Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas
Departamento de Gestão de Políticas Públicas

JULIANA MOREIRA MORAES

Blockchain e o compartilhamento de dados na esfera da Administração Pública Federal Brasileira: análise do bCPF

Brasília – DF
2019

JULIANA MOREIRA MORAES

Blockchain e o compartilhamento de dados na esfera da Administração Pública Federal Brasileira: análise do bCPF

Monografia apresentada ao Departamento de Gestão de Políticas Públicas como requisito parcial à obtenção do título de Bacharel em Gestão de Políticas Públicas.

Professora Orientadora: Doutora Christiana Soares de Freitas

Brasília – DF
2019

JULIANA MOREIRA MORAES

Blockchain e o compartilhamento de dados na esfera da Administração Pública Federal Brasileira: análise do bCPF

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Gestão de Políticas Públicas da Universidade de Brasília do (a) aluno (a)

Juliana Moreira Moraes

Doutora Christiana Soares de Freitas
Professor-Orientador

Doutor Daniel Bin
Professor-Examinador 1

Brasília, 9 de julho de 2019.

“Online identity and reputation will be decentralized. We will own the data that belongs to us.”.

MOUGAYAR, William, 2016, p.159.

RESUMO

A Internet não só revolucionou a forma como os indivíduos executam suas tarefas diárias, compartilham informações e buscam entretenimento, como também representa uma fonte de coleta e tratamento de dados. Alguns entendem que estaríamos vivendo uma Revolução Digital. No âmbito da Administração Pública, percebe-se o desenvolvimento de novas ferramentas de gestão automatizadas marcadas pelo Governo Eletrônico e pelo Plano de Dados Abertos. O chamado Big Data e os metadados, em teoria, asseguram a anonimização dos dados, contudo são usados no mercado crescente de dados pessoais que se sustenta, não exclusivamente, na baixa disseminação de informação para os usuários, gerando um desequilíbrio de poderes. A cultura advinda de um capitalismo de acumulação, combinada com a adoção de inovações tecnológicas, engendraram novas formas de *marketing* e acabaram por moldar inclusive a atuação do Estado por meio da automatização de prestação de serviços, implementação e execução de políticas públicas, bem como do exercício da função de vigilância. Nesse sentido, verifica-se a aplicação da tecnologia *Blockchain* como solução aos problemas que colocam em risco os dados pessoais do usuário e de que forma essa nova tecnologia vem se enquadrando ao panorama de atuação estatal. Será realizado o estudo de caso do bCPF – *blockchain* permissionada e federativa -, desenvolvido pela Dataprev para a Receita Federal e com participação do Conselho de Justiça Federal, em face de doutrina, artigos científicos e documentos que demonstrarem pertinência. Apesar de os estudos acerca da *Blockchain* serem ainda iniciais e superficiais, acredita-se que a mesma, sendo uma tecnologia descentralizada de registro e transmissão de dados, autônoma, imutável e altamente segura, teria capacidade de coibir violações de privacidade no âmbito do compartilhamento de dados pessoais, bem como contribuir para a desburocratização do serviço público.

Palavras-chave: Proteção de Dados Pessoais. Vigilância. Informação. Dados. Blockchain. Privacidade. Administração Pública. Desburocratização. bCPF.

LISTA DE ILUSTRAÇÕES

Figura 1 - Planta interna do Panóptico de J. Bentham.....13
Figura 2 - Blockchain como uma base de dados distribuída. 34
Figura 3 - processo criptográfico de chaves simplificado.....38
Figura 4 - modelo de compartilhamento de dados centralizado da RFB.....51
Figura 5 - modelo de compartilhamento de dados do bCPF 53

LISTA DE ABREVIATURAS E SIGLAS

BC – *Blockchain*

CI – *Contrato Inteligente*

CJF – *Conselho de Justiça Federal*

DATAPREV - *Empresa de Tecnologia e Informações da Previdência Social*

G2G – *Govern-to-Govern*

GDPR – *General Data Protection Regulation*

LAI – *Lei de Acesso à Informação*

LGPD – *Lei Geral de Proteção de Dados Pessoais*

P2P – *Peer-to-Peer*

RFB – *Receita Federal Brasileira*

SUMÁRIO

1 INTRODUÇÃO 6

1.1 Objetivo Geral 8
1.2 Objetivos Específicos 9
1.3 Justificativa 9
1.4 Metodologia 10

2 Análise tecnopolítica contemporânea 13

2.1 Capitalismo de Vigilância 13
2.2 Características do Capitalismo de vigilância 16
2.2.1 Sociedades de Controle na Contemporaneidade 16
2.2.2 Sociedades de controle e as ameaças à transparência, pilar da democracia 18
2.3 A democracia e a Tecnologia Blockchain 20
2.3.1 Dados pessoais 21
2.3.2 Perspectivas de Proteção de Dados Pessoais e a Blockchain 24

3 O uso da Blockchain no setor público 28

3.1 Desafios e limitações da inovação no setor público 28
3.2 Noções introdutórias sobre Blockchain 31
3.3 Componentes da Blockchain 36
3.3.1 Endereço ou chave pública 37
3.3.2 Chave privada ou senha 37
3.3.3 Token 37
3.3.4 Criptografia 37
3.3.5 Carimbo de tempo 39
3.3.6 Blocos 39
3.4 Tipos de Blockchain 40
3.5 Smart Contracts 42

4 Aplicação prática de Blockchain no mundo 44

4.1 Desafios na adoção da Blockchain no governo 46

5 Discussão e análise de dados 48

5.1 O caso do bCPF 48
5.2 Blockchain como uma solução estratégica 54
5.3 Da segurança e da proteção de dados pessoais 55
5.4 Da auditabilidade 57

6 Conclusão 60

REFERÊNCIAS 62

1 INTRODUÇÃO

Temos a Internet como a maior expressão da sociedade informacional, consistindo em uma rede de compartilhamento de informações aberta, sem proprietário e desenvolvida de forma colaborativa (SILVEIRA, 2017, p. 20 e 23). Em razão da descentralização da arquitetura da Internet, Sérgio Amadeu a denomina "teia de conexões" (SILVEIRA, 2017, p. 24).

A evolução das tecnologias da comunicação em rede e a retomada da chamada "era informacional" por meio do surgimento da Internet permitiram o desenvolvimento de uma nova forma de relação social e, com isso, de um novo mercado: de compra e venda de dados pessoais (SILVEIRA, 2017, p. 11). As empresas de coleta e tratamento de dados lucram em cima desses dados, obtidos muitas vezes sem o conhecimento do titular, e, com isso, possibilitam anúncios feitos por empresas compradoras com maior eficiência, personalização e probabilidade de adesão, modulando o comportamento do usuário.

Nesse diapasão, percebe-se que a Internet não é neutra, isto é, não está dissociada de interesses políticos e econômicos, vide:

> Fazer tecnologia é, sem dúvida, fazer política e, dado que a política é um assunto de interesse geral, deveríamos ter a oportunidade de decidir que tipo de tecnologia desejamos. Mantendo o discurso que a tecnologia é neutra favorece a intervenção de experts que decidem o que é correto baseando-se em uma avaliação objetiva e impede, por sua vez, a participação democrática na discussão sobre planejamento e inovação tecnológica. (GARCÍA et al, 2000, p. 132).

Os dados pessoais são "o elemento-chave para a formação de perfis de comportamento, de consumo e até de opções culturais e política" (SILVEIRA, 2017, p. 11).

Ainda, é importante destacar que vivemos uma nova fase do Capitalismo, no qual verifica-se um conflito entre a expansão econômica e a interceptação de dados, vigilância e direito à privacidade, sendo crescimento econômico e privacidade inversamente proporcionais nesse contexto do novo mercado de compra e venda de dados (SILVEIRA, 2017, p. 11). Em cotejo ao retro mencionado, temos o Capitalismo de Vigilância de Shoshana Zuboff, o qual pressupõe a comercialização de dados pessoais obtidos por meio de ferramentas e recursos de vigilância, tratado de maneira mais aprofundada em seu livro *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.

Esse tratamento de dados possui capacidade preditiva, representando o mercado de venda de dados uma comercialização de domínios futuros (SILVEIRA, 2017, p. 40). Em face do mercado de dados pessoais, surge um campo de estudo da microeconomia da interceptação

de dados pessoais, o qual conta com a captura, o cruzamento e a junção de informações (SILVEIRA, 2017, p. 43). Trata-se de um mercado altamente lucrativo, pendendo entre o legal e o ilegal, ainda mais em virtude de sua capacidade modulatória de comportamento, da informação reduzida que o usuário possui e dos postulados legais sobre a matéria. Desta maneira, há grande vulnerabilidade dos usuários quanto aos dados que transacionam via *Internet*, tendo a tecnologia evoluído mais velozmente que a sua regulação.

Nesse panorama evolutivo tecnológico, surge a chamada *Blockchain*, uma cadeia de blocos criptografados que carregam informações condensadas geradas a partir de uma transação digital, sem a figura de um terceiro intermediador, tendo em vista que a validação dos dados é transferida a uma rede de computadores distribuídos horizontalmente. Nesse sentido, destaca-se a seguinte definição de *Blockchain*:

> Blockchain é uma base distribuída de dados que mantém uma lista encadeada com todos os registros dos elementos de um conjunto, bem como os registros temporais de qualquer criação de novos elementos e modificação destes, impossibilitando assim revisão e adulteração dos mesmos (Lucena e Henriques, 2016, p. 692).

