REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

UTILIZAÇÃO DE REDES *BLOCKCHAIN* NA ADMINISTRAÇÃO PÚBLICA PARAPROTEÇÃO DAS INFORMAÇÕES[1]

USE OF BLOCKCHAIN NETWORKS IN PUBLIC ADMINISTRATION FOR THE PROTECTION OF INFORMATION

Matheus Teixeira Fernandes[2]
Faculdade Processus – DF (Brasil)
Lattes: http://lattes.cnpq.br/3204635391120386
Orcid: https://orcid.org/0000-0001-9749-5764
E-mail: matheus.ft2@gmail.com

Resumo
O tema deste artigo é sobre a Utilização de Redes Blockchain na Administração Pública para Proteção das Informações. Investigou-se o seguinte problema: A Falta de Segurança das Informações na Administração Pública. Cogitou-se a seguinte hipótese "O Uso de Redes Blockchain para que seja utlizada redes em blocos com mensagens criptografadas". O objetivo geral é Explicar os benefícios e malefícios do uso das Redes Blockchain, assim, podendo aplicar essa ferramenta para a proteção dos Dados (Informações) da Administração Pública. Os Objetivos específicos são: Explicar o conceito de Administração Pública; Explicar o conceito das Redes Blockchain; e Explicar como seria a Implementação das Redes Blockchain para a Segurança das Informações. Este trabalho é importante para um operador do Direito devida a Interpretação Legislativa da Implementação de Novas Tecnologias no Âmbito Jurídico; para a ciência é relevante por causa da Evolução Tecnológica sobre o uso da Internet na Atualidade, e para que seja Utilizada de forma Segura, o Uso das Redes Blockchain com Mensagens Criptografas; agrega a sociedade pelo fato de serem Redes mais Seguras, assim podendo dificultar invasões de hackers em sistemas públicos. Trata-se de uma pesquisa qualitativa teórica com duração de seis meses.

Palavras-chave: Administração Pública. Blockchain. Segurança. Informações.

Abstract
The theme of this article is about the Use of Blockchain Networks in Public Administration for Information Protection. The following problem was investigated:

[1] Este manuscrito contou com a revisão linguística de Roberta dos Anjos Matos Resende.
[2] Graduando em Direito pela Faculdade Processus, DF, Brasil

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

The Lack of Information Security in the Public Administration. The following hypothesis was considered: " The use of blockchains networks with encrypted messages". The general objective is to Explain the benefits and disadvantages of using Blockchain Networks, thus, being able to apply this tool for the protection of the Data (Information) of the Public Administration. The specific objectives are: Explain the concept of Public Administration; Explain the concept of Blockchain Networks; and Explain how the Implementation of Blockchain Networks for Information Security would be. This work is important for a Law operator due to the Legislative Interpretation of the Implementation of New Technologies in the Legal Scope; for science it is relevant because of the Technological Evolution on the use of Internet nowadays, and for it to be used in a Safe way, the Use of Blockchain Networks with Encrypted Messages; it adds to society because they are more Safe Networks, thus being able to difficult hacker invasions in public systems. This is a qualitative theoretical research with a duration of six.

Keywords: Public Administration. Blockchain. Security. Information.

Introdução

Décadas após as ideias de Weiser (1991), a globalização das redes de computadores e tecnologias da informação tornaram-se uma realidade. A tecnologia é essencial para trazer mudanças profundas à sociedade, mudar a maneira como os indivíduos interagem com os artefatos de computação e a organização dos sistemas neste espaço ciberfísico. Como resultado dessa revolução, surgiram diversos modelos de computação nos quais a tecnologia é transparente para os usuários, os dados são coletados no ambiente e processados de maneira coordenada, eficiente e distribuída, de modo que os dispositivos realizam operações autônomas e se comunicam entre si.

Relatórios da Cisco Systems (2016), estimam que cerca de 500 bilhões de dispositivos estarão conectados à Internet até 2030. Segundo Yu et al. (2018), no ano de 2018, a quantidade de dispositivos conectados à internet ultrapassou a população mundial. Os objetos interconectados além de capturar informações e interagir com o mundo físico, podem ainda fornecer serviços com uma ampla gama de aplicativos usando os padrões existentes da Internet. Dados da McKinsey & Company (2019), houve um aumento de cerca de 90% entre os anos de 2014 e 2019, em relação ao número de empresas que aderiram a essa modalidade e a perspectiva de crescimento em 2022 é de 13,6%.

Os aplicativos que utilizam a várias modalidades de conexão, abrangem vários campos, como saúde, educação, serviços públicos, cidades inteligentes e construção civil, logística e agricultura. Todos esses objetos físicos e a infraestrutura de comunicação subjacente transformam a Internet originalmente estática em uma

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

Internet totalmente integrada obtendo um espaço inteligente (RAJ; RAMAN, 2017; GUBBI et al., 2013).

A alta conectividade e a rápida troca de informações permitem a implementação de novas funções, que permitem a inteligência aplicada capaz de processar grandes quantidades de dados trazendo comodidade, produtividade e diversos benefícios aos usuários dessa modalidade (HE et al., 2016).

No entanto, no panorama associado a administração púbica, por conta das imensas quantidades que são trafegados na rede, alguns desafios de privacidade e segurança, torna-se relevante ao se considerar o impacto das vulnerabilidades nesta situação. Além disso, devido à rápida evolução desses dispositivos e aos desafios de desenvolvimento associados à infraestrutura heterogênea e outras características inerentes as preocupações com questões de privacidade e segurança são frequentemente ignoradas (CHIANG; ZHAND, 2016).

Diante do avanço digital, a tendência é que tudo se torne digital, mais eficientee transparente. Desse modo, os responsáveis pela administração pública, de estados e municípios, devem estar atentos aos novos modelos de gestão e conectividade.

Neste cenário, buscar alternativas eficientes para que as informações sejam apresentadas com transparências e de modo seguro é necessário a utilização de tecnologias capazes de tal realização. Uma das alternativas possíveis para solução de problemas e proteção de dados, estão nas chamadas tecnologias *Blockchain*, que recentemente recebeu atenção por fornecer alternativas promissoras. Blockchain é baseado em uma rede ponto a ponto, ou P2P (*Personal to Personal*) que usa criptografia para fornecer segurança descentralizada.

Portanto, este trabalho busca elencar a utilização das tecnologias Blockchain para como solução para redes da administração pública de modo que possa proporcionar mais segurança e eficiência para os gestores públicos.

Justificativa

Este trabalho justifica-se pela relevância do tema abordado, tendo em vista a importância da segurança das informações no que tange o direito digital. Com o grande volume de informações na rede e o crescimento de ataques virtuais, são necessários meios e ferramentas para proteção desses dados, tanto fisicamente quanto legalmente.

Segundo Pereira (2005), para garantir a segurança da informação em ambiente digital constitui, cada vez mais, uma preocupação geral e que necessita a colaboração de todos os envolvidos no processo, ou seja, organismos públicos, privados, universidades, empresas e até pelos cidadãos, de forma individual ou coletiva.

