Personal data, big data, cultural heritage and GDPR: realities and challenges

Antonia Pediaditaki[1]

[1] *Lawyer (LLM, DEA), Member of the Athens Bar Association, Athens, Greece*

Abstract

The present paper investigates the new realities and challenges created by the digital hybrid life of citizens, using apps in light of the recent coronavirus pandemic. The traditional notion of "ownership" is seen together with "data unbundling", which is considered as an option of data management, while GDPR and AI Act need to be applied in parallel.

Keywords

Data protection, GDPR, big data, artificial intelligence, museums, coronavirus

1. Introduction

In a rapidly expanding and hybrid world, physical reality integrates with digital and virtual reality in ways that are frequently unconceivable. Apps gain momentum and use all the possibilities offered by the Internet of Things which, by gathering data through sensors, make data collection and data analysis possible where it would have been unthinkable before.

This new hybrid world is just as real as the old physical world, but it demands a different mindset to really see and fathom what its effects are on us and what its wider societal, economic and political consequences are, especially considering the very recent coronavirus pandemic.

Of course, we will all accept that what happens on a physical screen is "real" (the screen is physically there, the images can be seen, sounds can be heard), but it is different from a painting where you can feel the actual image (and not a projection of that image) by physically touching the canvass. A painting is physical and static. However, a computer screen, although physical, is meant to create impressions on our mind, which we consider to be equal to an impression of, for example, a painting. But, although we can certainly touch the screen, the images as such cannot be touched; they are not made of paint but are the result of software which projects these images on our screen so we will accept them as "real". Computer images are virtual and dynamic.

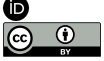
The legislation, however, still takes this old physical and static perception of reality as its very foundation. We expected to have time to consider either the adaptation of existing rules or the development of new rules. The coronavirus pandemic, by causing an incredibly fast rise to various apps (especially e-health related) showed however, that the time is running out, and we need to give answers here and now.

The purpose of this paper is to focus on the ways data protection and cultural heritage interact, in relation with GDPR, considering the very recent coronavirus crisis and the realities and challenges revealed on this occasion.

MBD2024: International Conference On Museum Big Data, November 18-19, 2024, Athens, Greece

* Corresponding author.

tpediaditaki@gmx.com



Moreover, in this paper we will deal with the legal nature of data gathered in apps. More precisely, we need to question whether these data can "belong" to (or be "owned" by) anyone or are these data to be considered "res nullius", what does "belonging" ("owning") mean and, if data can belong to anyone, to whom do they belong? To rephrase the question: is it possible to speak about a property entitlement concerning data gathered by various museum apps and, if such entitlement can be accepted, what its content is and to whom such entitlement should be allocated? These questions seem fundamental.

2. Data ownership or data unbundling: the use case of Coronavirus pandemic

The rise of the digital economy with its virtual reality is the result of developments which are relatively recent. The era of mechanization, steam engines and waterpower and the rise of mass production and the widespread use of electricity took decades; however, the development of electronic and IT systems and automation happened very rapidly. Today, we experience a world where those who do not follow changes closely are always overtaken by the constant consecutive innovations in research and development, especially the technology which is widely used in everyday life.

If we wish to give a proper response to such changes, lawyers need to understand – at least at a basic level – technological advances related to cyber-physical systems, Distributed Ledger Technology (i.e. blockchain), Artificial Intelligence and the Internet of Things. These are stages from the First to the Fourth Industrial Revolution, as described by K. Schwab. This is all going to at such a fast pace that developments seem difficult to follow and comprehend; this results in making it hard to learn how to live with these advances, let alone start thinking about redesigning the law to adapt it for this new hybrid world. Third World countries have a far less developed IT structure than can be found in, for example, the European Union, North America and China. All of this echoes how we look at the use of IT and apps as part of modern culture.

The coronavirus pandemic has created (and still does create) havoc in countries all over the world and, pressed by an urgent need to react and prevent the spread of the disease against a background where, until now, no effective – preventive or curative – medication has been found. This is why it is quite understandable that IT solutions have been quickly looked at and chosen.

Monitoring and tracing & tracking apps have overtaken daily life and created new ways of doing things, while they have also created new problems and challenges ahead. So, IT has proved to be a prime facilitator. Where societies have become or are in the process of becoming more affected by technological change and, consequently, develop into information societies, a large part of the population will most likely use a mobile phone. These phones can only work if they are connected to a wider network, which allows them to be followed. Localization data is gathered by, among others, telephone providers and has turned out to be a very valuable source of information which can be used for various purposes, in the beginning for Covid-19 purposes and then for other wider objectives.