Por se tratar de uma tecnologia relativamente nova, não existem métodos regulatórios ou, até mesmo, compreensão integral de seu uso em nenhuma área. Tudo a seu respeito é meramente introdutório e especulativo, contudo, até a Administração Pública está se adequando e buscando utilizar a *Blockchain* a seu favor.

Não foi apenas a tecnologia que sofreu diversas alterações ao longo do tempo, a Administração também teve suas mudanças, principalmente após a Terceira Revolução Industrial, com a assimilação das novas tecnologias e desenvolvimento de novas ferramentas e técnicas de gestão pública.

Logo, o Estado possui um papel fundamental na sociedade da informação e na organização social eficiente. Nesse sentido, temos que

> Na era da informação, os governos demonstram ter plena consciência de que o futuro será condicionado pela forma como as novas tecnologias de informação e comunicação serão assimiladas, assim como pelo êxito e rapidez dessa absorção. Quanto maior a visão de que a informação, o conhecimento e seu uso apropriado serão as fontes de controle e riquezas na economia digital, mais o acesso à tecnologia da informação torna-se crucial e necessário. (Brito, 2006, p. 110).

As tecnologias da informação, seu desenvolvimento e a participação da população tiveram início com a publicização dos dados governamentais, visto que pouco ou nada se sabia acerca de suas atividades internas. Houve o movimento mundial do Governo Eletrônico, buscando-se

aplicar as tecnologias da informação para aperfeiçoar e aumentar a eficiência dos serviços públicos prestados e as comunicações interna e externa (CHAHIN, 2004).

Buscando melhorar a comunicação interna, a Dataprev desenvolveu para a Receita Federal, com a participação do Conselho de Justiça Federal (CJF), um serviço de troca de informações da base de cadastro dos CPF's, utilizando a tecnologia *Blockchain,* denominado bCPF. Trata-se de um projeto-piloto, entretanto há previsão de que, até julho de 2019, diversas entidades de todos os poderes e esferas venham a aderir a esse serviço.

O modelo atual de compartilhamento de dados na Administração Pública encontra respaldo no Decreto 8.789/2016, e está regulamentado na Portaria nº 58/2016. Nessa lógica:

> [...] o órgão interessado em acessar dados de outro órgão preenche uma Solicitação de Acesso a Bases de Dados e encaminha para a Secretaria de Tecnologia da Informação do Ministério do Planejamento – STI/MP. Esta negociará com o órgão responsável a Permissão de Acesso a Bases de Dados. Uma vez concedida, essa permissão tem validade permanente e não precisa ser renovada. Após a cessão da Permissão, são negociadas questões técnicas e de custeio. (Portal Governo Digital do Ministério da Economia).

Com a adoção do bCPF, podemos dizer que essa lógica de compartilhamento de dados na Administração Pública pode ser alterada e quiçá até ser simplificada, na medida em que a gestão desses dados passará a utilizar uma tecnologia que facilita a comunicação entre os órgãos integrantes. Contudo, de que maneira será alterado o modelo de gestão pública com a implementação de soluções que se utilizem da tecnologia *blockchain*? Haverá mesmo uma mudança de modelo de gestão?

O intuito dessa pesquisa, logo, é analisar, a partir do contexto da Administração Pública, gestão e tecnologia, especificamente da *Blockchain*, os benefícios que uma *Blockchain* como o bCPF poderia propiciar nos trâmites internos do ponto de vista da eficiência. Procura-se responder a seguinte questão de pesquisa: "De que maneira o bCPF assegura a confiabilidade da proteção dos dados pessoais?".

1.1 Objetivo Geral

O objetivo do presente trabalho é verificar de que maneira o bCPF pode assegurar a confiabilidade da proteção de dados no compartilhamento da base de CPF's por meio do levantamento de possíveis vantagens e desvantagens do uso da tecnologia *Blockchain* pela

Administração Pública Federal, bem como pela revisão da literatura sobre os aspectos intrínsecos a tecnologia, proteção de dados e gestão pública.

1.2 Objetivos Específicos

a) Analisar a relação da Administração Pública Federal com a tecnologia e a proteção de dados pessoais a partir de um contexto tecnopolítico;
b) Apresentar os aspectos relevantes da tecnologia *Blockchain* para a compreensão do seu uso na Administração Pública;
c) Explicar o modelo atual de compartilhamento de dados do Governo Federal;
d) Discutir potenciais vantagens e desvantagens do uso do serviço bCPF na proteção de dados.

1.3 Justificativa

O espaço digital da Internet conta, desde o seu surgimento e em escala crescente até os dias atuais, com um enorme quantitativo de usuários, realizando constantes trocas de informação e utilizando diversas ferramentas digitais para garantir maior comodidade e agilidade nas tarefas rotineiras. Contudo, em tudo que se faz no ambiente *on-line*, o usuário deixa algumas "pegadas digitais", dados e metadados que podem ser facilmente coletados e agrupados, gerando um reconhecimento de seu titular, ainda que o mesmo não tenha consciência de que isso ocorra.

Vivenciamos, hoje, um novo tipo de Capitalismo, o chamado Capitalismo de Vigilância, no qual o mercado de dados se torna altamente lucrativo e atraente aos agentes econômicos e estatais, na medida em que permite um grande controle e modulação de comportamentos sem que o indivíduo afetado tenha conhecimento do que lhe ocorre. Os dados pessoais, portanto, são a grande chave nessa ignição da cultura e economia de acumulação em que o acúmulo de capital passa a contar com um acúmulo de informações pessoais, em vários setores da economia, desenvolvendo-se algoritmos "autodidatas" e cruzando-se os dados por meio do Big Data em troca de lucro e poder pelos intermediadores dos dados.

A pesquisa encontra relevância no momento em que se aprovam leis protetoras de dados pessoais ao redor do mundo, inclusive no Brasil, bem como surgem novas tecnologias descentralizadoras como é o caso da *Blockchain*, que excluem a presença de um terceiro intermediador na transação de dados.

Apesar de haver um grande abismo entre o desenvolvimento de uma tecnologia e o acompanhamento jurídico regulatório da mesma, a Administração Pública, assim como a sociedade civil, se adequam a essas inovações tecnológicas, visto que as mesmas modelam as relações de maneira gradual, porém veloz.

O estudo não tem por finalidade esgotar a temática discutida, qual seja a análise dos aspectos que envolvem o uso da *Blockchain* no setor público, porém servindo de base para estudos futuros, uma vez que a tecnologia é muito recente e pouco se conhece sobre suas implicações e consequências.

1.4 Metodologia

O presente estudo foi delineado nos moldes de uma pesquisa documental com abordagem qualitativa. Acerca da pesquisa documental, cabe ressaltar que, por "documentos", a interpretação se dá de maneira ampla, incluindo os materiais escritos como jornais, revistas, obras literárias e científicas, entre outros (GODOY, 1995, p. 21-22).

Nesse mesmo sentido, citamos que

> A fonte de coleta de dados está restrita a documentos, escritos ou não, constituindo o que se denomina de fontes primárias. Estas podem se recolhidas no momento em que o fato ou fenômeno ocorre, ou depois" (MARCONI; LAKATOS, 2006, p.62).

Foram analisadas leis constitucionais e federais, tanto nacionais quanto internacionais, sobre proteção de dados, privacidade ou de regulamentação do uso da Internet de um modo geral, como as seguintes leis brasileiras: o Marco Civil da Internet, a Lei de Acesso à Informação (LAI) e a Lei Geral de Proteção de Dados Pessoais (LGPD). Também foram analisadas a Diretiva 95/46/CE e o *General Data Protection Regulation* (GDPR) europeus. Outrossim, foram estudadas obras literárias e artigos científicos, podendo destacar algumas obras e autores principais, como: Post-scriptum sobre as sociedades de controle de Deleuze; Democracia & Segredo de Bobbio; Big Data: The End of Privacy or a New Beginning? International Data Privacy Law de Rubistein; Tudo sobre tod@s de Silveira; Bitcoin: A Peer-

to-Peer Electronic Cash System de Nakamoto; Blockchain para negócios: promessa, prática e aplicação da nova tecnologia da internet de Mougayar; dentre outros.

Podem ser considerados documentos, ainda, fontes secundárias, a exemplo de "[...], pesquisa que usa a correspondência de outras pessoas" (MARCONI; LAKATOS, 2006, p.63).

Acerca dos documentos, temos que eles

> Representam ainda uma fonte "natural" de informação. Não são apenas uma fonte de informação contextualizada, mas surgem num determinado contexto e fornecem informações sobre esse mesmo contexto (LÜDKE e ANDRÉ, 1986, p. 39).

Além do mais, "[...] a análise documental indica problemas que devem ser mais bem explorados através de outros métodos. [...] ela pode complementar as informações obtidas por outras técnicas de coleta" (LÜDKE e ANDRÉ, 1986, p.39).

Ademais, é importante ressaltar o seguinte entendimento de Arilda Schmidt Godoy quanto à pesquisa qualitativa:

> A pesquisa qualitativa tem o ambiente natural como fonte direta de dados e o pesquisador como instrumento fundamental. Os estudos denominados qualitativos têm como preocupação fundamental o estudo e a análise do mundo empírico em seu ambiente natural (GODOY, 1995, p. 62).

Ainda, por se tratar de uma pesquisa qualitativa, esta é predominantemente descritiva e interpretativa. Consideram-se todos os elementos do ambiente como essenciais à pesquisa, não se limitando a variáveis, observando o ambiente como um todo.

