Roberto Cirillo

I. Introduction

The fully fledged name of the GDPR is "**on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [...]"**[1]

However, much of the public debate about the new regulation has focused on the part regarding the **protection of data**: the stress on aspects such as privacy and security by design have indeed dominated most of the topic, since their impact on the design of information and communication technologies (ICT) as well as the on the juridical status of subjects involved and their conditions of treatment of data are so deep.

In spite of this, the second part of the title ("**on the free movement of such data**") throws us a glimpse of the **broader intent of the regulation**. The protection of data (or better, "of natural persons with regard of personal data") should ***not forbid or hinder*** the ***movement*** of such data, which – moreover – should be ***free*** **.** In these few keywords, we see the intent of the regulators ***not to kill the data economy by means of data protection***.[2] We see here the awareness of the regulator about the huge potential of data as the new basic pillar for both Public Organizations and Institutions and businesses.

This awareness likely arises from the (recent) historical background and pre-conditions that made data economy's potential so clear, and can maybe partly justify the many "grey areas" that the GDPR is remarked to have left. As for the background, the GDPR faces the acknowledgment that data economy grew within the **business** (remarkably, *American* businesses): so, the production of data and their treatment was conceived of as **to generate profit**, not really to preserve or protect persons' rights (unless they would affect the profit). This is especially clear in the matter of **profiling and privacy**. Profiling is not itself a "bad thing", because as advertisers say to users, "You will still receive ads, but they may not be relevant to you". Which means at least two things: from the business point of view, this means being able to make more accurate market segments and reduce inefficiency in addressing products or services to the "right customers"; from the user-customer's point of view, this means being addressed by relevant information: when marketing and communication are really *informative* to a customer, a good ad can satisfy his/her informational need. This is why the GDPR stresses on the **consent**: customers should be informed and aware about which information they are **willingly** providing to business so as to allow them to build accurate profiles. On the contrary, business (and in particular digital services) have tried to build environments that they fully control, where people more or less freely and spontaneously show and leave traces of their behaviour (and personality). This affects privacy if the data subject has no control or power over the data that he/she generated.

On the second hand, **not only businesses built up a system of data**. **Public Organizations and Institutions** actually have plenty of data about people. Persons' health data are just one example (and one that is especially attractive for businesses). The treatment of Public Organizations' data needed a regulation in order not only to avoid rights violations; but it has become a way to express and concretely implement the principle of **transparency of Public Organizations** towards citizens: citizens can employ their right to control over Institution by means of data, that has to be accessible (under certain conditions) and has to be measurable[3] .

The **"grey areas"** that the GDPR seems to be criticized for mainly address the tools that it enables with. The regulation seems to be designed more to set principles and less to provide tools and roles to take actions (despite the creation of new functional roles such as the DPO). This, however, seems to be done on purpose: the GDPR means to instruct with guidelines, rather than being a list of do's and dont's. **This characterization is due to its intent to be substantial in the impact,** and not just a formal checklist (as Authorities of data protection often point out). It is known, indeed, that the GDPR was initially conceived of as a European *directive* and not a general *regulation***.** In short, the character of the GDPR focuses more on showing and pointing to the purposes, and less on the way to achieve them.

However, this characterization in "setting the principles" has introduced some new important elements and key points, that – again – make the regulation effective in its impact for both businesses and Public Organizations.

II. New Key Elements

Based on the previous legal corpora regarding privacy, fragmented in the variety of national laws, the GDPR tries to harmonize their principles into a new perspective, without discarding what's been done before. Thus, what's important here is the **new perspective.**

In order to set up a new framework on the treatment of data, the GDPR brings in new elements that were not typical of the regulations which it relies on. For instance, privacy laws did not really have anything to do about the idea of portability, which indeed comes from the regulation of telecommunications.

As mentioned in the beginning, the intent of the GDPR is not to kill data economy by means of data protection. Within this perspective, some elements have been introduced in order to ease and favor the circulation of data while still giving guarantees on the protection. Whereas I recognize the principles of privacy- and security-by-design as key technological elements on the protection side, I would like to highlight the role of **portability** and **interoperability** as the key elements on **the "economic side".**

Triggered by the fundamental questions of this award, I have further elaborated on their implications and extended their scope.