The data which is collected by all these apps is not only a source of personal information about citizens' private life, but also a source of information from the perspective of public interest (such as public health for example) and the dire need to run research about various issues (primarily health issues, to find cumulative medication). The gathered data is therefore as well as being primarily of a personal nature, also of non-personal (general interest: e.g. public health) nature. In other words: the use of the apps brings to the surface a deep conflict between, on the one hand, the need to protection of everyone's personhood by shielding people from having to give up their privacy regarding personal location and other personal data, for they are part of how they live and who they are, and, on the other hand, the public interest (e.g. public health and medical research), and, of course, further social/societal and economic interests.

And is here that trouble starts: From a traditional legal standpoint, we need to remember that the legislator (e.g. in property law), leans towards resolving around what we can find in the physical world outside us. This is why lawyers encountered grave difficulties when dealing with intangible things, such as monetary claims and the outcomes of human creativity. In some legal systems, monetary claims were not considered to be "things" and could for that reason not be owned, but as monetary claims represent considerable monetary value one could be "entitled" to the claim, and the claim could be offered as security for a loan. Regarding the products of human creativity, it was also clear that such products represented considerable economic value and could not be ignored. Because these products were even further away from the objects of traditional property law than monetary claims, the final outcome of the theoretical struggle was to consider the law that governs these products as a new, separate legal area with its own framework, although – very much as we saw with claims – not infrequently mimicking traditional property law.

In the case of the fundamental building blocks of the digital economy: data, questions about their legal status have become even more pressing than earlier problems caused by the growing economic importance of monetary claims and human creativity. All the problems triggered by the growing impact of IT on our lives are coming together here. The world has become hybrid, with both real and digital aspects which, more and more, interact and even integrate. This hybrid world functions based on technology, both physical (hardware) and non-physical (software), that results in data, which by their very technical nature can be copied, combined, shared, etc. in ways which until relatively recently were inconceivable in the real world. Data provides a meaning to us (and about us), in other words: information is now so readily available that is seems as if we as human beings are now also becoming hybrid personalities. Our "real" life now merges with our "virtual" life and becomes hybrid. IT companies sometimes – up to a certain degree - tend to have more information about us that we do ourselves.

This is why we need to be protected against the unlimited and unjustified use of data which affect us as a person (privacy and data protection), but it also cannot be denied that these very data are part of the present digital economy (and consequently the free flow of non-personal data) and might be of crucial importance from the perspective of the societal/economic benefits.

Quite recently, the Court of Justice of the European union clarified that privacy and data protection are fundamental human rights and that, for this reason, personal data only under the strictest conditions can be transferred from Europe to the USA (CJEU Case C-311/18 Facebook Ireland and Schrems). The court states: "*It follows that, since, first, a transfer of personal data, such as that at issue in the main proceedings, for commercial purposes by an economic operator established in one MS to another economic operator in a third country, falls, as is apparent from the answer to the first question, within the scope of the GDPR and, second, the purpose of that regulation is, inter alia, as is apparent from recital 10 thereof, to ensure a consistent and high level of protection of natural persons within the EU and, to that end, to ensure a consistent and homogenous application of the rules for the protection of fundamental rights and freedoms of such natural persons with regard to the processing of personal data throughout the EU, the level of protection of fundamental rights required by Article 46 (1) of that regulation must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union (2012).*"

In this framework, the notion of "Digitale Souveränität" is very interesting, which first appeared in a discussion paper from the German Ministry of Traffic and Digital Infrastrusture. But even if sovereignty is limited in the way as is done by this German government paper on digital sovereignty, such personal sovereignty can only be given and defended by a State acting under its public international law sovereignty. Data is then, consequently, "things" under the control of the State and the State can take data from individual citizens in the public interest. This is clearly the idea underlying the control of data flows in countries which created or are creating digital firewalls around them, demanding that data which are created, processed, analysed and transferred must remain on servers within that State's territory.

When it comes to the existing EU legislation regarding data as such we see that neither the ePrivacy Directive, the General Data Protection Regulation (GDPR), the Regulation on a Framework

for the free flow of Nonpersonal data, the EU's laws on intellectual property, nor the Trade Secrets Directive contain a framework for accepting ownership of data outside the protection of personal data, trade secrets and software. Several reports have been published on this, and they all come to the same conclusion, with which the European Commission now apparently agrees.

However, this leaves the question unanswered whether data, as such, can be owned and if the European Union still should not introduce such a notion. Given that, at least for the time being, no unambiguous EU law in this area exists, answers can only be given at the level of the Member States, resulting in the need for a comparative legal examination.