As mudanças no ambiente que nos encontramos centrados nos dias atuais são de grande influência para a mutação dos direitos individuais e coletivos, sendo, portanto, necessária a compreensão das inovações tecnológicas frente à proteção de dados e da gestão dos serviços públicos. Para tanto, buscou-se analisar os conceitos de dados pessoais, de Big Data e os desafios que ele representa nos dias atuais, do Capitalismo de Vigilância, dos direitos à privacidade e proteção de dados, como direitos autônomos, e da tecnologia Blockchain.

Trata-se, ainda, de uma pesquisa avaliativa. A pesquisa avaliativa é concebida por meio de uma tratativa crítica da realidade, ou no caso, da política ou programa a ser avaliado. Destarte, a autora apresenta três funções desempenhadas pela pesquisa avaliativa, quais sejam: função técnica, por meio do fornecimento de subsídios/dados para o acompanhamento e, caso seja necessário, reestruturação da política/programa; função política, por meio da concessão de informações à sociedade para auxiliar na efetivação de controle social da política/programa; e, função acadêmica, por meio do estudo aprofundado da essência da política pública avaliada

com implicância cognitiva (SILVA E SILVA, 2013, p. 44). Nesse sentido, pode-se verificar funções política e acadêmica do presente estudo, visando trazer mais conhecimento acerca do uso da *Blockchain* e verificar suas vantagens e desvantagens na esfera do setor público.

O exame dos dados se deu pela análise de conteúdo, com a interpretação de textos constantes de livros, artigos científicos, legislação e sítios eletrônicos acerca da proteção de dados pessoais no ambiente da Internet, bem como da aplicação da tecnologia *Blockchain* na Administração Pública utilizando-se o bCPF como estudo de caso. Por conseguinte, Bardin (2009) dispõe o seguinte:

> [...] descrever a história da 'análise de conteúdo' é essencialmente referenciar as diligências que nos Estados Unidos marcaram o desenvolvimento de um instrumento de análise de comunicações é seguir passo a passo o crescimento quantitativo e a diversificação qualitativa dos estudos empíricos apoiados na utilização de uma das técnicas classificadas sob a designação genérica de análise de conteúdo; é observar a posteriori os aperfeiçoamentos materiais e as aplicações abusivas de uma pratica que funciona há mais de meio século (BARDIN, 2009, p.15).

Destaca-se, também, a utilização de análise de discurso, a partir da qual não serão analisados apenas o escrito, busca-se verificar o contexto de surgimento das leis de proteção de dados – LGPD no Brasil e GDPR na Europa -, e da inovação tecnológica da *Blockchain*, panorama econômico e análise crítica da gestão pública.

E, por fim, serão realizadas entrevistas semi-estruturadas com alguns integrantes dos órgãos envolvidos na implementação do projeto bCPF. Primeiramente, realizou-se uma entrevista presencial com o auditor-fiscal da Receita Federal, lotado na Coordenação-Geral de Tecnologia e Segurança da Informação (COTEC), o responsável pelo projeto dentro desse órgão, para obtenção de uma maior compreensão acerca do funcionamento do compartilhamento de dados pelo bCPF e suas principais diferenças do modelo anteriormente adotado, bem como garantia de proteção de dados, controle e auditabilidade, instituições envolvidas e eventuais vantagens e desafios de implementação no setor público. Em seguida, foi remetido um questionário de entrevista via e-mail - em razão de conflito de agenda para entrevista presencial no momento da realização desse trabalho - ao Assessor de Diretoria na Dataprev, em face de a Dataprev ter desenvolvido o bCPF para a RFB, para maiores esclarecimentos sobre a tecnologia em si por trás do projeto como: a estrutura da rede, o credenciamento de participantes e segurança da *blockchain* foram alguns dos tópicos tratados.

Os dados foram analisados de maneira indutiva, não tendo como objetivo a verificação de hipótese, sendo a função da análise a correlação dos dados com as fontes de construção das teorias, partindo de um quadro teórico de base.

2 Análise tecnopolítica contemporânea

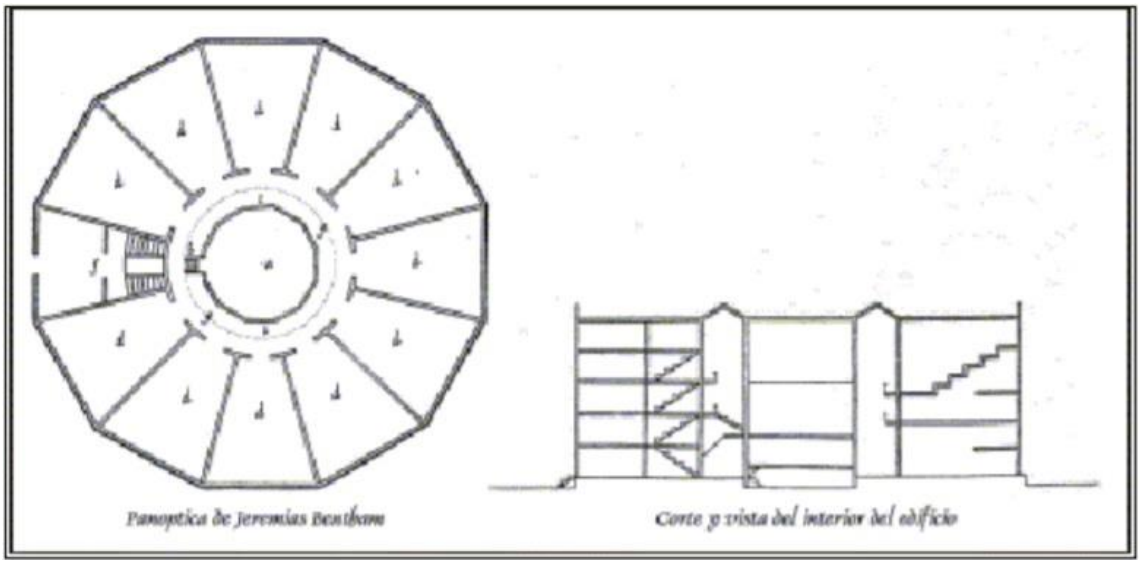
Não é novidade que a Administração Pública sofreu diversas alterações ao longo do tempo. Nesse capítulo, realizar-se-á um breve apanhado histórico das evoluções de cunho tecnológico e sua relação com a Administração Pública e regulações protetivas de direitos.

2.1 Capitalismo de Vigilância

O desejo de onisciência precede qualquer tecnologia, trata-se de uma questão inerente ao ser humano, anseio por poder ilimitado, o qual apenas aguarda por oportunidades de emergir, sendo a tecnologia o vassalo ideal nos dias atuais, conforme se extrai do artigo sobre Paradigma da Vigilância (2013) de Shoshana Zuboff.

À priori, Zuboff (2013) destaca a invenção do engenheiro naval, Samuel Bentham, na Rússia, o chamado Panóptico. Essa invenção teve como objetivo aumentar a eficiência de fábricas conduzidas com trabalho forçado de povos conquistados e, portanto, integrantes de diversas culturas. Consistia em uma estrutura poligonal e de orientação centrípeta, com um cubo de observação ao centro que permitia que alguns poucos administradores observassem a grande gama de operários e se mantivessem invisíveis para eles ao mesmo tempo. Pode-se notar a estrutura do Panóptico na figura abaixo.

Figura 1 - Planta interna do Panóptico de J. Bentham



Fonte: Bentham (1987).

Nesse enredo, seu irmão e filósofo, Jeremy Bentham, extraiu desse experimento um modelo estrutural capaz de obter disciplina de grandes populações de diversas instituições de permanência obrigatória, como prisões, manicômios, fábricas, hospitais, escolas e instituições públicas para indigentes, por meio da otimização da vigilância e de número reduzido de administradores.

O arranjo do Panóptico permite uma generalização em sua aplicação, "ele programa, ao nível de um mecanismo elementar e facilmente transferível, o funcionamento de base de uma sociedade toda atravessada e penetrada por mecanismos disciplinares" (FOUCAULT, 1987, p. 232).

Ademais, Zuboff (2013) traz uma aplicação desse modelo à era informacional, o denominando de Panóptico da Informação, em tradução livre, ou "*information panopticon*", desenvolvendo três regras: a primeira diz que tudo que puder ser mecanizado, o será; a segunda traz que tudo que puder ser informatizado, o será; e a terceira dispõe que, na ausência de contrapeso por meio de restrições e sanções, toda aplicação digital que puder ser usada para vigilância e controle será usada para tal fim, independentemente de sua intenção original de coleta.

Com o advento da Internet, seguido de diversas inovações tecnológicas, surgiu uma possibilidade de individualização, de separação entre pessoal e trabalho no uso das ferramentas digitais disponíveis. Nesse ponto, Zuboff (2013) aponta o surgimento de uma nova economia e de uma nova lógica social, que ela denomina de "Capitalismo Distribuído", o qual enxerga o usuário como fonte real do novo valor econômico. Deste modo, vendem-se os mais diversos equipamentos de expressão individual de maneira direta e o usuário pode configurá-lo conforme suas próprias preferências. Ou ao menos era isso que se pensava. Após vários escândalos mundiais, foi se percebendo que, apesar de o usuário ter propriedade sobre seu equipamento tecnológico, não a tinha plenamente sobre o conteúdo que ele mesmo produzia, visto que os canais digitais não encontravam dificuldade alguma em lucrar com a venda de dados de seus usuários a anunciantes. O poder exercido por eles em cima do usuário era deveras superior, já que o usuário era dono apenas do equipamento eletrônico, enquanto eles são donos dos servidores.