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

Com o Marco Civil da Internet denominado pela Lei 12965/2014, que regulamenta o uso da internet no Brasil, poucas legislações tratam do assunto e nãogarante com precisão medidas que devem ser utilizadas para a proteção contra crimes digitais.

Dessa forma, os riscos e ameaças existentes não tem fronteiras de natureza geográfica, política, linguística ou até mesmo digital, o que configura um aumento naquantidade de informação em formato digital disponível na internet, levando tambéma um crescimento das estratégias de promoção da segurança e redução do risco (PEREIRA, 2005).

Diante desse cenário, o crescimento do direito digital como ferramenta de gestão de risco e de governança tem tido alta relevância, tendo como característica estar orientado por regulamentações, contratos legais e leis.

Para Pinheiro (2012), as empresas passaram a enfrentar a problemática trazida pela perda do monopólio da ferramenta de trabalho e os dados podem ser vazados muito facilmente, pois, com o alto consumo e o barateamento do acesso aos recursos essenciais do modelo de produção digital, qualquer colaborador pode se tornar um concorrente da noite para o dia, levando consigo o conhecimento adquirido.

Metodologia

De acordo com Minayo; Deslandes; Gomes (2015, p.16), a metodologia pode ser entendida como o caminho através do pensamento e a prática exercida na abordagem da realidade. Sendo assim, pode-se afirmar que a metodologia inclui simultaneamente a teoria da abordagem (o método), os meios como sendo os instrumentos de operacionalização do conhecimento (as técnicas) e a criatividade do pesquisador (sua experiência, sua capacidade pessoal e sua sensibilidade).

Ubirajara (2014, p. 27), a pesquisa pode ser caracterizada quanto aos objetivos ou fins, ao objeto ou meios e também correlação com à abordagem dos dados. Diante disso, este trabalho pode ser caracterizado como pesquisa explicativa, pois tem como foco identificar os fatores que determinam ou contribuem para a ocorrência de um fenômeno (UBIRAJARA, 2014). Neste caso, trata-se de identificar os fenômenos quepodem melhorar o gerenciamento da qualidade na administração de materiais com foco nas empresas de cosméticos.

Em relação aos objetos ou meios, pode-se dizer que este é trabalho bibliográfico, pois é desenvolvido através de fontes já estruturadas em formas de livros acadêmicos, publicações e artigos científicos, bem como em lei, doutrina ou jurisprudência.

Foram selecionados artigos científicos, extraídos de busca realizada no Google

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

Acadêmico a partir das seguintes palavras-chave: “Blockchain, Segurança da informação, Redes, Proteção de dados”; livros acadêmicos dos autores Robert Alexy,Danilo Doneda, Alessandro Hirata; bem como websites de jurisprudência.

Utilização de Redes Blockchai na Administração Pública para Proteção das Informações
Administração Pública

A administração pública, segundo Meirelles (2020), é o aparelhamento organizado, ordenado e preordenado pelo Estado afim de fazer a máquina publica se movimentar com o objetivo de atender as demandas da sociedade. Portanto, ela é parte do corpo de órgãos criados para pôr em prática os objetivos do governo. Já o estado, pode ser dito como a pessoa jurídica de direito público posicionada no topo da organização de um país, e que abarca todas as instituições e entes que administram a coisa pública (LIMA, 2020).

Neste contexto, a Administração Pública é fundamental pois é a base do Estado, sendo a parte estrutural que operacionaliza e concretiza as demandas da sociedade. Sendo a base do Estado, está subordinada à Constituição Federal de 1988 que traz em si um capitulo próprio sobre ela.

Dentre os pontos apontados pela Constituição de 1988 sobre a administração pública, tem-se previsões quanto aos cargos, as atividades e atuação dos seus servidores, regime próprio de previdência e estabilidade, no que tange à disposição de que a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios deverá obedecer e ser vigilante quanto aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência (BRASIL, 1988).

O princípio de legalidade, segundo Moura (2012), rege que todas as ações doEstado devem estar pautadas e fundamentadas na lei, consequentemente na Constituição, ou seja, qualquer decisão ou ação deve seguir o que determina o textoda lei, de modo a evitar eventuais afrontas e garante uma maior segurança jurídica atodos que estão submetidos ao Estado.

O princípio de impessoalidade, de acordo com Meirelles (2020), também denominado de princípio da finalidade administrativa, elucida que o administrador público só deve praticar as ações ou atos para seu fim legal, ou seja, com base na leie não levando em conta julgamento pessoal e interesses individuais.

Para Lino (2014), o princípio de moralidade rege que o administrador tenha o dever de ser ético, evitando assim atos incompatíveis com a atuação da Administração Pública.

O princípio de publicidade, para Lima (2020), diz que os atos públicos devem ter publicidade, ou seja, todas as ações devem ser de conhecimento da

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

sociedade. Para Moura (2012), essa publicidade só é válida se for no sentido de produzir efeitosjurídicos, a exemplo do Diário Oficial, conhecido e passível de visualização da sociedade. Por fim, o princípio de eficiência, abarca como sendo uma tentativa de melhorar a prestação de serviços na sociedade, de modo a melhor empregar o dinheiro público (LIMA, 2020).

Nos últimos anos, com a expansão da tecnologia e com a necessidade de adaptação da administração pública aos meios digitais, houve a necessidade de acelerar a movimentação da operacionalização da máquina pública, tendo em vista que muitos processos ainda são muito burocráticos e morosos, pois são muitos caminhos, formulários, documentos e agentes públicos envolvidos no que deveria ser uma simples resolução de demanda administrativa.

Para Heckert e Aguiar (2016), com uma maior exploração das Tecnologias da Informação e Comunicação (TICs) e com uma conscientização política da sociedade, esses recursos estão modificando a relação entre sociedade e Estado, tornando as atividades públicas mais transparentes.

De acordo com Nobre Júnior (2017) só a publicação dos atos oficiais não os torna transparente, é necessário objetividade, eficácia e o controle, sendo o foco de uma administração pública seja translúcida, cristalina, de modo que a sua atuação seja visível para a sociedade, possibilitando a defesa de direitos subjetivos, a participação eficiente no procedimento administrativo e o acesso à informação da ação administrativa.

Diante disso, tornar as informações transparentes e seguras é necessário quea administração pública adote ferramentas que possam melhorar a entrega de informações para o usuário.

Redes Blockchain

O blockchain consiste em um banco de dados descentralizado e distribuído, que permite manter os registros de forma imutável e inviolável, proporcionando robustez, segurança e transparência. A criptografia é usada para vincular blocos paraformar uma rede ponto a ponto (P2P) para manter esses registros.

Mougayar (2018) define o termo blockchain de forma diferente a partir de três perspectivas apresentadas no Quadro 1.

Quadro 1 - Diferentes perspectivas sobre definição de Blockchain.

Perspectiva	**Definição**
1. Técnica	Base de dados de *back-end* que mantém um registro distribuído abertamente.
2. Corporativa	Rede de trocas para valores em movimento entre partes.

