Chapter 6

Decentralized Data and Privacy:

Exploring the Conflict Between Distributed Ledger Technology and the Right to Be Forgotten Under GDP

Akash Bag
https://orcid.org/0000-0001-8820-171X
Amity University, India

Paridhi Sharma
O.P. Jindal Global University, India

Pranjal Khare
O.P. Jindal Global University, India

Souvik Roy
Adamas University, India

ABSTRACT

Our personal information, or "digital footprint," is gathered and used in today's digital age. Digital footprints are kept, unlike snow footprints. There is a large market for this data, which businesses utilize to analyze consumer preferences. Businesses collecting a lot of data in one place pose a privacy risk. Thus, people are worried. Businesses prefer not to utilize intermediaries to manage client data to save money. Therefore, new technology is needed to make online interactions safer and more efficient. We're considering "distributed ledger technology." This technology is interesting because it securely collects, stores, and processes data without central authority. It has data immutability, transparency, and safety. A problem exists. The European GDPR (general data protection regulation) may conflict with this technology. This chapter will examine this tension, focusing on the right to be forgotten, which permits people to delete their data. It will examine how this new technology and existing privacy policies can function together or need tweaking.

DOI: 10.4018/979-8-3693-0472-3.ch006

INTRODUCTION

In today's digital society, it is hard to forget. The Internet is a public memory for society where anyone can access all the information we humans produce. Enough amounts of data are generated through new digital solutions and services, combined with the expanding use of computers and new technologies. Collecting and processing this enormous amount of information has become a central part of companies' business, as they build large parts of their business on knowing as much as possible about the individual to adapt and provide their services (Al-Abdullah et al., 2020). The fact that people increasingly leave behind digital footprints is not without consequences.

On the one hand, it is easy to imagine a scenario where information about where you are, what you like, and who you spend time with can be used if it falls into the wrong hands. In part, humans risk losing control over our information and the ability to influence others' image of ourselves. Therefore, the developed technical solutions must meet the needs set from a data protection perspective. The legislator must know how the increased digitization and its challenges must be met through data protection to protect the individual and his right to privacy. At the same time, the legislation mustn't become rigid and undynamic. It leaves room for continued technological development (Chase, 2019).

An example of technology that is currently developing at a rapid pace is distributed ledger technology (DLT). The technology can be briefly summarized as a digital system for recording transactions and data transfers without relying on a central actor. The technology is better known under the name blockchain technology or smart contracts and is used to secure and increase control over information by providing various new solutions for identification, data transfer, increased traceability, and a reduced risk of manipulation (Burman, 2020). At the same time, one of the characteristics of the technology is immutability, which means that it is very difficult to delete data from a DLT, and any updates are permanently recorded for posterity (Berberich & Steiner, 2016). Thus, despite the technology's many potential positive effects, there are great concerns about the data protection challenges that the system can create. DLT is primarily associated with blockchain technology virtual currencies and information storage on distributed databases (Berberich & Steiner, 2016). However, the potential for DLT extends far beyond just information storage. In the public sector, utilities are expected to use the technology to calibrate electricity supply, and in healthcare, the technology is expected to improve medical treatment. Technology offers online platforms the infrastructure for specific events; for example, DLT is the building block of the next generation internet, Web 3.0.7. At the same time, banking is undergoing major changes in the financial sector, where technology is used to streamline transactions and make payments increasingly "*intelligent*." This development shows how urgent it is to clarify the DLT and individual data protection issue (Voss, 2016).

This chapter aims to highlight the difficulties that DLT causes for the individual's right to the protection of personal data to investigate the possibilities of ensuring effective data protection without limiting technological innovation and highlighting the potential solutions. Against the background of this purpose and the conflict mentioned above between DLT and GDPR, I intend to investigate the relationship between DLT and GDPR in this chapter. This will be achieved by answering the following question: *How does the use of DLT relate to the right to be forgotten?* To guide the chapter's investigation of the above question, three main aspects of the relationship between GDPR and DLT will be investigated: 1) what are the difficulties associated with deleting data on a DLT, and 2) whether it is possible to apply the GDPR to DLT and 3) whether it is possible to design secure personal data processing on DLT despite the limited possibilities to delete data.