E é nessa lógica que Zuboff (2015) nos apresenta o termo "Capitalismo de Vigilância", em seu artigo *Big Other: surveillance capitalism and the prospects of an information civilization* para o *Journal of Information Technology*. Esse modelo teórico pressupõe que o *Big Data* não é apenas um objeto, efeito ou capacidade tecnológica e, sim, um processo

autônomo que está bem acima da composição estrutural da nova lógica institucionalizada de acumulação de dados completamente ciente e capaz de gerar efeitos denominado Capitalismo de Vigilância.

Nesse sentido, depreende-se que o poder detido pelos agentes responsáveis por plataformas de aplicações digitais, os quais coletam e monetizam em larga escala e de maneira arbitrária os dados pessoais de seus usuários, em face do panorama econômico neoliberal, de desvalorização de direitos sociais e do estado de bem estar social, acaba por facilitar abusos da individualidade em dimensões coletivas a partir do momento em que se desconsideram as personalidades ao buscar modular os comportamentos dos usuários, por meio de algoritmos, e comprometendo direitos que deveriam ser assegurados pelo Estado.

Esse novo tipo de monetização está diretamente ligado à nova arquitetura global de coleta e análise de dados que suscita ganhos e penalidades direcionados a uma modificação de comportamentos e transformação dos dados em commodities, geração de lucro. Ademais, os agentes coletores de dados, por intermédio de suas ferramentas de vigilância, acumulam dados e acabam por atrair um montante significativo de capital de vigilância enquanto editam suas próprias políticas e relações sociais.

Dentro da lógica de Capitalismo de Vigilância, Zuboff (2015) aponta uma arquitetura global de computadores, os quais serviriam como intermediários ao transformar uma mensagem eletrônica de uma organização limitada em spam inteligente e internacionalmente atingível que ela chama de "*Big Other*", o qual possui uma arquitetura automatizada e ubíqua. Essa lógica inovadora institucional possibilita o desenvolvimento de novas técnicas de dominação em ferramentas inesperadas e ilegíveis de extração e controle que finda por privar o indivíduo de seu próprio comportamento, modulando o mesmo e influenciando em suas escolhas.

Quanto à participação no "*Big Other*", Zuboff (2015) afirma que participam aqueles que possuem recursos materiais, cognitivos e financeiros para acessá-lo. Já o acesso ao "*Big Other*" se dá por decisão dos novos mercados de controle do comportamento, composto por aqueles interessados em vender oportunidades de influenciar comportamentos e aqueles interessados em adquiri-las.

Essa natureza automatizada e onipresente do "*Big Other*", suas derivações em habilidades de vigilância, e função generalizada de vigilância, reforça eventuais novos recursos da lógica de acumulação, entretanto, minimiza relações históricas entre mercado e democracia, na medida em que afasta a empresa do consumidor, apresentando uma relação de indiferença.

Zuboff (2015) destaca que o Capitalismo de Vigilância, portanto, não exige a reciprocidade de consumo e mão-de-obra entre esses dois atores para o seu funcionamento, como ocorre no Capitalismo tradicional. Ainda, ela enaltece não só a inexigência de democracia para a prosperidade do Estado num Capitalismo de Vigilância, como a ameaça da democracia na receita pública decorrente da vigilância.

Existem várias dimensões para o Capitalismo de Vigilância, segundo a desenvolvedora dessa teoria. A primeira delas é a imbricação entre as autoridades públicas e privadas nas atividades de vigilância, implicando em colaborações e interdependência entre esses atores. A segunda dimensão envolve a apreensão com relação ao Capitalismo de Vigilância e suas implicações se sobreporem a preocupações globais como igualdade e mudanças climáticas, que nos afetam universalmente. A terceira questão foca na velocidade de evolução social comparada à do projeto institucional de vigilância.

Ressalta-se, por fim, o seguinte entendimento apresentado por Zuboff (2015): a ignorância induzida por engodo não é um contrato social e a liberdade advinda da incerteza não é liberdade. A opacidade do Estado apenas gera uma sensação de liberdade, contudo sem concedê-la realmente.

2.2 Características do Capitalismo de vigilância

2.2.1 Sociedades de Controle na Contemporaneidade

As chamadas “sociedades disciplinares” de Foucault são as organizações sociais por meio do confinamento (DELEUZE, 1992, p. 219). Passa-se do espaço familiar, para o escolar, depois a caserna, a fábrica, às vezes o hospital e, ocasionalmente, a prisão, que seria a maior definição de confinamento (DELEUZE, 1992, p. 219).

A disciplina é o meio de exercício do poder, contando com a vigilância difundida socialmente, num processo de individualização e de responsabilização própria e do outro, na qual o indivíduo vigia as suas próprias atitudes e as dos terceiros que o cercam. Nas sociedades disciplinares, opera-se pela generalização da disciplina e pela massificação do confinamento.

Atualmente, vive-se um período de transição das sociedades disciplinares paras as denominadas, por Deleuze, como sociedades de controle (DELEUZE, 1992, p. 220). Não há de

se falar em melhora ou piora de sistemas, pois cada um traz suas liberações e sujeições (DELEUZE, 1992, p. 220). Vivemos uma sociedade em redes contemporânea, estando conectados por meio das redes sociais, sendo que cada indivíduo vivencia seu próprio panóptico, todos vigiam todos e não temos consciência de quem nos vigia em nosso mundo virtual.

Deleuze percebe os diversos meios de confinamento como variáveis independentes, ocorrendo um recomeço do zero em cada transição de espaço e, mesmo havendo linguagem comum aos espaços, essa seria analógica (DELEUZE, 1992, p. 220-221). Em contraponto, entende que os meios de controle são variáveis inseparáveis, compondo um sistema de geometria variável e de linguagem numérica (DELEUZE, 1992, p. 221). Nesse sentido, destaca-se o seguinte

> Os confinamentos são *moldes*, distintas moldagens, mas os controles são uma *modulação*, como uma moldagem auto-deformante que mudasse continuamente, a cada instante, ou como uma peneira cujas malhas mudassem de um ponto a outro (DELEUZE, 1992, p. 221).

Ao contrário de como ocorreria nas sociedades disciplinares de Foucault, nas sociedades de controle não haveria fim, sendo os espaços "metaestáveis e coexistentes de uma mesma modulação, como que de um deformador universal" (DELEUZE, 1992, p. 221-222).

Nas sociedades disciplinares, existem dois polos, o da assinatura – que serve para identificar o indivíduo – e o do número da matrícula – que serve para indicar a posição desse indivíduo na massa (DELEUZE, 1992, p. 222). Por outro lado, nas sociedades de controle, o essencial é uma cifra, ou seja, uma senha que marcaria o acesso ou a rejeição à informação, tornando os indivíduos divisíveis e as massas em amostras, dados, mercados ou "bancos" (DELEUZE, 1992, p. 222).

Faz-se, ainda, uma correspondência entre a sociedade e a máquina, no sentido em que, nas sociedades antigas soberanas havia o manuseio de máquinas simplórias; nas sociedades disciplinares, o uso de máquinas energéticas, com risco passivo de entropia e ativo de sabotagem; e, nas sociedades de controle, há a condução de máquinas de informática e computadores, com risco passivo de interferência e ativos de pirataria e vírus (DELEUZE, 1992, p. 223). Não se trata de mera evolução tecnológica, como também uma mutação elementar no próprio capitalismo (DELEUZE, 1992, p. 223).

Com as sociedades de controle, os diferentes espaços analógicos das sociedades disciplinares deixam de convergir para um proprietário, Estado ou entidade privada, passando

a representar cifras, moldáveis, de uma só empresa. (DELEUZE, 1992, p. 224). Ademais, o êxito do mercado passa a se dar pela tomada de controle, que é de curto prazo, rotativo, contínuo e ilimitado, ao contrário da disciplina, que seria de longa duração, descontínua e infinita (DELEUZE, 1992, p. 224).

2.2.2 Sociedades de controle e as ameaças à transparência, pilar da democracia

Bobbio explana que a Democracia seria idealmente o poder do visível contraposta a qualquer forma de autoritarismo. Ainda, menciona que "o poder autocrático se subtrai do controle do público de dois modos: ocultando-se, isto é, tomando as decisões no "conselho secreto", e ocultando, isto é, mediante o exercício da simulação ou da mentira, considerada instrumento lícito de governo" (BOBBIO, 2015, p. 30). Ademais, Bobbio defende que não há democracia sem a opinião pública, do direito à informação acerca de decisões a serem tomadas de cunho coletivo e de exprimir críticas quanto a elas (BOBBIO, 2015, p. 41).

Nesse sentido, Gomes ressalta que "o melhor momento para a efetividade de um regime de transparência é quando práticas e políticas estão em processo, estão acontecendo" (GOMES, 2018, p. 7). Caso contrário, pode haver dano já sofrido pelos cidadãos e violação do direito à transparência.

Bobbio salienta que segredo equivale a poder e que os que entendem ser o segredo inato de quem exerce o poder é partidário de regimes autocráticos (BOBBIO, 2015, p. 47). Portanto, quanto maior for a abertura de dados, maior será o exercício de democracia e vice-versa. Cabe destacar a promulgação do Decreto nº 9.690, de 23 de janeiro de 2019, o qual altera disposições da Lei de Acesso à Informação, no sentido de autorizar a ocupantes de cargos comissionados do Grupo-DAS 101.6 ou de hierarquia superior, os quais são indicados politicamente, classifiquem informações como ultrassecretas em casos de ameaça à segurança da sociedade ou do Estado ou deleguem para comissionados do Grupo-DAS 101.5 ou superior a classificação de informações secretas, conforme disposto no art. 30, §§ 1º e 2º. Ainda, traz a permissão de delegação dessa função a dirigentes máximos de autarquias, fundações, empresas públicas e sociedades de economia mista. Antes, essa prerrogativa de classificação pertencia apenas ao presidente, ao vice-presidente, a ministros de Estado, a comandantes das Forças Armadas e a chefes de missões diplomáticas ou a consulares permanentes no exterior. Com essa alteração, pessoas indicadas pelo governo teriam um poder enorme a sua disposição, podendo,

conforme o interesse político, ocultar o acesso dos cidadãos a determinadas informações públicas. E como ficaria a Democracia? Nesse caso, seria uma tendência do pêndulo a ir para um contexto de menos Democracia, ou seja, de menos dados abertos. Contudo, é um exemplo meramente ilustrativo, visto que essa alteração acabou não vigorando.