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

3. Legal	Um mecanismo de validação de transações que não requer apoio de intermediários.

Fonte: Adaptado de Mougayar (2018)

Trata-se de uma mudança de paradigma que ainda está em andamento, pois propõe uma nova forma de negociação que desafia os modelos consagrados que existem há muitos anos. A principal inovação trazida pelo blockchain é fornecer confiança sem a necessidade de uma organização central, o que tem muitas implicações.

O modelo de confiança atual é baseado em uma entidade confiável que se concentra neste conceito. Um exemplo da esfera social é o controle das transações financeiras, que são regidas por regras estabelecidas e contam com instituições bancárias, que realizam transações entre clientes e atuam como intermediárias entre eles. Outros exemplos incluem governos, que se definem como pontos de controle e autoridades confiáveis. Também podem ser mencionados os notários, que atuam como intermediários entre duas partes que desejam realizar transações e celebrar contratos por meio de contratos.

O problema desse modelo é que ele conta com participantes centralizados, que são responsáveis por garantir a confiança do sistema. Blockchain fornece uma mudança de paradigma ao introduzir essa camada de confiança em um modelo distribuído, de modo a realizar a transferência direta, confiável e segura de ativos.

Cada membro da rede possui uma cópia da base de dados, que será continuamente atualizada e verificada. Por se tratar de uma rede P2P, é de natureza distribuída, não é controlada por uma entidade central e não existe um único ponto de falha (SAGHIRI et al., 2018).

O conceito de criptografia assimétrica também é um dos fundamentos do conceito. A identidade de um usuário blockchain é definida por um par de chaves de criptografia (uma privada e uma pública). A chave privada é utilizada para assinar transações na rede, enquanto a chave pública representará o usuário, por exemplo, no caso do Bitcoin, representa a carteira do usuário. Isso permite o anonimato e traz privacidade para a web.

Seu funcionamento é baseado em transações, blocos, hash e miner. As transações são operações criadas pelos participantes do sistema. Pode ser uma troca, transferência bancária ou qualquer outro tipo de informação que venha a ficar registada no sistema (BANAFA, 2017). Essas transações são registradas em blocos, e o bloco a ser inserido na cadeia precisa ser verificado.

A causa ou causa é um conjunto de blocos formando uma cadeia, na qual são feitos os registros de transações que constituem o banco de dados do blockchain. Todos os usuários podem acessar esse banco de dados público e distribuído.

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

Uma vez que as informações são inseridas em um bloco e o bloco é verificado e vinculado à rede, ele não será mais modificado, apenas novas informações serão adicionadas. Cada bloco é composto por informações do bloco anterior e possui um hash usado como link entre os blocos anteriores. O Hash garante a integridade das informações sem ter que analisar todos os dados. Todo o histórico de transações é armazenado no razão, portanto, os registros são considerados imutáveis.

A verificação do bloco ocorre durante o processo de mineração. Os mineiros são entidades responsáveis por usar recursos de computação caros para resolver problemas matemáticos complexos. O processo de resolução desses problemas depende do algoritmo de consenso utilizado. Os mais famosos são o teste de trabalhoe o teste de equidade.

Tipos de Blockchain

O blockchain pode ser classificado de acordo com o tipo de acesso aos dadose o processo de verificação envolvido no bloco para cadeia. Quanto ao tipo de acesso, pode ser público, que é baseado em uma rede pública, ou seja, qualquer usuário pode fazer parte da rede, ou privado, que é restrito, ou seja, apenas alguns usuários podem participar.

Quanto à participação no processo de verificação de bloqueio, ela pode ser: autorizada ou não autorizada. No primeiro caso, qualquer usuário pode ser um validador ou minerador, enquanto no segundo caso, apenas alguns usuários podem exercer tal função (MACHADO, 2018).

Embora a tecnologia blockchain seja normalmente citada pela rede Bitcoin ouassociada à criptomoeda, várias redes têm sido propostas e utilizadas para os maisdiversos cenários. Exemplos de blockchains públicos e não licenciados são Bitcoin eEthereum, enquanto Hyperledger e Ripple são licenciados (CHICARINO et al., 2017).

Dias (2019) propõe uma análise comparativa entre as principais tecnologias ou plataformas de blockchain porque são citadas no trabalho. Nesta comparação, conforme mostrado na Figura 1, o domínio de aplicativo de cada plataforma, classificação de permissão, algoritmo de consenso usado, linguagem usada paradesenvolver contratos inteligentes (ou contratos inteligentes), se aplicável, o ambientede execução de contrato inteligente, modelo de dados e o nome de a criptomoeda, caso seja aplicável.

Figura 1 - Tipos de Blockchain e comparação entre diversas tecnologias

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

Plataforma	Domínio	Tipo de *blockchain*	Mecanismos de consenso	*Smart contracts*	Ambiente de execução de *smart contracts*	Modelo de dados	Cripto moeda
Bitcoin	Cripto moeda	Sem permissões	PoW	–	–	UTXO	BTC
Ethereum	Aplicações descentralizadas Cripto moeda	Sem permissões	PoW	Solidity	EVM	Conta de utilizador	ETH
Quorum	Múltiplos setores	Com permissões	Raft IBFT	Solidity	EVM	Conta de utilizador	–
Hyperledger Fabric	Múltiplos setores	Com permissões	Framework conectável	Java Node.js Go	Dockers	Conta de utilizador	–
Corda	Serviços financeiros	Com permissões	Framework conectável	Java Kotlin	JVM	UTXO	–
Ripple	Cripto moeda	Com permissões	Sistema de votos probabilísticos	–	–	UTXO	XRP
Tezos	Aplicações descentralizadas Cripto moeda	Sem permissões	PoS	Michelson	Dockers	Conta de utilizador	Tezos
BigchainDB	Múltiplos setores	Com permissões	Tendermint	–	–	Conta de utilizador	–

Fonte: Adaptado de Dias (2019)

Crimes cibernéticos e Criptomoedas

Na verdade, o crime cibernético existe desde o advento da Internet e sempre foi uma preocupação geral do governo e da sociedade, porque qualquer pessoa no mundo que usa dispositivos eletrônicos será afetada por certos tipos de atividades criminosas, como atividades ilegais de hackers.

De acordo com Ghassan Dreibi, gerente de desenvolvimento da Cisco, uma empresa especializada em soluções de telecomunicações, “da maneira como nos relacionamos com a Internet hoje, quase todo mundo pode estar infectado”. Além disso, o hacking pode afetar de forma universal A ordem social é não afetando apenas indivíduos individualmente. Por exemplo, na queda de energia no Espírito Santo em setembro de 2007, a agência de inteligência dos Estados Unidos atribuiu o incidente às ações de terroristas cibernéticos. O ataque resultou em assaltos a lojas, acidentes de telefones celulares, caos no trânsito e desabamento de hospitais. Nesse caso, existe a criptomoeda, que é um novo tipo de moeda digital que não pode ser controlada por não estar vinculada a nenhum tipo de banco estadual, facilitando assim as transações. Além disso, outro fator que atrai a atenção dos usuários para o uso de tais moedas são as suas cotações, que geralmente são mais valiosas do que as moedas físicas, precisamente porque não são tributadas e não são regulamentadas pelo banco central.

