Marco Ciurcina (Polito) & Andreu Belsunces (Tecnopolítica)

Introduction

Europe is a reference on data regulation and is setting an example for other countries and regions. GDPR was an important step towards governmental privacy protection, subject empowerment, awareness around privacity among private and public, even more after the massive GDPR "spam" this summer. In a broader sense, GDPR is a new protection from the monopolistic trends of surveillance capitalism.

Generally, Data Law models regulate personal data in 3 axis: as a fundamental right, as an economic asset, as a means of control.

GDPR is shaking the digital word providing for new rights for data subjects and new obligations for personal data controllers and processors that empower the data subject more than in the past.

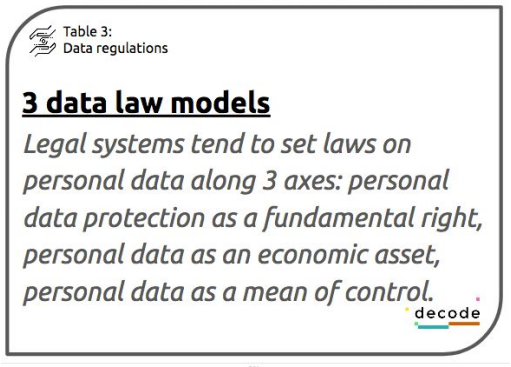
GDPR does not provide for an unlimited power for the data subject: GDPR provides for exceptions (processing by a natural person for purely personal activity, processing by competent authorities for the prevention of threats to public security, etc.) and limited control for the data subject on her personal data (no right to prohibit data export in all circumstances, no right to prohibit certain uses, etc.).

Free licenses are a consolidated legal model apt to foster the creation of digital commons including personal data, nevertheless, today, free licenses applicable to data do not deal with obligations provided by privacy laws protecting personal data. Free licenses consist in unilateral legal acts (acts made by the creator of the artifact addressed to the users).

The opportunities are related to new technologies as Distributed Ledger Technologies (Blockchain), which offer a more complex protection in terms licenses, users and differents contracts, so enrich further regulation possibilities like consent right to erasure, the possibility of portability right and in general a more granular management of personal data.

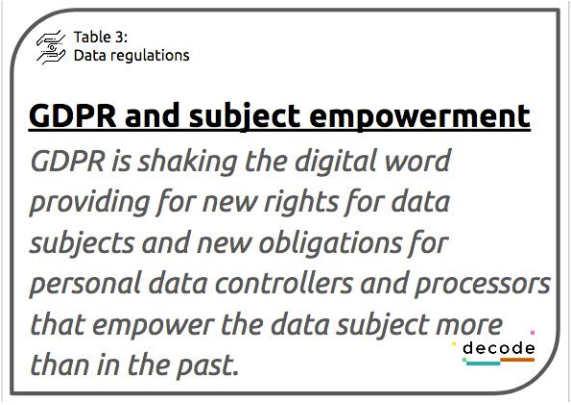
In general, the risks have been related to targeting people and to the question of who really affects regulations like GDPR (too much regulation might be detrimental for entrepreneurial ecosystems and benefits larger corporations that can adapt to new regulations)

Some doubts arise when talking about regulating the data used and produced by AI systems, possibilities have strong and legal data regulation, tracking of users agreements.



Other: which are the limits of data regulation?; How users can keep track of their agreements? How to regulate data processing in black boxed systems, specially AI?

There are different paradigms in personal data regulation across the world: as a right, as an economic asset, and as a mean of control. But what are their limits? How far can these norms be enforced, especially across legal jurisdictions? Also, how can users manage the agreements they come to with different actors on the digital sphere? How can they keep track of all of them and ensure they are being respected? Furthermore the issue of how to make compatible data processing rules with black boxed systems such as AI, in which the precise operations performed by the algorithmic machine are not transparent, was discussed too. No conclusions were reached on this regard.



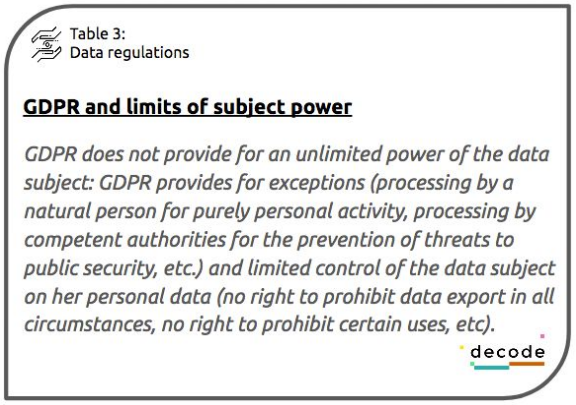
Opportunities: less monopolistic digital economy; a way to protect citizens; portability right; create awareness among companies and public administration.

Several opportunities were diagnosed as resulting from the establishment of GDPR. The first is the advance towards a less monopolistic digital economy, with incentives pushing against the accumulation, control and use of big databases by a few big

players. It also represents an advance towards citizen protection. It enshrines a number of rights, especially the right to privacy. Furthermore, it also introduces new notions such as data portability, which grants citizens further freedom for operating across and beyond digital platforms. Finally, it promotes a new awareness of this issue among companies and public administrations, as well as citizens.