Por outro lado, Gomes destaca que o segredo também pode ter um valor democrático, do ponto de vista utilitarista (o bem maior pode não ser atingido se permanecerem as práticas secretas) e kantiano (privacidade, reserva, confidencialidade, que dependem de segredo, estão a fundamento da liberdade) (GOMES, 2018, p. 15). Logo, é imprescindível que algumas informações sejam mantidas sigilosas para a garantia de segurança e soberania do Estado. Para tanto, a LAI prevê, em seu art. 23, algumas das possibilidades de classificação da informação em sigilosa, como é o caso de risco à defesa e à soberania nacionais ou à integridade do território nacional; prejuízo ou risco a negociações ou as relações internacionais do País ou que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais; risco à vida, à segurança ou à saúde da população; risco à estabilidade financeira, econômica ou monetária do País; prejuízo ou risco a planos ou operações estratégicos das Forças Armadas; prejuízo ou risco a projetos de pesquisa e desenvolvimento científico ou tecnológico; risco à segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; e comprometimento das atividades de inteligência.

Destarte, Bobbio cita a noção de Carl Schmitt sobre caráter representativo e representação, e a publicidade da tomada de decisão. Contudo, não defende que todos os atos devam ser públicos, trazendo como exemplo de segredo o voto secreto (BOBBIO, 2015, p. 62-63).

Entretanto, faz-se necessário diferenciar “segredo” de “mistério”. O primeiro não possui, per se, uma valoração de bom ou mau, podendo variar de acordo com o caso concreto. Já o segundo representa a não possibilidade de conhecimento do que é bom, útil e oportuno, seja por dificuldade de acesso, seja por intervenção de algum poder, ou até mesmo por falta de capacidade cognitiva de compreensão da informação. (BOBBIO, 2015, p. 78).

O segredo é fruto de uma tomada de decisão, ao passo que o mistério seria uma limitação da vontade e da razão, o que Bobbio chama de “sinal da nossa impotência” (BOBBIO, 2015, p. 78). Ademais, o segredo seria algo passível de contestação, já o mistério apenas existe, independente da nossa vontade, podendo tentar solucioná-lo, mas nunca o coibir (BOBBIO, 2015, p. 78). Por fim, Bobbio determina o segredo como um “artifício institucional”, em contraponto ao mistério, que seria a própria limitação do nosso saber (BOBBIO, 2015, p. 78-

79). Entretanto, apesar de se tratarem de realidades diferentes, não estão totalmente dissociadas, podendo o segredo ser usado como ferramenta para auxiliar na perpetuação de um mistério, por exemplo (BOBBIO, 2015, p. 79-80).

2.3 A democracia e a Tecnologia Blockchain

A Democracia jaz no princípio da publicidade, um dos mais fundamentais princípios, também chamado de "poder visível" (BOBBIO, 2015, p. 78), do qual derivam tantos outros, como é o caso da transparência. A opacidade de atuação do Estado é o que coloca em risco a Democracia, visto que o governo democrático necessita de controle dos cidadãos. A implementação de tecnologias como o *blockchain*, o qual possui mecanismos de auditabilidade e controle próprios, pode auxiliar no exercício desse controle do cidadão na medida em que se guarda o registro de todas as atividades exercidas pelos seus integrantes. Logo, apesar de haver meios não tão explícitos, as formas de fiscalização da atuação governamental pelos cidadãos também evoluem, mesmo com os desafios tecnológicos que existem e que ainda estão por surgir.

Ademais, existem outros fatores que indicam o sistema democrático, como é o caso da proteção de dados pessoais dos cidadãos, ainda mais em face de um Capitalismo de Vigilância, no qual o mercado de dados seria o mais lucrativo nos dias atuais. A *blockchain*, considerando sua natureza imutável e criptográfica dos dados, bem como de integridade da informação e de meios de fiscalização, apresenta um modelo que garante a segurança e a proteção dos dados pessoais dos que a utilizam, podendo ser cogitada como uma solução para problemas de privacidade e de vazamento de dados pessoais. Nesse sentido, seria a BC uma solução pra mais democracia? Ou ela vai reduzir ainda mais o poder do Estado e, com ele, reduzir o poder dos cidadãos? A garantia da segurança dos dados do cidadão pelo uso da BC poderia significar maior exercício de Democracia e menos panópticos na medida em que a tecnologia possui uma estrutura descentralizada e transparente de poder, podendo representar uma alternativa para combater o Capitalismo de Vigilância.

2.3.1 Dados pessoais

Tendo em vista que, no cenário atual, os dados representam uma fonte de matéria prima da economia, cabe conceituar "dados pessoais" para fim de melhor compreender o tipo de dados de que tratará essa pesquisa. Todavia, não há uma definição única e pacífica, a mesma ocorre de acordo com o mercado de dados, visto que influencia em sua capacidade de ser coletado e comercializado (SILVEIRA, 2017, p. 43).

Nesse sentido, Amadeu cita a classificação de Bruce Schneier em seis tipos de dados, vejamos:

> [...] dados de serviços, fornecidos para abrir uma conta (por exemplo, nome, endereço, informações de cartão de crédito, etc.); dados divulgados, que são introduzidos voluntariamente pelo usuário; dados confiados, como comentários feitos sobre as outras pessoas; dados incidentais, sobre um usuário específico, mas enviados por outra pessoa; dados comportamentais, que contém informações sobre as ações que os usuários realizam ao utilizar um site e são utilizados pela publicidade segmentada; e os dados inferidos, que são as informações deduzidas dos dados, perfil ou atividades (SCHNEIER, apud AMADEU, 2017, p. 44).

A título exemplificativo, destaco algumas definições de dados pessoais ao redor do mundo retiradas do sítio *DLA Piper*[1]: na **Argentina**, dado pessoal é qualquer tipo de informação relacionada a indivíduos identificados ou identificáveis ou a entidades legais. No **México**, trata-se de informação acerca de sujeito identificado ou identificável. Nos **Estados Unidos da América**, há variação quanto ao conceito, a Comissão Federal de Comércio considera dado pessoal informação que possa razoavelmente ser usada para entrar em contato ou distinguir uma pessoa, incluindo endereços de IP e equipamentos identificadores, porém, algumas leis americanas federais entender por dado pessoal inclusive informações que por si só não possam gerar identificação do sujeito, isso porque existe o mecanismo de re-identificação de sujeitos de dados usando-se dados não pessoais, o que enfraquece a eficiência da anonimização (2013, RUBINSTEIN, p. 77). No **Canadá**, trata-se de qualquer informação sobre a identificação de um indivíduo. Na **Índia**, as leis de privacidade preceituam dado pessoal como qualquer informação que esteja relacionada à pessoa natural, direta ou indiretamente, bem como outras informações que estejam disponíveis ou prováveis de estarem disponíveis para entidades

[1] DLA Piper. **Data Protection Laws of the World**. Disponível em: <https://www.dlapiperdataprotection.com/index.html?c=IL&c2=&t=definitions>. Acesso em: 10/11/2018.

corporativas que sejam capaz de gera identificação do indivíduos. Em **Israel**, entende-se como dados referentes à personalidade, status pessoal, relações pessoais, estado de saúde, posição econômica, qualificações vocacionais, opiniões e crenças do indivíduo.

Ainda, segundo a Diretiva 95/46/CE da União Europeia, dados pessoais são:

> [...] qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.

O Regulamento Geral sobre Proteção de Dados Europeu nos define o seguinte em seu art. 4º, vejamos:

> [...] Para efeitos do presente regulamento, entende-se por:
>
> 1) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;[2]

[2] => razão: 26, 27, 28, 29, 38:
(26) Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação.
(27) O presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas.
(28) A aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento e os seus subcontratantes a cumprir as suas obrigações de proteção de dados. A introdução explícita da «pseudonimização» no presente regulamento não se destina a excluir eventuais outras medidas de proteção de dados.
(29) A fim de criar incentivos para aplicar a pseudonimização durante o tratamento de dados pessoais, deverá ser possível tomar medidas de pseudonimização, permitindo-se simultaneamente uma análise geral, no âmbito do mesmo responsável pelo tratamento quando este tiver tomado as medidas técnicas e organizativas necessárias para assegurar, relativamente ao tratamento em questão, a aplicação do presente regulamento ea conservação em separado das informações adicionais que permitem atribuir os dados pessoais a um titular de dados específico. O responsável pelo tratamento que tratar os dados pessoais deverá indicar as pessoas autorizadas no âmbito do mesmo responsável pelo tratamento.

> [...]

Ademais, podemos destacar a definição trazida pela Lei de Acesso à Informação, em seu art. 4ª, inciso IV, de que informação pessoal seria aquela relacionada à pessoa natural identificada ou identificável.