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

Diante dessa situação, juristas, autoridades fiscais e reguladores legais estãocada vez mais preocupados com a incerteza dessas moedas nos campos jurídico e econômico, especialmente em termos de comportamento ilegal. No entanto, apesar das características duvidosas da criptomoeda, muitos países a reconheceram em seus cenários econômicos e os supervisionaram adequadamente para evitar tais atos anti-legais. Em relação à padronização da moeda digital, a especialista em direito digital do INSPER e a especialista em blockchain e design thinking Tatiana Trícia dePaiva Revoredo, da Blockchain Academy, anunciaram:

> Um estudo recente realizado em mais de 60 países mostrou que alguns países parecem ter aceito e reconhecido com segurança as criptomoedas (Holanda, Argentina, Bélgica, Bulgária, Vietnã, Alemanha, Israel, Canadá, Luxemburgo, Noruega, Cingapura, França, Finlândia, República Tcheca República, Suécia e Japão), enquanto outros países expressaram apenas opiniões positivas sobre o assunto (Polônia). [...]. Também há dúvidas sobre se a qualidade da criptomoeda é durável. europarl.europa.eu europarl.europa.eu thumb up thumb down. Finalmente, alguns governos querem ou estão proibindo-os em seu território (China, Jordânia), enquanto outros governos os baniram efetivamente em seus territórios (Tailândia). (Revoredo, 2017).

O crime mais comum envolvendo criptomoeda é explorar essas moedas digitais sem consentimento, instalar programas no computador sem o conhecimento do proprietário e criar anúncios e anúncios falsos com o objetivo de espalhar pragas e infectar computadores. Outra prática comum é resgatar dados roubados. Os criminosos infectam o computador da vítima com malware (software nocivo) e sequestram seus dados, bloqueando o acesso para que ele possa solicitar o resgatedessas informações. Trata-se do uso de moeda virtual que deve ser paga., O que torna difícil rastrear comportamentos ilegais.

> O crime cibernético pode ser dividido em: apropriado ou inapropriado. A primeira é a ofensa criminal que existe apenas no campo do ciberespaço, como os ataques de negação de serviço-negação de serviço (DOS). A má conduta se refere ao uso de tecnologia como meio de comportamento criminoso. Um bom exemplo desse tipo de crime são as ameaças feitas por e-mail. (Andrade, 2015, p. 1).

Portanto, é importante destacar que embora a Internet e a tecnologia proporcionem muitos benefícios aos seus usuários, o mundo virtual ainda é um localde enormes riscos. Relacionado a isso está a criptomoeda. Embora não seja uma moeda criada para esse fim, tornou-se mais uma ferramenta do crime cibernético devido à falta de supervisão nacional.

Utilizaçao e limitaçoes do Blockchain

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

O blockchain pode apresentar diversas utilizaçoes além das criptomoedas, de modo que cada aplicaçao pode se tornar uma vantagem ou desvantagem (BOVÁRIO; SILVA, 2018). Segundo Bichara (2018), a tecnologia blockchain pode trazer simplicidade no comprimento das obrigaçoes tributárias no Brasil, de modo que a confiança dos dados disponibilizadas na rede pode facilitar o trabalho de fiscalizaçaoao reduzir a margem para evasao fiscal.

Dados da Federação Brasileira de Bancos (FEBRABRAN, 2020) juntamente com a Deloitte expos dados relevantes em ao crescimento tecnológico no ano de 2019. Segundo a pesquisa, os bancos aumentaram em 48% os investimentos em tecnologia tanto em *software* como em *hardware*. O investimento em novas tecnologias correspondeu a 20% em Internet das Coisas (IoT), 35% em blockchain, 35% em Robotic Process Automation (RPA) para processos backofficee 72% em Inteligência Artificial.

Gates (2017) lista uma série de atividades que o blckchain pode desempenharem algumas instituiçoes no mundo, no que corresponde a área financeira:

- Transferências de valor entre companhias e países pode se beneficiar com o aumento da velocidade das transações usando a tecnologia blockchain.
- A substituição das várias camadas de autenticação pela tecnologia blockchain pode dar transparênciaas diversas transações
- A utilização da tecnologia blockchainpara substituir intermediários no mercado de compra e vendas de ações.
- Livros-razão manuais sendo substituído pela tecnologia tanto em administrações públicas como em privadas.

Segundo Lima (2020), o papel que a blockchain pode desempenhar para contribuir para que o Brasil atinja o ideal de transparência dos atos e informações públicas é justamente de intermediária da informação. Também é evidente que a tecnologia não explicará os dados e as informações, mas sim como ela, associada auma inteligência artificial que selecione qual informação é de interesse de quem, porexemplo, é capaz de, assim que os atos públicos e a informação pública passam a existir, enviar instantaneamente essa informação para o celular do cidadão (LIMA, 2020).

Desse modo, quando se trata dos possíveis impactos da tecnologia blockchain na administração pública, a transparência de dados é um dos principais fatores, conforme Figura 2.

Figura 2 - Principais impactos da utilização da tecnologia blockchain na

REVISTA PROCESSUS MULTIDISCIPLINAR

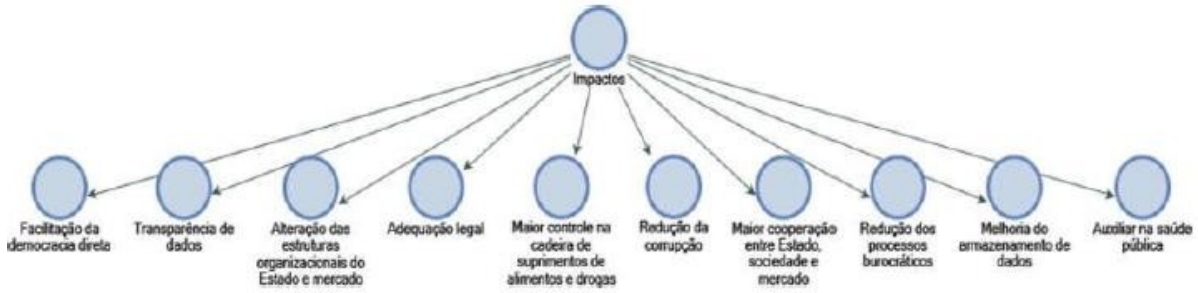
PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

administração pública



Fonte: Adaptado de Moura; Brauner; Janissek-Muniz (2020)

Privacidade e risco

Privacidade refere-se a vários conceitos, incluindo retenção fora da esfera social, proteção do conhecimento de outras pessoas e proteção de indivíduos contradanos. No âmbito jurídico, trata-se do direito de estar sozinho e sozinho (HIRATA, 2017). Por muito tempo, a proteção da privacidade foi um tema secundário, nem valea pena, e só se tornou relevante no final do século 19 (DONEDA, 2006).

O autor propõe outras definições, como Shils (2006), que associa a privacidadeà interação, comunicação e percepção, em que existe uma relação zero. Gavison(1980) propôs que o conceito pode ser estabelecido a partir dos aspectos quantitativos relacionados a alguém (informação, atenção e contato físico) e determinar os três componentes da privacidade: confidencialidade, anonimato e isolamento. Segundo Garvison (2008), esses elementos são independentes, mas que se relacionam entre si.