"*What is the role of other stakeholders (consumers organisation, the industry and the public sector) in securing a more equitable state of affairs"* And more: Within the framework of GDPR new elements in the regulation, which elements can constitute a "competitive advantage" for businesses?

"What would be the most adequate relation between consumers and their personal data?". And which of those advantages can be the most helpful and useful for consumers? Do we need to distinguish between citizen and consumer?

In order to ground these questions down to actual applications, I will make here a broad overview of value proposition from public organizations, industries and companies that have created solutions. These solutions are just examples of how the new principles stated in the GDPR can be elaborated and exploited.

The solutions I have identified are:

- SPID (Italian solution and system for the digital identity) ;
- Weople (a newly founded company; I will provide further details and discussion later on) ;
- Data Transfer Project (by Apple, Facebook, Google, Microsoft, Twitter).

SPID

According to and following the European and Italian agendas in the digital transformation, SPID (essentially, a unique digital identity for citizens) is a very important key asset. Technologically, SPID doesn't differ too much from Personal Accounts in digital services and social networks. Also, working as a single-sign-on technology, it allows access to all platforms that integrate it into their systems: this resembles of course the practices of social login, including data sharing across platforms. What is the difference then? The control of data by the data subject is the difference! Currently SPID allows access to all main public administration services. Since it's based on the regulation of Public Organizations, data sharing across platforms and policies of consent and access to personal data are strict. Interestingly, although the personal data collected may be mainly of administrative type, this does not exclude an economic exploitation of some types of data (which the data subject should provide consent for anyways). Apart from all the possible interactions between public and private sectors that could meet in this solution, the principle in use here is **INTEROPERABILITY**. The role of the public sector here is especially important to set the ***standard.*** As being the source of authority, the public sector is able to decide the (minimum) requirements and its digital service could constitute the **"control room"** (and dashboard) where every citizen could switch on and off which personal data can be used by whom. The dark side of this solution is of course centralization, with all consequent risks about data security and breaches. I would like to point out one special note about **consumer organizations** (also as being a member of the Italian *Altroconsumo*). Much of the concerns I about digital privacy derive from the fact that digital services can track people all across websites, mobiles, apps, and so on. As said above already, this is useful for businesses in order to profile users as customers. In situation where every customer is profiled with respect to the products of his/her interest and prices of his/her purchases, an economic profile could be outlined. **What if prices could change according to how much one person is able or ready to spend for that product?** The economy would shift its paradigm from the cost of production for every product to an auction for every product. (An example we are already used to is the changing price of air or train companies, depending on the time of purchase). Would this have implications for my rights as consumer? The question could be: if a customer is able or ready to spend more for a product, should he/she spend more? **Is it economic discrimination? I think consumer organizations, supported by public organizations with proper tools, should monitor this issue.**

WEOPLE

Weople is a company that leverages on the principles of **PORTABILITY**. Its value proposal is to become the e-wallet of personal data. The promise to customers is – beyond storing data in the most secure ways – to get paid for receiving ads. The core idea is: if people generate data that companies use, people should also take some part of the economic profit. This principle is already at place in the mechanism of artists' royalties (and copyright more broadly). The debate could rely on the question: is the source of data (or even the art work) always part of the value chain? I challenge: if so, why the same does not apply for agricultural producers? Clearly, the debate is too wide if try to find arguments and references in other industries and sectors.

What I highlight here is the implications of portability. **Portability** as defined in the GDPR **does not imply cancelation or deleting** of data from the original source. It simply enables the data subject (or his/her representant) to ask for a copy of that data. Deletion would have to be one more request. Then, I wonder, **data portability would generate a multiplication of data?** If meant as in telecommunications (as for phone numbers), portability should be defined as transfer? (Where a number or data can be stored and managed *exclusively by one controller*). I think further specifications are needed on the definition of portability and a consumer organization could lobby on this over the Regulator.