Por fim, a Lei Geral de Proteção de Dados Pessoais brasileira nos apresenta, em seu art. 5º, os conceitos a seguir:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> [...]

Logo, podemos entender por dados pessoais aquelas informações capazes de identificar ou levar à identificação de determinada pessoa, física ou jurídica, ainda que descaracterizadas, codificadas ou decorrentes de pseudônimos. Desta maneira, logicamente, os dados anônimos não poderão ser considerados dados pessoais, visto que inviabilizam, em regra, a identificação da pessoa. Contudo, isso não é absoluto, há que se fazer a ressalva do fenômeno da re-identificação mencionado anteriormente, visto que é possível "desanonimizar" esse dado para obter a identificação.

Por fim, cabe salientar que as informações pessoais ou dados pessoais podem ser classificados de mais duas maneiras: dados anônimos e dados sensíveis. Dados anônimos são aqueles que não permitem a identificação do seu titular. Por outro lado, os dados sensíveis são aqueles de cunho extremamente íntimo e que podem potencialmente gerar um caráter discriminatório, visto que dizem respeito a questões de opinião, raça, etnia, gênero, saúde,

(38) As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança.

orientação sexual, dentre outros que se encontram no rol do GDPR Europeu, em seu art. 4º, bem como no art. 5ª, inciso III, do PL nº 5.276/2016 no Brasil. Ainda não há uma tutela específica de dados pessoais sensíveis no Brasil, a Lei Geral de Proteção de Dados europeia não apresenta definição dos mesmos.

2.3.2 Perspectivas de Proteção de Dados Pessoais e a Blockchain

2.3.2.1 Direito à privacidade e direito à proteção dos dados

Embora os conceitos de privacidade e proteção de dados possuírem uma origem comum na individualidade como integrante da personalidade do sujeito, na prerrogativa de controle sobre como viver uma vida digna – que se aplica tanto à vida privada, quanto a seus dados pessoais -, e ambos se encontrem em risco em face do mercado de dados pessoais, é cediço afirmar que se tratam de direitos diversos e autônomos entre si, conforme será demonstrado a seguir.

2.3.2.2 Direito à privacidade

O direito à privacidade pode ser vislumbrado no período da antiguidade clássica grega, no qual originou-se a dicotomia entre público e privado, sendo posteriormente seguida pelos romanos, criando-se duas esferas diferentes: a da *pólis* – integrada pelos cidadãos livres, representando o público – e a da *oikos* – integrada por indivíduos, representando o privado (2014, HABERMAS. p. 97-98). Contudo, a realidade pública não era exercida em um local específico, mas, sim, no âmbito da *léxis* (diálogo), sendo que a posição do cidadão na *pólis* estava diretamente ligado a sua posição no *oikos*. Segundo Hannah Arendt (2005. P. 33), essa distinção das esferas pública e privada era a fronteira das esferas da política e da família. Ademais, Arendt (2005. P. 38-39) prossegue destacando que, ao adentrar a esfera pública, o indivíduo existe de forma diferente, deixando de se relacionar com o que ele próprio é, mas relacionando-se com o que lhe é comum. Importante ressaltar que, aqui, o privado era material, remetendo à necessidade humana de sobrevivência (CACHAPUZ, 2006. P. 55).

No período da Idade Média, apesar de possuir uma roupagem diferente da que vemos nos dias atuais, já começava a se perceber uma necessidade de isolamento por parte dos indivíduos, sendo a vivência com privacidade um costume desenvolvido pelos nobres

(DONEDA, 2006. p. 125). Entretanto, destaca-se que essa possibilidade de isolamento permanece sendo um privilégio de poucos ou dos que optaram por viver distantes da comunidade (RODOTÀ, 2008. p. 26)

Nesse sentido, ainda, Rodotà (2008) aponta o surgimento da privacidade com a "desagregação da sociedade feudal" e a ascensão da burguesia, sendo de grande interesse do burguês a individualidade e, consequentemente, a proteção de seu próprio espaço, originando uma necessidade por intimidade (RODOTÀ, 2008. p. 26).

As diversas dimensões do pensamento acabaram por contribuir na alteração de percepções acerca do público e do privado, sendo pautado, ainda, na expressão da personalidade do indivíduo, que também observou mudanças ao longo do tempo.

Portanto, a ideia de privacidade não é inovadora, tendo sido identificada em outros períodos históricos e em outras sociedades, todavia somente começou a aparecer positivada no fim do século XIX e ser interpretada da forma como observamos atualmente nas últimas décadas (DONEDA, 2006. p. 4). Nesse sentido, temo que "O despertar do direito para a privacidade ocorreu justamente num período em que muda a percepção da pessoa humana pelo ordenamento e ao qual se seguiu a juridificação de vários aspectos do seu cotidiano" (DONEDA, 2006. p. 4).

Conforme remonta Doneda (2006, p. 4-5), a doutrina do direito à privacidade se deu com o artigo de Brandeis e Warren, *The right to privacy*, fruto de uma evolução bem delineada. Primeiro, há o individualismo extremo exprimido do direito de ser deixado só (*right to be left alone*), pautado num paradigma de privacidade de zero relacionamento, ausência total de comunicação entre indivíduos. Este fora o marco inicial, no qual, posteriormente, desenvolveu-se a noção de privacidade como aspecto fundamental e inerente ao exercício da personalidade da pessoa humana.

O direito à privacidade também se encontra vinculado à intimidade e ao secreto, o sentido do discurso se altera de acordo com a pessoa que o profere. Logo,

> Privacidade, então, deve ser vista antes de tudo como exercício de uma liberdade da pessoa, uma necessidade humana. Parte-se para uma visão da privacidade que é interna ao sujeito, faz parte dele, formando-o como ser humano. Seja trabalhando a privacidade como o estar só ou numa perspectiva mais contemporânea de controle informacional, não se pode perder o vínculo com a pessoa, como forma de manifestação da personalidade. Ter privacidade é fundamental ao indivíduo, não apenas em oposição ao público, mas numa relação interna, visto que não será possível a assunção de seus desejos sem a construção de seu espaço íntimo (2017, CANCELIER).

Entretanto, existe uma parte doutrinária que entende intimidade e privacidade como institutos diferentes, em razão da previsão em apartado dos termos no art. 5º da Constituição Federal de 1988. Todavia, não se vislumbram impedimentos à interpretação conjunta dos termos intimidade e privacidade, ambos inerentes à preservação do espaço pessoal do indivíduo, vinculadas aos direitos de personalidade.

Na era informacional atual, a compreensão do direito da privacidade e de seus limites tem se dado de maneira cada vez mais enfraquecida em face da constante troca e compartilhamento de dados, o que deixa o titular desses dados extremamente vulnerável e, às vezes, sem que ele mesmo tenha noção das consequências decorrentes dessa prática. No caso da relação privada, ainda é possível decidir se deseja estabelece-la ou não, ainda que existam fatores externos que influenciem grandemente nessa tomada de decisão pelo usuário. Todavia, a relação entre o cidadão e o Estado não é facultativa, sendo de grande importância o desenvolvimento de uma relação de confiança. É dever do Estado assegurar a proteção dos dados pessoais e do direito da privacidade de seus cidadãos. Nesse sentido, pode-se observar a *blockchain* como uma possível solução às questões de desconfiança no Estado em razão das próprias características da tecnologia, que serão destrinchadas posteriormente.

2.3.2.3 Direito à proteção dos dados pessoais

Em face da nova dimensão tecnológica e informacional, apenas o direito da privacidade demonstra insuficiência para abarcar todas as situações advindas do uso da *Internet*. Veiga e Rodrigues (2007), portanto, apontam o seguinte

> A privacidade era relativamente fácil de proteger no passado, por não se registarem recolhas significativas de dados pessoais e pela dificuldade de aceder àquela informação que não estava centralizada. Com o advento do computador estas variáveis alteraram-se substancialmente.

O advento de uma nova dimensão de coleta e tratamento de dados reascendeu a necessidade de atenção à privacidade, entretanto, o conceito desse instituto restou incapaz de refletir as novas relações sociais digitais que vão além da invasão externa na esfera privada, visto que a moeda de poder jaz na informação. Não significa dizer que a privacidade não possui nenhuma aplicação nesse plano, apenas que sua melhor atuação se dá no âmbito individual do que no campo mais abrangente e coletivo, como, por exemplo, no caso de controle de informação por grupos econômicos (VEIGA e RODRIGUES, 2007, p. 66).

Ao contrário do direito à privacidade, que se encontra positivado em Códigos e na Constituição Federal no Brasil, o direito à proteção de dados pessoais se encontra tutelado em

leis esparsas, o que torna sua proteção um pouco mais frágil. Isso se dá, inclusive, pela veloz evolução das relações cibernéticas, possibilitando o surgimento de novas violações. Essas violações dizem respeito ao tratamento de dados pessoais, o que pode, conjuntamente, envolver ou não uma violação à privacidade do indivíduo.

Ainda, segundo dispõem Veiga e Rodrigues (2007), a proteção à privacidade visa manter o sigilo da vida privada, preservando as escolhas do indivíduo de opiniões de terceiros. Trata-se de uma "noção pré-informática". Por outro lado, destacam que "[...] os dados pessoais não têm de ser íntimos, mas somente pessoais, isto é, respeitantes ao indivíduo" (VEIGA e RODRIGUES, 2007, p. 65).

Destarte, não se contesta a necessidade sócio jurídica de tratamento autônomo dos referidos direitos, posto que atendem problemas específicos da esfera da intimidade. O ordenamento jurídico parte da premissa da intimidade ao tratar da proteção de dados pessoais, contudo este se mostra muito mais amplo, compreendendo, inclusive, a autodeterminação informativa do titular de dados (VEIGA e RODRIGUES, 2007, p. 66).