Vários autores distinguem entre intimidade e privacidade. Segundo Dotti (2010), a intimidade está inserida na vida privada, esses dois conceitos serãodefinidos como dois círculos, sendo que o menor é a representação da intimidade - ateoria dos círculos concêntricos. Atendendo à proposta do autor, a intimidade será mais interna, enquanto a vida privada abrangerá outros aspectos. A intimidade éregida pelo princípio da exclusividade, que possui três atributos: estar só, que serefere ao desejo de ficar só; confidencialidade, que se refere à exigência de sigilo; eautonomia, que se refere à liberdade de decidir se fazer de si mesmo o centro de informação (MARQUES, 2010).

Outros autores ainda publicam ideias semelhantes, áreas com mais níveis de proteção ou outra nomenclatura, como mais áreas internas, áreas de vida privada e áreas sociais e públicas (SAMPAIO, 1998). Na entrada, embora a

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

nomenclatura seja diferente, esses termos têm a mesma finalidade, e suas magnitudes são basicamente diferentes (MORAIS, 2002).

Nesse caso, ambos serão usados como sinônimos, ou seja, as referências a privacidade incluem intimidade, honra, imagem, inviolabilidade da casa, comunicação e telegrama, sigilo de dados e comunicações telefônicas. Quando a padronização daterminologia não interfere na análise dos tópicos relacionados, alguns trabalhos também realizaram a padronização da terminologia.

A análise do conceito de privacidade até agora é de âmbito geral, sem considerar o quadro técnico existente. Considerando apenas o contexto humano, na perspectiva dos direitos individuais, já existe muita complexidade, ao adicionar essa camada ao contexto, o foco é ainda maior. Se nos primeiros dias de adoção de tecnologias mais simples, como fotografia instantânea e notícias impressas, as preocupações da sociedade com o fim da vida privada aumentaram, hoje ela atingiu um cenário antes inimaginável.

No contexto da Internet e das Tecnologias de Informação e Comunicação (TIC),o conceito de privacidade está relacionado com a recolha de dados pessoais existentes e o controlo de quem tem acesso a este conjunto de informações. De acordo com a pesquisa de Mekovec e Vrcek (2011), as questões de privacidade online envolvem o tipo e a qualidade das informações coletadas; o controle dessas informações e o conhecimento das práticas de privacidade. Portanto, é necessário fornecer uma forma de controle para os proprietários dos dados e regulamentar o registro e a utilização desses dados por terceiros (LIN et al., 2017).

De acordo com a pirâmide do conhecimento ou estrutura hierárquica DIKW (Data-Information-Knowledge-Wisdom) (ELIOT, 2014), conforme mostrado na Figura3, os dados são a representação dos atributos do objeto na forma original (ACKOFF,2009), formando a base da pirâmide, e após sua o processamento é transformado em informação. Portanto, a proteção de dados é um tópico recorrente e desempenha umpapel importante na privacidade e segurança dos sistemas de computador.

Figura 3 – Pirâmide da Hierarquia DIKW

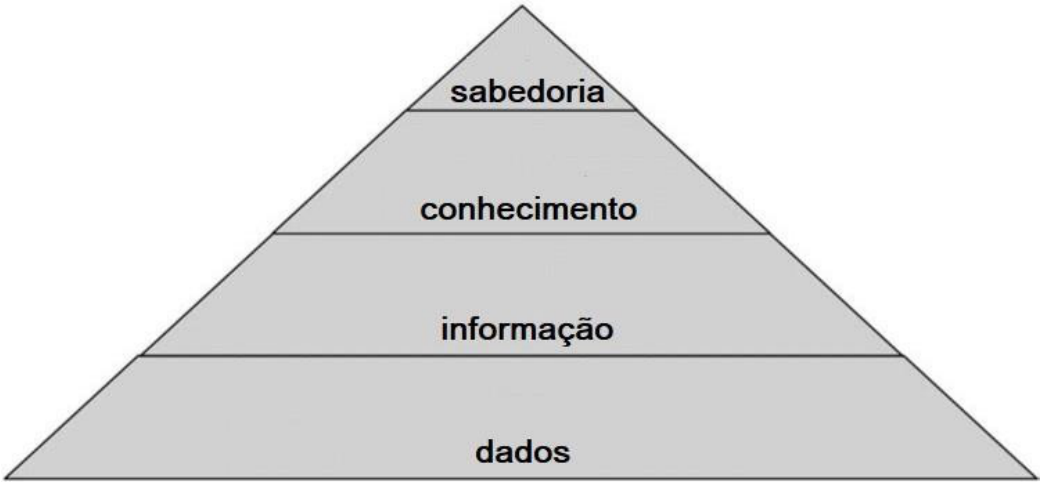
REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021



Fonte: Adaptado de Rowley (2007)

Com o desenvolvimento da tecnologia de comunicação de dados, a quantidade de dados coletados, processados, manipulados e transmitidos atingiu uma escala sem precedentes. Devido à aplicação da computação pervasiva e à transparência das formas de interação com esses sistemas, esses dados são coletados de forma inconsciente por seus proprietários e, muitas vezes, sem consentimento, o que podeter múltiplas consequências.

Solove (2008) propôs uma taxonomia de privacidade baseada em quatro grupos de atividades que podem causar problemas de privacidade:

- coleta de informações;
- processamento de informações;
- disseminação de informações;
- intrusão.

Como pode ser visto na Figura 4, essas atividades estão relacionadas a doisparticipantes:

1. detentores de dados, que são indivíduos diretamente afetados pelas atividades de taxonomia;
2. detentores de dados, que representam entidades (outros, empresas, governos) coletam e processar esses dados.

Figura 4 - Taxonomia da privacidade.