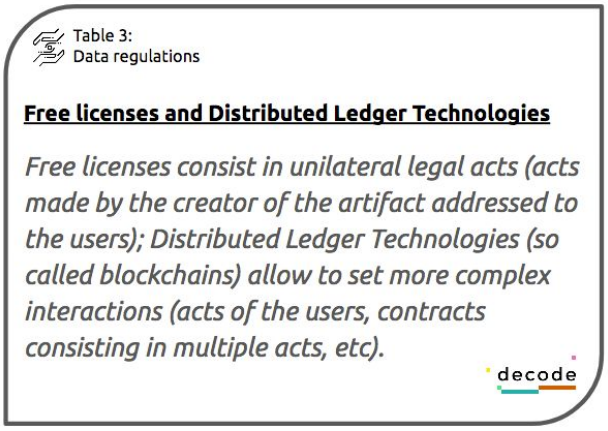
Risks: excessive regulation; Consent dynamic `art 13 & 14 transparency.
Two risks were diagnosed. One is the risk of excessive regulation and normatives that damage the entrepreneurial ecosystem, while benefiting big corporations. Also, consent dynamics may become trickier and more complex, and transparency may not fare better.

Other: Government limits GDPR in specific low level of risk, like in areas such as health.



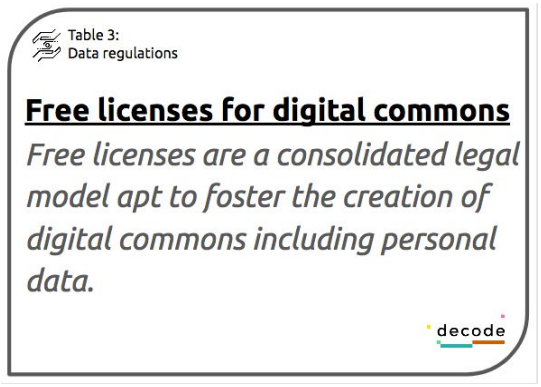
Other: GDPR spam; differences between personal and sensitive data; city regulations.
With regard to GDPR and the limits of subject power, several points were raised. After the massive GDPR “spam” this summer has there been a increasing about data awareness? If not, the power of the subject GDPR tries to enshrine may be

limited; power without empowerment and awareness is much less so. Another key consideration raise concerned the need of differentiating personal data and sensitive data, they are partially overlapping sets, with the former being broader. Finally, the question of whether cities can or should carry on data regulations was discussed.



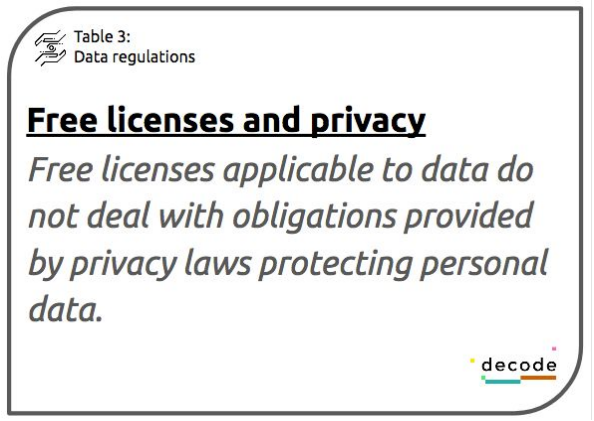
Opportunities: different arrangements for different situations; consent right to erasure; besides smart contracts; Blockchain preserves the usage of data creating new limits and possibilities of regulation

A number of opportunities were explored with regard to free licenses and smart contracts, which are two different types of tools that can be used for managing personal and other types of data. The they cover different arrangements and situations. In general, smart contracts may cover more situations and actions on the side of the actors contributing to a given database. They may better serve to ensure both consent while posing new questions around the right to erasure. Blockchains can serve to register the usage of data in a much more transparent and granular way. However, because of their orientation to permanent and open registration of operations, they pose the challenge to rights such as the right to forgetting.



Risks: Asian tech giants are in breach of the rules; Viral aspect for personal data.

Several risks were noticed with regard to free licenses. Free licenses have limits that concern the respect of the rules they try to set. For instance, the case was posed of how asian tech giants may not be respecting them. Application of their legal terms may be contingent on the primary territorial jurisdiction under which a given corporation operates, in cases such as China the respect for privacy may be lower than in Europe. A second risk, concerning the virality of free licenses, may imply a loss of control over the use of personal data after release, which the implications to rights such as privacy or forgetting.



Opportunities: Design new family of licenses; Any opportunity behind that?

The limits of current free licenses pose the need and the challenge of creating a new generation of licenses, which are more GDPR adapted. This opens an opportunity for actors to set new terms for the use of data, better adapted to the current sociotechnological landscape.

Risk: targeting people

Insofar as the situation remains as it is, people may be targeted on the bases of use of personal data (even anonymized) under free licenses. This poses a potential conflict between existing models of free licenses and privacy.

Shared view

A first intuition was that GDPR is not a solution for every problem. It is an opportunity for Europe to lead in this field and grant more rights to citizens. Data portability is a key opportunity and part of a strategy for citizen control over personal data. Finally, against free licenses, smart contracts and blockchain represent an opportunity because free licenses are not dealing with privacy issues, so the latter two provide a much more granular way of managing data.