3 O uso da Blockchain no setor público

3.1 Desafios e limitações da inovação no setor público

A inovação é uma grande ferramenta competitiva de mercado para o setor privado, sendo fundamental no estabelecimento e no sucesso de empresas em seus respectivos mercados (TIDD et al, 2008, p. 25). A vantagem competitiva pode advir de tamanho ou patrimônio, contudo as empresas que conseguem convergir conhecimento com avanços tecnológicos no desenvolvimento de produtos/serviços (ofertas) e na forma que criam/lançam os mesmos obtém mais sucesso (TIDD et al, 2008, p. 25). O desenvolvimento de produtos novos permite capturar, reter e aumentar a lucratividade de novas fatias de mercado, ao passo que, quanto aos produtos antigos e estabelecidos, o crescimento da competitividade não está relacionado apenas a preço, tendo pertinência outros fatores não-econômicos também, como modelo, customização e qualidade (TIDD et al, 2008, p. 25). A introdução de novos produtos tem deveras importância frente à constante mudança do meio ambiente e nos campos socioeconômico e legal, que geram oportunidades e restrições (TIDD et al, 2008, p. 25). A vantagem de competitividade jaz na prestação de melhores serviços, de maneira mais rápida, barata e de melhor qualidade (TIDD et al, 2008, p. 26).

Conforme Schumpeter, a inovação tecnológica tem por fim a obtenção de vantagem estratégica, remetendo aos "lucros de monopólio" que serão obtidos inicialmente pelo empresário implementador da inovação (SCHUMPETER apud TIDD et al, 2008, p. 27). Entretanto, as vantagens decorrentes de inovação vão perdendo seu poder competitivo na medida em que outras empresas as imitam: resulta no surgimento de outras inovações, o que gerará amortização de lucros de monopólio até que se atinja um novo equilíbrio. O ciclo se repete em próximas inovações (SCHUMPETER apud TIDD et al, 2008, p. 27). Ademais, Schumpeter menciona o processo de "destruição criativa", segundo o qual "há uma constante busca pela criação de algo novo que simultaneamente destrói velhas regras e estabelece novas – tudo sendo orientado pela busca de novas fontes de lucratividade" (SCHUMPETER apud TIDD et al, 2008, p. 27).

Tidd (2008, p. 30) apresenta os 4 P's da inovação, quais sejam:

- Inovação de produto – mudanças nas coisas (produtos/serviços) que uma empresa oferece;

- Inovação de processo – mudanças na forma em que os produtos/serviços são criados e entregues;
- Inovação de posição – mudanças no contexto em que produtos/serviços são introduzidos;
- Inovação de paradigma – mudanças nos modelos mentais subjacentes que orientam o que a empresa faz.

Inovação é processo de conhecimento, seja ele obtido por meio de experiência anterior, explícito em sua forma (codificado e possível de acessar, discutir, transferir, etc), seja ele alcançado de modo tácito (conhecido, mas sem formulação) (TIDD et al, 2008, p. 35). A gestão da inovação se fundamenta na capacidade de transformar essa incerteza em conhecimento e o coeficiente de incerteza é diretamente proporcional ao grau de radicalização da inovação, ou seja, quanto mais radical for a opção, mais incertezas decorrerão (TIDD et al, 2008, p. 35). O desafio é desenvolver uma gestão de inovação para o período de estabilidade e também para o de alta incerteza e velocidade de mudança (TIDD et al, 2008, p. 38).

A teoria da inovação de ruptura de Christensen assinala o mercado como gatilho da inovação, além das rupturas geradas pelas inovações tecnológicas (TIDD et al, 2008, p. 49). Nesse sentido, destaca-se que

> O maior desafio com que as empresas encontram dificuldade de lidar nesses casos não está no avanço tecnológico em si, mas na mudança de configuração tecnologia/necessidade para os mercados usuais e novos. O "dilema do inovador" a que alude o título do primeiro livro de Chrístensen refere-se às dificuldades que os jogadores Já estabelecidos encontram em administrar simultaneamente aspectos estáveis (sustentáveis) e descontínuos (desconstrutores) (TIDD et al, 2008, p. 49).

Em face dos gatilhos de descontinuidade, Tidd (2008, p. 53-56) cita algumas fontes capazes de causar descontinuidades:

- Novo mercado;
- Nova tecnologia;
- Novas regras políticas;
- Situação sem perspectivas;
- Mudança de maré no comportamento/sensibilidade de mercado;

- Desregulamentação/Mudanças nos regimes regulatórios;
- Fraturas ao longo de “linhas de falhas”;
- Eventos imprevistos;
- Inovação de modelo de negócio;
- Alterações no paradigma tecno-econômico;
- Inovação de arquitetura;
- Alterações no paradigma tecno-econômico – mudanças sistemáticas que impactam setores inteiros ou mesmo sociedades inteiras.

A tentativa de inovação pode resultar em falhas catastróficas, porém a empresa que não inova tem poucas chances de sobrevivência no mercado. Todavia, a inovação deixa de representar somente uma vantagem competitiva no setor privado e passa a integrar as noções de desenvolvimento do setor público também. Koch e Hauknes (2005, p.7) dispõem o seguinte acerca da inovação no setor público:

> A inovação no setor público pode incluir a produção de “coisas” materiais ou produtos, mas envolve, mais frequentemente do que no setor privado, a aplicação de “coisas” já existentes ou a prestação de serviços, acompanhada por mudança organizacional e desenvolvimento de política pública.

No caso do setor público, é possível organizar os tipos de inovações em algumas categorias. Koch e Hauknes (2005, p.8) apresentam os seguintes tipos:

- Serviço novo ou melhorado;
- Processo de inovação;
- Inovação administrativa;
- Inovação de sistema operacional;
- Inovação conceitual;
- Mudança radical de racionalidade.

Entende Thompson (apud Klumb e Hoffman, 2016, p. 85-86) que a estrutura burocrática das organizações públicas pode representar enormes barreiras no que tange à capacidade inovativa. Logo, “a impessoalidade, a formalidade, a hierarquia e outros princípios

da burocracia limitam o espaço para a criatividade, o questionamento e a experimentação, fatores necessários para identificar e explorar novas possibilidades" (Klumb e Hoffman, 2016, p. 86). Outras barreiras destacadas por Klumb e Hoffman (2016, p. 86) são a resistência à mudança ou ausência de capacidade de aprendizagem organizacional.

Além da complexidade e burocratização determinante do setor público, percebe-se a questão da escassez dos recursos públicos para a realização de sua atividade constitucional de prestação de serviços públicos em face das restrições orçamentárias e ligados ao desenvolvimento econômico do país, segundo aponta Pedrosa (2019).

Ademais, mudanças políticas também são responsáveis por limitar a atuação da gestão da informação no setor público. Pedrosa (2019) destaca que

> [...] há alta rotatividade dos gestores, devido ao vínculo precário e transitório desses com a administração pública e, em decorrência disso, é preciso lidar com a excessiva mudança da equipe técnica. A cada mudança de gestão, tem-se um recomeço e adaptação dos projetos preexistentes. Muitas vezes, projetos de transformação são abandonados, por não se adequarem a nova política de governo.

3.2 Noções introdutórias sobre Blockchain

No ano de 2008, Satoshi Nakamoto apresentou ao mundo a chamada *Bitcoin*, uma versão *peer-to-peer* de dinheiro eletrônico, a qual permite a transferência pecuniária sem a necessidade de um intermediário, qual seja uma instituição financeira (NAKAMOTO, 2008, p. 1). A capacidade descentralizadora propiciada pela *Blockchain* poderia auxiliar no desenvolvimento de diversos setores, inclusive do setor público, cuja característica burocrática é marcada por uma morosidade na prestação de informações e serviços.

Em análise ao que Nakamoto (2008) define em sua pesquisa, Mougayar destaca os seguintes aspectos fundamentais:

- Transações e interações eletrônicas *peer-to-peer*
- Sem instituições financeiras
- Prova criptográfica no lugar de confiança centralizada
- Confiança em rede, em vez de em uma instituição unificada (MOUGAYAR, 2017, p. 3).

A *blockchain* é a inovação tecnológica na qual se encontra fundamentado o *Bitcoin*. Mougayar divide o conceito de *blockchain* em três definições complementares: uma técnica, uma corporativa e uma legal. A definição técnica é de que a *blockchain* representaria uma base de dados *back-end*[3] que mantém um registro distribuído e que possibilita sua inspeção abertamente; a corporativa é de que se trata de uma "rede de troca para movimento de transações, valores, ativos entre pares"; e, a legal, é a que seria um "mecanismo de validação de transações que não requer apoio de intermediários" (MOUGAYAR, 2017, p. 4). As capacidades da tecnologia *blockchain* seriam a soma das três definições (técnica, corporativa e legal).

Tendo em visto que a *blockchain* não possui um intermediário confiável e se encontra estabelecida em um ambiente que não possibilita uma identificação fácil de seus usuários, a confiança entre as partes se dá por meio de quatro características principais da rede *blockchain*, são elas:

- Livro-razão: a tecnologia usa um único livro-razão para proporcionar um histórico de transações completo. Ao contrário dos bancos de dados tradicionais, as transações e os valores em uma *blockchain* não são substituídos;
- Segurança: a *blockchain* é segura criptograficamente, assegurando, assim, que os dados contidos no livro-razão não possam ser adulterados e que os dados sejam comprováveis;
- Compartilhada: a rede é compartilhada entre vários participantes, o que garante a transparência entre os nós participantes da *blockchain*;
- Distribuída: a *blockchain* pode ser distribuída, o que possibilita dimensionar a quantidade de nós da rede para torná-la mais resistente a ataques de maus atores, visto que quanto maior o número de nós, menor será a capacidade de um ator ruim influenciar o protocolo de consenso usado pelo *blockchain* (Yaga et al, 2018, p. 2-3).