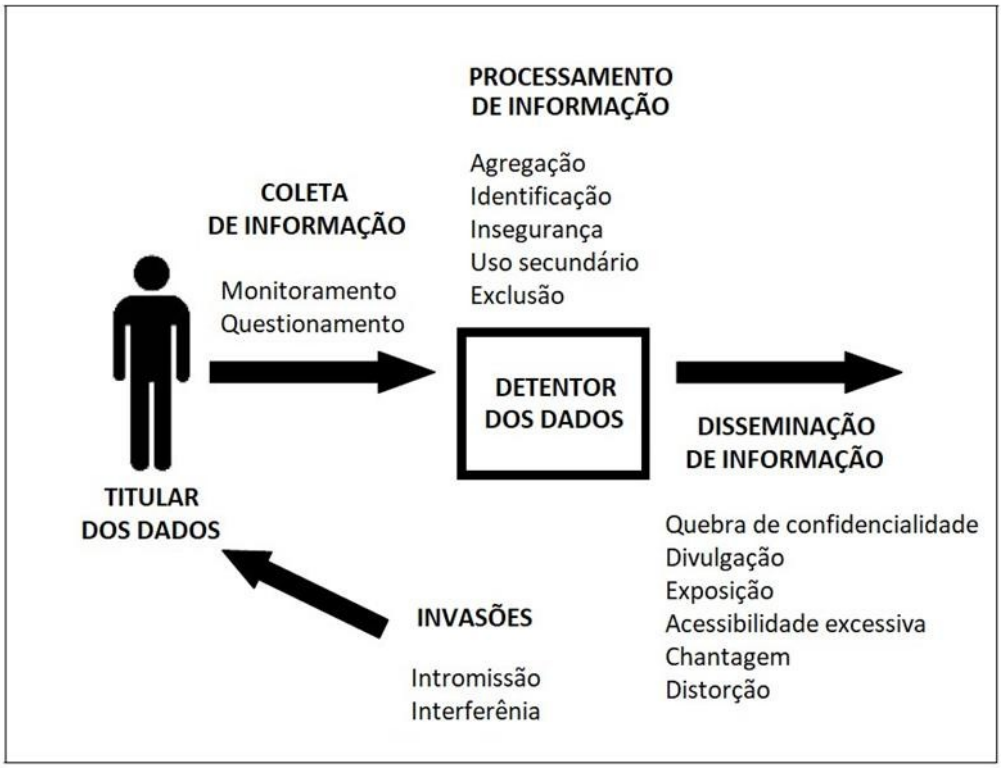
REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021



Fonte: Adaptado de Solove (2008)

O primeiro grupo de atividades (coleta de informações) está relacionado à coleta de dados. A coleta pode ser feita através do monitorando ou perguntas. Vigilância inclui observar, ouvir e registrar atividades pessoais. Por sua vez, fazer perguntas baseia-se na obtenção direta de informações e em fazer perguntas aos indivíduos.

O segundo grupo de atividades (processamento de informações) envolve o uso, armazenamento e manipulação dos dados coletados, e pode ser realizado de cinco formas diferentes:

- Agregação, ou seja, a combinação de dados sobre uma pessoa de diferentes fontes;
- Identificação, incluindo informações de contato de um indivíduo específico;
- Inseguro, que é o descuido ao proteger as informações armazenadas;
- Uso secundário, o que significa que as informações coletadas serão utilizadas para fins não acordados pelo proprietário;
- Exclusão, ou seja, não informar o titular dos dados que outras pessoas possuem sobre ele.

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

O terceiro grupo de atividades (divulgação de informações) refere-se à divulgação de dados pessoais ou simplesmente ameaças à divulgação dessas informações. Isso pode acontecer de seis maneiras diferentes:

- Violação de confidencialidade;
- Divulgação;
- Exposição;
- Acessibilidade excessiva;
- Aceitar subornos;
- Distorção.

Como o nome indica, uma violação da confidencialidade é uma violação da promessa de manter as informações do titular confidenciais; divulgação é a divulgação de informações confiáveis que afetam a forma como os outros julgam seu caráter (ou seja, imagem pessoal); a exposição inclui corpo nu, nudez ou outras funções físicas e até pesar ou dor pessoal.

Acessibilidade excessiva é definida como maior acesso a informações pessoais; chantagem é uma ameaça de vazamento de informações pessoais; desfalque é o uso da identidade do titular em benefício de terceiros; distorção é a disseminação de informações falsas sobre indivíduos.

Por fim, o quarto grupo de atividades refere-se a intrusões em assuntos privados relacionados ao titular dos dados. A invasão pode ocorrer de duas maneiras:

- Invasão, ou seja, perturbando a paz e o isolamento de alguém;
- Intervenção, ou seja, o governo intervém na decisão de um indivíduo sobre seus assuntos privados.

Ponciano et al. (2017) Discutindo privacidade no contexto da Internet das Coisas, e após pesquisar usuários e realizar uma análise extensa sobre este tópico, listou três questões principais de privacidade do usuário em um sistema típico de Internet das Coisas, sao elas: coleta de dados, Inferir informações dos dados coletados e compartilhar informações do usuário com terceiros.

A coleta de dados citada neste trabalho segue um modelo semelhante ao modelo descrito na Taxonomia de Privacidade Solove (2008) mencionada acima, pois é baseada na coleta indireta por meio de dispositivos do usuário e coleta direta por meio de perguntas. Inferência é a descoberta de novas informações por meio de dados coletados do usuário, que podem ser usados para diversos fins, como identificação de amigos do usuário e publicidade (como recomendação de produtos e serviços). Finalmente, o compartilhamento de informações do usuário com terceiros pode ocorrer como parte da operação do sistema ou devido a mau funcionamento.

Rosner (2016) revelou seis riscos de privacidade no contexto da Internet of Things:

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

- vigilância intensiva,
- coleta de dados não autorizada;
- coleta de informações médicas de informações;
- interrupção do contexto de informação;
- diversificação das partes interessadas;
- supervisão do governo.

Esses riscos estão listados na Quadro 2.

Vale ressaltar alguns pontos relacionados aos riscos listados. Relacionado aorisco de vigilância forte está o direito à privacidade sob o direito de ficar sozinho. Quanto aos riscos da "coleta de dados não consensual, também é possível discutir dados de crianças e adolescentes, o que se soma à gravidade deste ponto.

Quanto ao risco de coleta de informações médicas, o cenário da aplicação é que sensores de baixo custo (como em relógios ou telefones celulares) capturem dados relacionados à saúde humana e combinados com a aplicação de tecnologia de mineração de dados para gerar informações confiáveis sobre saúde pessoal. Como resultado, os consumidores enfrentam vários riscos e são vulneráveis a constrangimento, danos à reputação e discriminação.

Quadro 2 - Riscos à privacidade

Risco	Descrição
1. Monitoramento intenso	Aplicação intensa do sensoriamento, dispositivos conectados para monitoramento da atividade humana.Rastreamento de todos os movimentos das pessoas.
2. Coleta de dados não consentida	Dados de qualquer natureza são coletados, devem haver autorização do titular dos dados, utilização para fins comerciais.
3. Coleta de informações médicas	Dados de dispositivos comuns (e.g. batimentos cardíacos, padrões de soo, pressão sanguínea) se distinguem de informações médicas? Não deveriam estar submetidos à mesma regulamentação? Informações médicas são dados sensíveis que, se divulgadas, colocam os consumidores em posição devulnerabilidade à constrangimento e danos.
4. Quebra de contextos da informação	Risco gerado pela “fusão de sensores”. Dados de diferentes contextos são reunidos e geram novas informações acerca do indivíduo. Desrespeito do limite das informações de cada contexto é uma

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

	violação à privacidade.
5. Diversificação dos *stakeholders*	Elevado volume de dados sendo gerenciado por atores com pouca ou nenhuma experiência sobre políticas de segurança e privacidade.
6. Vigilância governamental	Possível transferência dos dados coletados por empresas privadas para o governo, através de requisição legal.

Fonte: Adaptado de Rosner (2016)

Para complementar os riscos e desafios, Tzafestas (2018) listou uma lista de recursos da Internet das Coisas que podem causar problemas éticos. A lista é mostrada no Quadro 3, incluindo recursos e respectivas descrições.