DATA TRANSFER PROJECT

This project can be considered as the counterpart of data portability. Its current contributors are Apple, Facebook, Google, Microsoft, Twitter. Not surprisingly these contributors have teamed up to find a common solution on how to share the data without making a war. These companies have built their commonly said "empires" on the data they collect and process about their users. And this solution leverages on the principle of **INTEROPERABILITY**. Differently from the case of SPID, interoperability here looks like **a technological business-driven solution**. If this was just a "front scenes" operation for legal compliance (while trying to hinder data sharing behind the scenes), much of its potential would be lost. However, given its contributors, this project a huge potential to set and become a standard *de facto* for interoperability.

There are pros and cons of this. Currently, on the one hand, **the fragmentation of personal data** in different digital service providers hinders them from creating a unique and detailed personal profile. What if these services could exchange data without the user to be informed about it and give consent? Currently, this is how commercial partnerships work for website; and indeed explicit consent on third parties was introduced. On the second hand, the approach adopted the DTP is to use open-source code, so that anyone can – at least in principle – check what data is being transferred. And this also goes into the direction of **company and business transparency** (instead of hiding behind industrial secret), which especially for big tech companies, has been a big deal so far.

One more pro is that these companies are, at the moment, way more powerful from a technological point of view. And a distribute rather than centralized collection of data (like in the case of SPID and WEOPLE) would probably be an advantage for security.

III. CONCLUSION

The GDPR has cast a new perspective on the data scenario, both for its treatment and the status of players involved. Its substantial approach aims at empowering subjects with real rights able to make an effect. In order to achieve this, the tools I consider to have the right balance between power of the principle and the effectiveness of the action are portability and **interoperability**, with the latter being even **more important**. In a scenario where most customers *use* these services without being able to *master*, my answer to how should the relation be between consumers and their data, I say it should be **distributed control.** By this I mean that every citizen should be provided with a digital identity by default (just like an ID card), with some basic data. All external services should rely on this, but this does not mean that all data produced by these services should be centralized. **Digital identity should work as a control room**, by which every user should be able to switch on and off the access that third parties require.

1 Official Journal of the European Union : REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

2 Data economy nuovo (dis)ordine mondiale: tutte le sfide e i paradossi

3 GDPR, chap. 3, sect. 1, art. 12

Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Caravaca, S. (2019, 11 29). *Data economy nuovo (dis)ordine mondiale: tutte le sfide e i paradossi.* Tratto da https://www.agendadigitale.eu/cultura-digitale/data-economy-nuovo-disordine-mondiale-tutte-le-sfide-e-i-paradossi/

Ciccia Messina, A. (. (2020). *Condizioni di liceità del trattamento dei dati per interesse pubblico.* Corso di perferzionamento in Data Protection e Data Governance, Università degli studi di Milano, Scienze Giuridiche Cesare Beccaria , Milano.

Finocchiaro, G. (1/2019). La «digital revolution» nel settore finanziario. Una nota di metodo.,. *«ANALISI GIURIDICA DELL'ECONOMIA»,*, pp. 313 - 326.

Finocchiaro, G. (2017). Effetti giuridici dei documenti elettronici. In G. Finocchiaro, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno. Commento al Regolamento UE 910/2014* (p. pp. 351 - 352). Torino: Giappichelli.

Finocchiaro, G. (2019). Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali. In F. Giusella, *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101, Bologna, Zanichelli, 2019,* (p. 1-26).

Niger, S. (2020). *Trasparenza amministrativa e trattamento dei dati.* Università Studi Calabria, Scienze Giuridiche Cesare Beccaria. Milano: Università Studi Milano.

Orofino, M. (2020). *Trattamento categorie particolari di dati.* Università degli Studi di Milano, Scienze Giuridiche Cesare Beccaria. Scienze Giuridiche Cesare Beccaria.

Pagliarini, E. (2020, 01 17). *Negozio automatico, riconoscimento facciale e sanità digitale.* Tratto da https://www.radio24.ilsole24ore.com/programmi/2024/puntata/negozio-automatico-riconoscimento-facciale-e-sanita-digitale-190913-ACGQ1lCB

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. (2016).
Tratto da https://eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Tiani, V. (2019, 11 25). *Oltre il Gdpr: il manifesto di Buttarelli sul futuro della privacy in Europ.* Tratto da https://www.wired.it/internet/regole/2019/11/25/privacy-europa-gdpr- buttarelli/