As DAOs estão sujeitas à legislação de proteção de dados pessoais

27.09.2022 4 minutos de leitura

Autores

Felipe Palhares

Áreas relacionadas

Proteção de Dados e Cybersecurity

Assuntos

Proteção de Dados e Cybersecurity DAOs

Em uma DAO não há uma única organização que determina sozinha a finalidade e os meios de tratamento de dados pessoais

Uma DAO é uma organização governada e gerida por regras codificadas por meio de contratos inteligentes (smart contracts) executados em blockchains. A DAO é de natureza descentralizada, pois não possui autoridade central, e é autônoma, na medida em que suas ações são executadas por contratos inteligentes, sem a necessidade de um intermediário. A própria estrutura das DAOs implica diversos desafios à sua regulação, especialmente em relação à proteção de dados pessoais.

É importante discutirmos se as DAOs tratam dados pessoais e, portanto, estão sujeitas às legislações de proteção de dados pessoais. Dados pessoais são informações que, direta ou indiretamente, se relacionam a pessoa natural identificada ou identificável. As DAOs podem tratar vários dados pessoais relacionados aos seus membros, por exemplo. Esses dados, ainda que criptografados ou pseudoanonimizados, podem levar à identidade de um membro. Isso ocorreu, por exemplo, na rede Bitcoin, quando uma pesquisa da Cornell University, em 2014, revelou que endereços IP podiam ser encontrados a partir de chaves públicas, levando à identificação dos usuários.

Uma blockchain pública, por exemplo, não armazena informações como nomes ou endereços, mas mantém um registro de valores de hash, chaves públicas e outros dados de transações, que podem ser classificados como dados pessoais, na medida que as informações geralmente são suficientes para identificar o usuário.

A pseudoanonimização pode dificultar a identificação do titular dos dados, mas não a impossibilita, assim como a criptografia, que possibilita o acesso aos dados apenas por meio de chaves de criptografia. Embora essas técnicas possam ser utilizadas como medidas de segurança, não dispensam necessariamente a aplicação das leis de proteção de dados. A inaplicabilidade das leis de proteção de dados pessoais ocorreria nas hipóteses em que de fato os dados fossem anonimizados, ou seja, o dado perderia a possibilidade de associação, direta ou indireta, a um indivíduo de forma irreversível, assim como nos casos em que as informações codificadas não se relacionariam a uma pessoa natural.

Em relação às figuras dos agentes de tratamento de dados, as legislações de proteção de dados não foram elaboradas para sistemas descentralizados, mas para estruturas centralizadas que decidem e operam atividades de tratamento de dados pessoais. Contudo, as DAOs são caracterizadas pela ausência de uma autoridade central, ou seja, seus membros têm participação na governança da organização e podem contribuir para a definição de suas regras e diretrizes, dificultando a categorização dos agentes de tratamento de dados pessoais e sua responsabilização no caso de violação à proteção de

dados pessoais.

Em uma DAO não há uma única organização que determina sozinha a finalidade e os meios de tratamento de dados pessoais. Assim, há quem defenda que os membros da DAO seriam controladores conjuntos, quando determinarem conjuntamente as finalidades e os meios de tratamento de dados pessoais e, consequentemente, cada um seria responsável por eventuais violações à legislação de proteção de dados pela DAO.

Entretanto, essa lógica, na prática, incorre em diversos desafios quando pensamos na responsabilização de 1.000, 10.000 ou 100.000 membros que compõem a DAO por eventuais danos causados pelo tratamento de dados pessoais. Além disso, a arquitetura das DAOs envolve distintos atores (e.g. membros fundadores, membros votantes ou não votantes, desenvolvedores de smart contracts, etc.), que possuem características e funções diferentes que devem ser consideradas para definir adequadamente os agentes de tratamento de dados.

Outro ponto a ser considerado são os direitos dos titulares de dados, incluindo o direito de corrigir ou excluir dados pessoais. Conforme apontado, a natureza da tecnologia blockchain não permite a exclusão ou correção de informações, na medida que cada bloco possui um valor de hash do bloco anterior e qualquer modificação nos blocos resultará em alterações de blocos subsequentes, o que evita que a blockchain seja adulterada. Além disso, nas DAOs nenhum membro ou outro indivíduo pode, unilateralmente, alterar ou excluir os smart contracts, sem o consenso de outros membros.

Como se vê, as legislações de proteção de dados foram construídas em um cenário de tratamento de dados pessoais centralizado e não levam em consideração as peculiaridades de tecnologias descentralizadas. A falta de atenção às complexidades dos sistemas descentralizados resulta em diversos desafios para a aplicação das legislações de proteção de dados em atividades de tratamento de dados baseadas em tecnologias descentralizadas.

Por isso, as atuais legislações não são capazes de dar as respostas necessárias frente aos desafios postos pelas DAOs. À medida que as tecnologias baseadas em sistemas descentralizados se tornam amplamente utilizadas, faz-se necessário que as legislações forneçam uma estrutura legal dentro da qual a blockchain possa ser utilizada, adaptando-se para essa nova realidade.

>>> Este artigo foi escrito por nosso sócio Felipe Palhares e por nossa advogada Bárbara Iszlaji, ambos da área de Proteção de Dados e Cybersecurity. O artigo foi publicado pelo portal Exame no dia 26/09/2022. Clique aqui e confira o conteúdo na íntegra.

>>> Este conteúdo faz parte do e-book "DAOs: Desafios Jurídicos das Organizações Autônomas Descentralizadas". Clique aqui para ler mais artigos.

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Felipe Palhares