DECODE DDDC pilot: a techno-legal perspective
Fostering digital commons including personal data

Executive summary

This report provides a techno-legal diagnosys of the DECODE DDDC pilot in light of the goal of the DECODE project of fostering digital commons including personal data.

In short, these are the main findings of this report.

1. Legal systems tend to set laws on personal data along 3 axes: personal data protection as a fundamental right, personal data as an economic asset, personal data as a mean of control.
2. 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.
3. 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.).
4. Free licenses are a consolidated legal model apt to foster the creation of digital commons including personal data.
5. Free licenses applicable to data do not deal with obligations provided by privacy laws protecting personal data.
6. Free licenses consist in unilateral legal acts (acts made by the creator of the artifact addressed to the users); Distributed Ledger Technologies (so called blockchains) allow to set more complex interactions (acts of the users, contracts consisting in multiple acts, etc.).

1. Legal systems and personal data protection

Generally speaking, the different legal systems include laws that deal with personal data for 3 different purposes.

Sometimes personal data are subject to legal acts that have the purpose of protecting the data subject assuming that personal data protection is a fundamental right.

As way of example, the GDPR is based on this principle.

In other cases, personal data (data more in general) are regulated as an economic asset, subject to protection in favor of the right holder.

As way of example, personal data could be subject to rights in favor of third parties (not being the data subject) when they are protected as trade secrets and/or, when they are arranged in databases and protected by copyright or by the *sui generis* right on databases.

Finally, laws regulating personal data could focus on the potential of control that could be achieved accessing to such data.

As way of example, different legislations enact laws that allow intelligence services to process personal data to prevent threats to public security, sometimes allowing them to perform mass surveillance practices, and/or the creation of “back doors”.

2. GDPR: more power to the data subject

Since few months Regulation 2016/679 (General Data Protection Regulation) entered into force.

EU citizens and companies all over the word are learning to deal with this new legislation providing for an enhanced protection for personal data.

According to Article 4(1), point 1, of GDPR, *‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’),* who is the identified or identifiable natural person which the data is referring to.

The same Article adds that *An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number,* *location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*[1].

GDPR provides for strong rights protecting personal data.

Among others, it is worth mentioning the following rights of the data subject:

- right of access by the data subject according to Article 15(1) of GDPR;
- right to rectification according to Article 16(1) of GDPR;
- right to erasure (or 'right to be forgotten') according to Article 17 of GDPR;
- right to restriction of processing according to Article 18 of GDPR;
- right of notification by the controller about rectification or erasure of personal data or restriction of processing according to Article 19 of GDPR;
- right to data portability according to Article 20(1) of GDPR;
- right to object according to Article 21(1) of GDPR;
- right to automated individual decision-making, including profiling according to Article 22 of GDPR.

The GDPR also provides for strong obligations for the controller[2] and the processor[3]:

1. obligation for the controller to comply with the principles provided by Article 5 of GDPR and with the conditions for a lawful processing according to Articles 6-10 of GDPR (i.e., consent by the data subject);
2. obligation for the controller to inform the data subject about the data processing according to Articles 12, 13 and 14 of GDPR;
3. obligation for the controller to implement technical and organizational measures that protect personal data by design and by default according to Article 25 of GDPR;
4. obligation for the controller to make agreements with processors according to Article 28 of the GDPR and with joint controllers according to Article 26 of GDPR;
5. obligation for the controller and the processor to provide instructions to the persons acting under its authority according to Article 29 of GDPR;
6. obligation for the controller and the processor to implement technical and organizational measures that ensure security according to Article 32 of GDPR
7. obligation for the controller and the processor to keep a record of the processing according to Article 30 of GDPR;
8. obligation for the controller to notify the supervisory authority according to Article 33 of GDPR and eventually communicate to the data subjects according to Article 34 of GDPR in case of data breach;
9. obligation for the controller to perform a data protection impact assessment according to Article 35 of GDPR and eventually a prior consultation of the supervisory authority according to Article 36 of GDPR;
10. obligation for the controller and the processor to designate a data protection officer according to Article 37 of GDPR;
11. obligations for the controller to transfer personal data to third countries or international organizations complying with the provisions of Articles 44-50 of GDPR.

3. GDPR: limits to the power of the data subject

Even if, up to date, GDPR provides for the strongest legal scheme protecting personal data, it is worth mentioning that there are exceptions to its applicability and that GDPR does not provide for an unlimited power for the data subject.

Concerning exceptions, Article 2(2) of GDPR provides that:

[1] This means, as way of example, that also email address and IP address shall be regarded as personal data.

[2] Article 4(1), points 7 of the GDPR states that data 'controller' is the *natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.*

[3] Article 4(1), point 8 of the GDPR states that data 'processor' is *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

This Regulation does not apply to the processing of personal data:
(a) in the course of an activity which falls outside the scope of Union law;
(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
(c) by a natural person in the course of a purely personal or household activity;
(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Concerning limits to the power of the data subject provided by the GDPR, the following examples could be considered:

- Article 3 of GDPR, under certain circumstances, does not apply to foreign entities which therefore are allowed to process personal data of people within EU without having to comply to the provision of the GDPR;
- Article 5(1) point. e) of the GDPR, under certain circumstances, allows storing personal data for further periods of time and for further purposes (not included in that for which the data was originally processed);
- Articles 13 and 14 of the GDPR do not require the provision of the details of the processors used by the controller for the processing;
- Articles 44-50 of GDPR, under certain circumstances, allow the controller to transfer personal data to third countries or international organizations even if the data subject did not provide her consent.