Os três recursos mencionados no trabalho de Witkowski (2017) trazem atenção adicional às questões de segurança e privacidade da IoT. Devido à sua onipresença,é difícil enxergar as fronteiras entre os espaços públicos e privados, além disso, devido às características do contexto, informações sobre diferentes cenas da vida pessoal podem se sobrepor.

Além disso, a otimização pode trazer riscos, dependendo da resposta dada pelo sujeito, e considerando a concessão de permissões individuais aos afetados com base nas consequências das ações realizadas pelo sujeito, além dos limites e formas de consentimento dado pelo usuário.

Quadro 3 - Características de IoT que podem causar problemas éticos

Característica	**Descrição do problema**
Miniaturização / Invisibilidade	sitivos cada vez menores e transparentes ao usuário, dificultando quaisquer inspeções, auditorias e controle de qualidade
Onipresença / Ubiquidade	ositivos em todos os lugares, limites invisíveis entre os espaços públicos e privados, não se sabe o limite da informação
Ultra conectividade	alta quantidade de dados (Big Data) que pode ser usada de forma maliciosa
Inteligência incorporada	Objetos inteligentes, dinâmicos e com comportamento emergente, substitutos de uma vida social. A privação desses objetos pode trazer problemas

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

Comportamento autônomo	Os objetos podem interferir de forma autônoma e espontânea nasatividades humanas, de formas não esperadas pelos usuários e projetistas
Operação descentralizada	Alto fluxo de informação e transferência de dados, dificilmente controlado. Faz-se necessário monitoramento e gerenciamento demodo adequado
Identificação	Objetos possuem uma identidade para se conectarem à rede. O acesso a esses objetos e o gerenciamento dessas identidades podecausar problemas cruciais de segurança e controle
Ambiguidade	naturais, artefatos e humanos será cadavezmais difícil

Fonte: Adaptado de Tzafestas (2018)

Referências

ACKOFF, Russell L. From data to wisdom. Journal of applied systems analysis, v. 16,n. 1, p. 3-9, 1989. (ACKOFF, 1989).

ALEXY, Robert. Teoria dos direitos fundamentais. 2008. (ALEXY, 2008).

ANDRADE, Leonardo. Cybercrimes na deep web: as dificuldades jurídicas de determinação de autoria nos crimes virtuais. Revista Jus Navigandi, jun. 2015. Disponível em: <https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicas-de-determinacao-de-autoria-nos-crimes-virtuais/4>. Acesso em: 25/05/2021. (ANDRADE, 2015)

BANAFA, Ahmed. IoT and blockchain convergence: benefits and challenges. IEEE Internet of Things, 2017. (BANAFA, 2017).

BEVILACQUA, Lucas; GOMES, Rayanne Ribeiro. A UTILIZAÇÃO DA TECNOLOGIABLOCKCHAIN NAS RELAÇÕES TRIBUTÁRIAS NO BRASIL. Revista de Direitos
Fundamentais e Tributação, v. 1, n. 3, p. 65-92, 2020. (GOMES, 2020).

BICHARA, Luiz Gustavo A. S.A relação entre blockchaine obrigações acessórias. Osdesafios da simplificação tributária no Brasil. In: Revista dos Tribunais | vol. 994/2018|p. 527 -542 | Ago / 2018 DTR\2018\16235. (BICHARA, 2018).

BOVÉRIO, Maria Aparecida; SILVA, Victor Ayres Francisco da. Blockchain: uma

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

tecnologia além da criptomoeda virtual. Revista Interface Tecnológica, v. 15, n. 1, p. 109-121, 2018. (APARECIDA, 2018).

BRASIL. Constituição Federal de 1988. Instituiu a Carta Magna.

CISCO. Internet of Things. Cisco. 2016. Disponível em: <https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf>. Acesso em: 30/05/2021.

CJF (Conselho de Justiça Federal). VI Jornada de direito civil. Brasília, 2013. Disponível em: <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/vijornadadireitocivil2013-web.pdf>. Acesso em: 30/05/2021.

CONTI, Mauro et al. Internet of things security and forensics: Challenges and opportunities. (ELSEVIER, 2018).

DIAS, R. P. N. Análise de plataformas blockchain. Dissertação (Mestrado em Engenharia Informática) – Faculdade de Ciências e Tecnologia, Universidade de (COIMBRA, 2019).

DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: (RENOVAR, 2006).

DOTTI, R. A. Proteção da vida privada e liberdade de informação: possibilidades e limites. Editora Revista dos Tribunais. São Paulo: RT, 1980. (DOTTI, 1980).

ELIOT, T. S. The Rock, chapter Part I. London: Faber & Faber, 1934. (ELIOT, 1934).

ELKHODR, M.; SHAHRESTANI, S.; CHEUNG, H. The internet of things: new. (ELKHODR, 2016).

FEBRABAN. DELOITTE. Pesquisa FEBRABAN de Tecnologia Bancária 2020. Disponível em < https://www2.deloitte.com/content/dam/Deloitte/br/Documents/financial-services/Pesquisa-FEBRABAN-Tecnologia-Bancaria-2020.pdf> Acesso em16.06.2021. (FEBRABAN, 2020).

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

GATES, Mark. Blockchain: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money. Breinigsville, Pensilvânia: Createspace Independent Publishing Platform. 2017. 126 p. (GATES, 2017).

GAVISON, Ruth. Privacy and the Limits of Law. The Yale law journal, v. 89, n. 3, p. 421-471, 1980. (GAVISON, 1980).

GUBBI, Jayavardhana et al. Internet of Things (IoT): A vision, architectural elements,and future directions. Future generation computer systems, v. 29, n. 7, p. 1645-1660,2013. (GUBBI, 2013).

HE, H. et al. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In: 2016 IEEE Congress on Evolutionary Computation (CEC). IEEE. 1015-1021, 2016.

HECKERT, Cristiano Rocha; AGUIAR, Everson Lopes de. Governança Digital na Administração Pública Federal: uma abordagem estratégica para tornar o governo digital mais efetivo e colaborativo - a ótica da sociedade. In: IX Congresso CONSAD de Gestão Pública, 2016, Brasília. Anais do IX Congresso CON SAD de Gestão Pública. Brasília: Consad, 2016. p. 1-60, p. 3. (ROCHA, 2016).

HIRATA, A. Direito à privacidade. Enciclopédia jurídica da PUC-SP. 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. interoperability, management and security challenges. International journal of. (HIRATA, 2017).

KHAN, Minhaj Ahmad; SALAH, Khaled. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, v. 82, p. 395-411, 2018. (AHMAD, 2018).

LIN, Jie et al. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, v. 4, n. 5, p. 1125-1142, 2017. (LIN, 2017).

LINO, Estevão José. Princípios Constitucionais da Administração Pública: como o princípio da legalidade afeta o agir eficiente do gestor público? 2014. 71 f.,

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

Monografia (Especialização) - Curso de Gestão Pública Municipal, Universidade Tecnológica Federal do Paraná, Curitiba, 2014. p, 39. (JOSÉ, 2014).

LIU, Chang et al. External integrity verification for outsourced big data in cloud and IoT: A big picture. Future generation computer systems, v. 49, p. 58-67, 2015. (LIU, 2015).

