DAOs and personal data protection

27.09.2022 3 min read

Authors

Felipe Palhares

Related areas

Data Privacy and Cybersecurity

Topics

Data Privacy and Cybersecurity
DAOs

DAO is an organization governed and managed by rules codified by smart contracts executed on blockchains. A DAO has a decentralized nature, thus lacking any central authority, and is autonomous, to the extent that its actions are executed by smart contracts, regardless of intermediaries. DAOs' structure entails several challenges to its regulation, especially with regard to the protection of personal data.

It is important to discuss whether DAOs process personal data and, therefore, are subject to data protection laws. Personal data is any information that, directly or indirectly, is related to an identified or identifiable natural person. DAOs may process many personal data in connection with their members, for instance. These data, even if encrypted or pseudonymized, are able to reach the identity of a member. This occurred, for example, in the Bitcoin network, when a research from Cornell University, in 2014, revealed that IP addresses could be discovered from public keys, leading to the identification of users.

A public blockchain, for instance, does not store information such as names or addresses, but rather keeps a record of hash values, public keys, and other data of transactions, that may be classified as personal data, to the extent that the information is usually enough to identify the user. The pseudonymization may hamper the identification of the data subjects, but does not turns it impossible, as well as cryptography, which allows access to the data only through cryptographic keys. Even though these techniques may be employed as security measures, they do not necessarily waive the application of data protection laws. This waiver of data protection laws would occur in the hypothesis in which the data is effectively anonymized, i.e., the data irreversibly losses the possibility to be associated, directly or indirectly, to an individual, just like the cases when the codified information has no connection with a natural person at all.

As for the controller and processor of personal data, data protection laws were not formulated for decentralized systems, but rather for centralized structures that decide and operate the processing of personal data. However, DAOs are characterized by the absence of a central authority, i.e., its members participate in the governance of the organization and can contribute to the definition of its rules and guidelines, hampering the framing of controllers and processors of personal data and their liability in case of violations to the protection of personal data.

In a DAO, no single organization determines the purposes and means of processing personal data. Hence, some argue that DAO members would be joint controllers when collectively determining the purposes and means of processing personal data, so that each one would be liable for possible violations of the data protection laws by the DAO.

However, this reasoning, in practice, incurs many challenges when we figure the accountability of 1.000, 10.000, or 100.000 members for potential

damages caused by the processing of personal data. Beyond that, DAOs' architecture covers distinct actors (e.g. founding members, voting and non-voting members, developers of smart contracts, etc.), owning different characteristics and functions that must be taken into account to adequately define data controllers and data processors.

Another issue to be considered are the rights of data subjects, including the right to rectification or erasure of personal data. As aforementioned, the nature of blockchain technology does not allow the exclusion or rectification of information insofar as each block owns a hash value of the previous one, and any modification in the blocks would result in the altering of the subsequent blocks, which prevents the blockchain from being tampered with. Additionally, in DAOs, no member or other individual is capable of, unilaterally, altering or excluding the smart contracts without the consensus of other members.

As can be seen, data protection laws were constructed in a scenario of centralized processing of personal data, not contemplating the singularities of decentralized technologies. The lack of attention to the complexities of decentralized systems results in various challenges for the application of data protection laws to the processing of data supported by decentralized technology.

Therefore, the current legislations are unable to provide the necessary answers when facing the challenges posed by DAOs. As new technologies based on decentralized systems become widely employed, it is necessary that laws furnish a legal structure in which blockchain could be used, adjusting themselves to this new reality.

>>> This content belongs to our e-book "DAOs: Legal Challenges for Decentralized Autonomous Organizations". Click here to read more articles.

› PROFESSIONALS

Professionals who combine legal insight and market perspective

Felipe Palhares