4. Free licenses and digital commons including personal data

Free software licenses emerged in the '80s as a legal tool to foster free software development and sharing: the free software communities were the first communities that shaped practices and tools (including legal tools) fostering the creation of digital commons.

In the early '80s the creation of free software was based on ethical reasons as a reaction to the emergence of the new paradigm of proprietary software. Richard Stallman says: "*My work on free software is motivated by an idealistic goal: spreading freedom and cooperation. I want to encourage free software to spread, replacing proprietary software that forbids cooperation, and thus make our society better*"[4].

Free software licenses played a key role in the growth of digital commons made of software.

Free software licenses are effective tools that allow solving problems typically handled by legal acts (laws, contracts, etc.). They allow to (a) eliminate uncertainty, (b) minimize transaction costs and (c) reallocate risk:

a) eliminate uncertainty: free software licenses are well known and recognized in the communities of free software developers and users (the fact that a program is available under the terms of a certain free software license makes it easy for the users to identify their rights and obligations);
b) minimize transaction costs: use of a free software license, instead of a license drafted *ad hoc*, reduces the costs associated with the adoption of the license;
c) reallocate risk: if a program is available under the terms of a free software license, the user can reasonably assume that the distributor did not deliberately include code in violation of third party rights.

In short, **free software licenses are efficient in building trust** among the people involved in the socio-technological systems that are built around free software projects and from the legal efficiency of the free software licenses follow social, economic, and other relevant effects.

More recently, other free licenses have been designed to foster the building of digital commons made up of creative works that are not software: the free software model has inspired attempts to

[4] See https://www.fsf.org/licensing/essays/pragmatic.html.

reproduce its dynamics in other areas of human activity and has led to the creation of new licenses for digital commons made of non-software works (newspapers, books, music, videos, databases, electronic designs, etc.).

Among these attempts, the case of the Creative Commons Public Licenses certainly deserves to be mentioned: although it was not the first attempt to create standard licenses for works other than software, it was certainly the most successful.

As a matter of fact, one of the Creative Commons licenses, the CC Attribution-Share-alike license, played a role in generating a relevant digital commons: the Creative Commons Attribution Share Alike license is currently used for Wikipedia[5].

In recent years, an increasing number of projects have aimed to foster the creation of digital commons that consist of databases, including different governments that started releasing public databases under the terms of free licenses.

CC Attribution, CC Attribution-Share-alike, and CC0 licenses have been used for databases, but new free licenses, specifically designed for databases, were also created, such as the licenses made by the Open Data Commons[6], including the Open Data Commons Open Database License (Odbl)[7], that is used for the OpenStreetMap project[8] (an other relevant digital commons).

Some of the most important digital commons available today are made of personal data.

As way of example, Wikipedia is made of contributions made by people identified by their email address and/or IP address from which they post their contributions.

Also the linux kernel is made by contributions of people identified and therefore is made of personal data (like the major part of free software projects).

5. Free licenses and privacy laws

Free licenses do not deal with obligations provided by privacy laws protecting personal data.

Usually, free licenses applicable to data deal with copyright and *sui generis* right on databases (sometimes with other rights) but do not deal with the obligations provided by privacy laws, like the GDPR.

The mere fact that a specific database is available according to a free license does not imply that the users of that database can avoid to comply with the obligations provided by privacy laws like GDPR (obligation to provide information, obligation to lawful processing, etc.).

Even if a database including personal data is available according to a free license obligations provided by privacy laws have to be managed in different ways adopting different legal tools: adoption of free licenses will not limit the privacy rights of the data subjects.

6. Legal acts fostering the creation of digital commons and Distributed Ledger Technologies

Free licenses consist in unilateral legal acts (acts made by the creator of the artifact addressed to the users).

Adoption of a free license consist of an act made by the author (or other copyright holder) of a work: she identifies the work to be licensed and publishes such work linking it to the license that she wants to apply to the work.

Users can access the work and use it according to the term of the license applied by the author.

As a matter of fact, up to date no other legal technique (contracts among publisher and user, unilateral acts of the users) has emerged as a valid technique to foster creation of digital commons.

Maybe, this has to do with the fact the “terms of service” and “privacy policies” today are set by the service providers (users of the personal data of the data subjects), which, usually, are interested in having control on the personal data.

Today, distributed ledger technologies (DLT), also called blockchains, and smart contract technologies running on DLT can allow to have more complex interactions (contracts, unilateral

[5] See https://www.wikipedia.org/.

[6] See https://opendatacommons.org/.

[7] See https://opendatacommons.org/licenses/odbl/.

[8] See http://www.openstreetmap.org/copyright.

acts of the data users, etc.) that are not set by the users of the data (service providers) but by the data subjects.

A smart contract is a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract. Many kinds of contractual clauses may be made partially or fully self-executing, self-enforcing, or both.

Scholars debate whether smart contracts should be considered ‘contracts’ in the traditional legal meaning: the point refers to what ‘contract’ means.

A contract in the traditional sense is an agreement between two or more parties to do or not to do something in exchange for something else, where mutual assent must be manifested by making a promise and/or rendering performance, and it may be written or spoken.

Sometimes smart contracts do not constitute contracts with legal effects. But smart contracts may be agreements.

DLT and smart contracts offer new opportunities for giving people the control of their personal data, allowing to choose what data they want to share and how.

In short and following a proactive approach, DLT and smart contracts could offer a new scenario for designing and inventing new tools and strategies for allowing privacy and data protection safeguards.

DECODE smart rules allow the conclusion of legally binding agreements or the making legally binding unilateral acts.

Such agreements or unilateral acts could be used to comply with privacy obligations provided by the GDPR (information, consent, etc.) and for other purposes with the goal of fostering the building of digital commons made of personal data.