MACHADO, R. N. Análise sobre otimização de blockchain para internet das coisas. 2018. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação), Universidade Federal de Pernambuco, 2018. (MACHADO, 2018).

MARQUES, A. N. G. Direito à intimidade e privacidade. Jus vigilantibus, 2010. (MARQUES, 2010).

MCKINSEY & COMPANY. Growing opportunities in the Internet of Things. Copyright©1996-2020 McKinsey & Company. Julho de 2019. Disponível em: <https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things>. Acesso em: 30/05/2021.

MEIRELLES, Hely Lopes. Direito Administrativo Brasileiro. 44. ed. São Paulo: Juspodivm, 2020. 824 p., p, 61-62. (LOPES, 2020).

MEKOVEC, R.; VRČEK, N. Factors that influence Internet users' privacy perception. In: 33rd International Conference on Information Technology Interfaces. Proceedingsof the ITI 2011. IEEE. 227-232, 2011. (MEKOVEC, 2011).

MINAYO, Maria Cecília de Souza; DESLANDES, Suely F.; GOMES, Romeu. Pesquisa social: teoria, método e criatividade. 34o Edição. Petrópolis/RJ: Vozes, 2015. (SOUZA, 2015).

MORAIS, A. de. Direito constitucional. 12. ed. 80 p. São Paulo: Atlas, 2002. (MORAIS, 2002).

MOUGAYAR, W. Commercial Blockchain: Promessa, Prática e Aplicação de Nova Tecnologia de Internet. Rio de Janeiro: Alta Books Editora, 2018. (MOUGAYAR, 2018).

MOURA, Andréa Félix Batista de. Os Princípios da Administração Pública Brasileira

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

e Suas Relações com o Setor Privado. 2012. 71 f., Monografia (Especialização) - Curso de Gestão Pública Municipal, Universidade Estadual da Paraíba, João Pessoa, 2012. p, 20. (BATISTA, 2012).

MOURA, Luzia Menegotto Frick de; BRAUNER, Daniela Francisco; JANISSEK - MUNIZ, Raquel. Blockchain e a Perspectiva Tecnológica para a Administração Pública: uma revisão sistemática. Revista de Administração Contemporânea, [S.L.], v. 24, n. 3, p. 259-274, jun. 2020. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/1982-7849rac2020190171. p, 268. network security & its applications. p. 85-102, 2016. (FRICK, 2020).

NOBRE JÚNIOR, Edilson Pereira. A transparência administrativa e a Lei 12.527/2002
- 10.12818/P.0304-2340.2017V70P249. Revista da Faculdade de Direito da UFMG, [S.L.], v. 70, p. 249-276, 29 dez. 2017. Revista da Faculdade de Direito da UFMG. (PEREIRA, 2017).

PEREIRA, Pedro Jorge Fernandes. Segurança da informação digital. Cadernos BAD, n. 1, 2005. (FERNANDES, 2005).

PINHEIRO, Patricia Peck. Segurança da informação na era digital. GV EXECUTIVO,v. 11, n. 2, p. 54-57, 2012. (PECK, 2012).

PONCIANO, Lesandro et al. Designing for Pragmatists and Fundamentalists: PrivacyConcerns and Attitudes on the Internet of Things. In: Proceedings of the XVI BrazilianSymposium on Human Factors in Computing Systems. p. 1-10, 2017. (PONCIANO, 2017).

RAJ, Pethuru; RAMAN, Anupama C. The Internet of Things: Enabling technologies, platforms, and use cases. CRC Press, 2017. (RAJ, 2017).

REVOREDO, Tatiana Tricia de Paiva. Criptomoeda: cenários e tendências globais. 27 de outubro de 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/criptomoedas-cenario-global-e-tendencias-27102017>. Horário da visita: 25/05/2021. (PAIVA, 2017).

ROSNER, G. Privacy and the Internet of Things. O'Reilly Media, Incorporated, 2016. (ROSNER, 2016).

ROWLEY, Jennifer. The wisdom hierarchy: representations of the DIKW

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

hierarchy. Journal of information science, v. 33, n. 2, p. 163-180, 2007. (ROWLEY, 2007).

SAGHIRI, Ali Mohammad et al. A framework for cognitive Internet of Things based onblockchain. In: 2018 4th International Conference on Web Research (ICWR). IEEE, 2018. p. 138-143. (MOHAMMAD, 2018).

SAKAMOTO, Sarah Gomes. Segurança, Privacidade e Blockchain no Contexto de Internet das Coisas. 2020. 65 p. Monografia de Especialização em Internet das Coisas, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2020. (GOMES, 2020).
SHILS, Edward. Privacy: Its constitution and vicissitudes. Law and Contemporary Problems, v. 31, n. 2, p. 281-306, 1966. (SHILS, 1966).

SICARI, Sabrina et al. Security, privacy and trust in Internet of Things: The road ahead. Computer networks, v. 76, p. 146-164, 2015. (SICARI, 2015).

SOLOVE, D. J. Understanding Privacy. Harvard University Press. 2008. (SOLOVE, 2008).

SWAN, Melanie. Blockchain: Blueprint for a New Economy. Sebastopol, California: O'Reilly Media Inc., 2015. 149 p. (SWAN, 2015).

TZAFESTAS, Spyros G. Ethics and law in the internet of things world. Smart cities, v.1, n. 1, p. 98-120, 2018. (TZAFESTAS, 2018).

UBIRAJARA, Eduardo. Guia de orientação de TCC's. Aracaju: FANESE, 2014.2 (caderno). (UBIRAJARA, 2014).

WEF (Fórum Econômico Mundial). Relatório de risco global de 2020. Copyright © 2020 World Economic Forum. Disponível em: <https://www.weforum.org/reports/the-global- risks-report-2020>. Horário da visita: 28/05/2021.

WEISER, Mark. The Computer for the 21 st Century. Scientific american, v. 265, n. 3,p. 94-105, 1991. (WEISER, 1991).

WITKOWSKI, Krzysztof. Internet of things, big data, industry 4.0–innovative solutions in logistics and supply chains management. Procedia engineering, v. 182, p. 763-769,2017. (WITKOWSKI, 2017).

REVISTA PROCESSUS MULTIDISCIPLINAR

PERIÓDICOS FACULDADE PROCESSUS

Ano II, Vol. II, n.4, jul.-dez., 2021

ISSN: 2675-6595

Data de submissão: 20/10/2021 Data de aceite: 17/11/2021

YANG, Yuchen et al. A survey on security and privacy issues in Internet-of-Things.IEEE Internet of Things Journal, v. 4, n. 5, p. 1250-1258, 2017. (YANG, 2017).

YU, Bin et al. Trustchain: Establishing trust in the iot-based applications ecosystemusing blockchain. IEEE Cloud computing, v. 5, n. 4, p. 12-23, 2018. (YU, 2018).

ZARPELÃO, Bruno Bogaz et al. A survey of intrusion detection in Internet of Things.Journal of Network and Computer Applications, v. 84, p. 25-37, 2017. (BOGAZ, 2017).