In that respect, the European Commission recently expressed the view that stakeholders do not favor a "data ownership" type of right, considering that it is immediately followed by admitting that we do need rules on access. However, one could argue that there is no much difference between ownership and access. Let's see then: Given the nature of data, what is ownership other than being in control of access, portability, transfer or erasure (including the desisting from control or processing of data)? To rephrase it, what else is there than the right to manage data in an environment where several people at the same time may have concurring or competing rights to access, portability, transfer and erasure? In such an environment, ownership of data means management of access. The EU legislation seems to move in that direction quite swiftly.

This question is closely related to the examination of the legal nature of property rights to data, considering general property rights that modern legislation recognizes. To give a direct answer, we could argue that property rights protect the right holder against claims by a relevant group of other subjects of rights of ownership.

Given now the very character of the object of ownership, which is data, i.e. the fact that data is intangible, as a cluster of data), a flexible and open approach as to the content of the right must be sought which must include a time factor. This means the following: As long as the data is on the user's phone, only the user is the "owner", allowing only the user access, portability, transfer and erasure. Afterwards, at a later stage, ownership is fragmented over relevant third parties, such as public authorities and service providers (e.g. museums).

The fragmentation of data in the above sense, is what we call "unbundling" in EU law. This demands a management structure of data ownership whereby it could be argued that at the end it all comes down to time management of access, because portability transfer and erasure (including the desisting from control or processing of data) are essentially all different aspects of giving, not-giving or ending access, with degrees of access varying over time.

Access management based on unbundling of ownership is not only a legal but also a strategic tool and as such it can contribute to a balanced distribution and allocation of rights. This methodology is not new in EU law. Let's recall that unbundling is a frequently exploited instrument in order to open up markets and break monopolies. Let's see cases in public transport (i.e. rail), gas and electricity markets and telecoms.

The starting point for unbundling is that no one single stakeholder or market participant should have full control over data. This can be done by splitting up a market, services or service providers to create competition. Such unbundling can be done in several ways through legal, operational, informational and ownership unbundling. "Legal and ownership unbundling" can go hand in hand and is intended to divide control over several market participants. "Operational unbundling" implies splitting up operations over several independent legal entities, and "informational unbundling" implies making information accessible to other market participants.

The latter approach can be found in recent policy papers by the European Commission to create European common data spaces and promote, perhaps even oblige, data sharing between business and governments, and among businesses. One of these common data spaces should be in cultural heritage. Such an informational unbundling can be done by giving access to other than those who create data. At the same time, by giving access to ownership unbundling has also been achieved. However, a clear and workable legal framework regarding time management of access rights must then be in place, which is very important but hard to achieve.

3. Conclusion

Considering the above elements, unbundling data ownership as data access management could be a way forward. Big and anonymous (or anonymized) data gathered in museums from visitors and users of spaces, seen in light of the GDPR framework, data gathering via Artificial Intelligence and modern tools for machine learning do present new challenges, and tend to create new problems, while we are still struggling to resolve the older ones.

However, it is obvious that the management of cultural heritage, exploiting new tools and seeking alternative solutions, will necessarily pass through the combined application of GDPR and AI Act, while these two legislations are not necessarily serving the same purpose. Data protection and big data are part of the same discussion without being part of the same solution.

The coronavirus pandemic proved that technology is a prime facilitator when traditional solutions collide. Now is the time to check if, in the framework of cultural heritage management, the private interest (i.e. data protection) and the public interest (i.e. bid data exploited for culture seen per se) can be seen in concordance without major conflicts.

Declaration on Generative AI

The author has not employed any Generative AI tools.

References

[1] K. Schwab, The Fourth Industrial Revolution, Penguin Random House, USA, 2016.

[2] K. Schwab, N. Davis, Shaping the Future of the Fourth Industrial Revolution: A guide to building a better world, Penguin Random House, USA, 2018.

[3] S van Erp, Who “Owns” the Data in a Coronavirus Tracing (and/or Tracking) App? In: E. Hondius E, M. Santos Silva, A. Nicolussi, P. Salvador Coderch, C. Wendehorst, F. Zoll, eds. Coronavirus and the Law in Europe, Intersentia; 2021:131-156.

[4] Bundesministerium fur Verkehr und digitale Infrastruktur,”Eigentumsordnung” fur Mobilitatsdaten? Eine Studie aus technischer, okomomischer und rechtlicher Perspektive, Berlin, 2017.

[5] A. Boerding et al., “Data ownership – A Property Rights Approach from a European perspective” (2018) 11 J. Civ. L. Stud., URL: https://digitalcommons.law.lsu.edu/jcls/vol11/iss2/5.

[6] J. Pohle, “Digitale Souveranitat” in: T. Klenk, F. Nullmeier and G. Wener (eds.), Handbuch Digitalisierung in Staat und Verwaltung, Springer VS, also available electronically URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3435017