[3] Front-end e back-end são termos usados para caracterizar interfaces de programas e serviços relativos ao usuário dessas interfaces. Uma aplicação front-end é aquela que interage diretamente com o usuário, o primeiro contato que ele tem com o programa. Já uma aplicação back-end trabalha indiretamente no suporte dos serviços de front-end, normalmente se comunicando com a fonte desses serviços, o server (BATTISTELLI, Juliana. **Os principais conceitos de back-end para começar a desenvolver para a web**. Blog Mastertech. 2017. Disponível em: <https://blog.mastertech.com.br/tecnologia/os-principais-conceitos-de-back-end-para-comecar-desenvolver-para-web/>. Acesso em: 11/07/2019).

Blockchain pode ser definida como um livro-razão – onde são lançadas entradas e saídas contáveis - digital distribuído que usa algoritmos criptográficos para verificar a criação ou a transferência de registros digitais em uma rede distribuída (FINCK, 2018, p. 667). O nome *Blockchain* se extrai da atividade de manutenção de um registro de todas as transações agrupadas em blocos, formando uma corrente, sendo esse processo viabilizado por meio de algoritmos de consenso que variam de acordo com a *blockchain* a ser formada (FINCK, 2018, p. 668). A integridade do livro-razão se mantém pelo chamado "consensus" ou consenso alcançado pelos participantes (FINCK, 2018, p. 668).

As *blockchains* são sistemas complexos fundamentados na combinação de três campos: engenharia de *software*, ciência da criptografia e teoria dos jogos, o que Mougayar denomina de "tríade de combustão dos campos de conhecimento" (MOUGAYAR, 2017, p. 11). Teoria dos jogos porque, na *blockchain* da Bitcoin, Satoshi Nakamoto precisou solucionar um enigma chamado "Problema dos Generais Bizantinos" para tolher ataques de um pequeno grupo de generais maliciosos que poderiam trair e atacar (MOUGAYAR, 2017, p. 11-12). A ciência da criptografia tem como função a garantia da segurança, respaldada principalmente em: *hashing*, chaves e assinaturas digitais (MOUGAYAR, 2017, p. 12). O desafio da engenharia de *software* jaz na combinação das anteriores para desenvolver liames da *blockchain* por meio da redução de incerteza pela certeza matemática (MOUGAYAR, 2017, p. 13).

As informações armazenadas numa *blockchain* têm sua segurança garantida pela criptografia, com chaves e assinaturas que determinem a função e os limites de capacidade de cada indivíduo na *blockchain* (FINCK, 2018, p. 668).

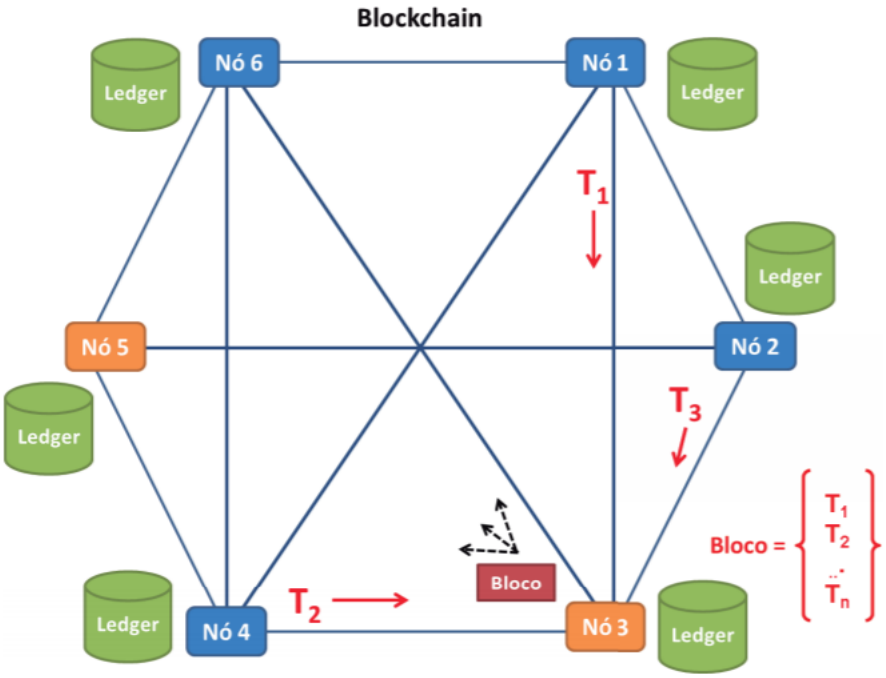
A *Blockchain* também tem sido denominada "internet de valor" (FINCK, 2018, p. 668), havendo previsão de que, em breve, verificaremos registros, identidades, autenticidade, direitos, trabalho cumprido, obras, contratos e outros processos a ativos suscetíveis de valoração por meio de uma pesquisa no Google, criando-se certificado digital de propriedade para tudo (MOUGAYAR, 2017, p. 31). Mougayar (2017), ainda, dispõe que, com a *blockchain*, não será mais possível forjar ou copiar certificados oficiais que a integrem, representando, portanto, o que faltava para uma "revolução da informação".

A estrutura inviolável da *Blockchain* faz emergir uma nova forma de confiança. Cria-se um estado de confiança pela adoção de sistemas criptográficos, contudo sem a necessidade de atores confiáveis, é a chamada confiança sem confiança (FINCK, 2018, p. 669). Deste modo, confiam-se nos resultados proporcionados pela tecnologia, sem precisar confiar em um

intermediário ou no outro com quem se realiza a transação, visto que a *blockchain* traz, em sua estrutura, mecanismos de segurança para todos os envolvidos.

Conforme a OECD, *Blockchain* seria uma forma de tecnologia de livro-razão distribuído que atua como um registro aberto e confiável de transações entre uma parte e outra (ou entre várias partes) que não é armazenada por uma autoridade central, sendo, assim, uma cópia armazenada por cada usuário usando *software* de *blockchain* e conectado a uma rede *blockchain* – também denominado "nó" (BERRYHILL et al, 2018, p. 10). Ao invés de uma autoridade central controlando a base de dados, todos os nós possuem uma cópia do livro-razão e as atualizações são propagadas na rede em questão de minutos ou segundos (BERRYHILL et al, 2018, p. 10). A maioria dos nós precisa revisar e validar a transação antes que a mesma seja verificada e registrada, o que dificulta a adulteração de dados, visto que qualquer nó pode inspecionar, aumentando, deste modo, a confiança e a integridade do dado (BERRYHILL et al, 2018, p. 11). Cabe salientar que a atuação dos nós se dá, na maioria das vezes, de maneira automática na *blockchain* pelo próprio *software* (BERRYHILL et al, 2018, p. 11).

Figura 2 - Blockchain como uma base de dados distribuída.



Fonte:BRAGA, 2017, p. 3. Il. color.

Como se pode observar na figura acima, a rede da *blockchain* é distribuída P2P[4], isto é, entre os nós que a compõem, podendo os nós consultar e alterar a base de dados de acordo com o seu acesso. Os blocos são os registros na base de dados e não podem ser modificados, representando, assim, o histórico dessa *blockchain*. Logo, destaca-se que "a base de dados somente aceita a inclusão de blocos novos e nunca a remoção ou modificação de blocos existentes" (BRAGA, 2017, p. 3).

Os blocos são, cada um, um conjunto de transações validadas e agrupadas de forma que a informação esteja acessível, porém impossibilitando eventuais tentativas de adulteração (BERRYHILL et al, 2018, p. 15). Ademais, destaca-se que os blocos são dependentes entre si, relacionados intrínseca e linearmente, em ordem sequencial dos próprios *hashes* únicos, formando, portanto, uma corrente verificável e rastreável (BERRYHILL et al, 2018, p. 15).

Nesse sentido, cabe ressaltar outro conceito-chave inerente à *blockchain*, que é o da imutabilidade. Em regra, quando uma transação é registrada no livro-razão da *blockchain*, não pode ser desfeita, o que fundamenta a questão da confiança nas transações realizadas por meio dessa tecnologia (BERRYHILL et al, 2018, p. 12). Ao contrário, num banco de dados centralizado, como a informação é armazenada em um único local, caso a segurança do servidor ou a autoridade que comanda o servidor sejam comprometidos, os dados podem ser alterados ou até excluídos e, muitas vezes, pode passar despercebido pelos demais usuários (BERRYHILL et al, 2018, p. 12).

Para que se possa melhor compreender a tecnologia *blockchain*, destacam-se os seguintes conceitos apresentados por Martinovic, Kello e Sluganovic (2017, p. 3-4, tradução livre):

- Confidencialidade: o conteúdo da informação é acessível somente àqueles autorizados a acessá-lo. Segredo é tido como sinônimo de confidencialidade e privacidade. É normalmente assegurada pelo uso de métodos criptográficos. Nesse sentido, pode-se afirmar que o segredo seria o equivalente a poder, visto que somente algumas pessoas terão acesso à informação (BOBBIO, 2015, p. 47) e um "artifício institucional" (BOBBIO, 2015, p. 78), uma ferramenta utilizada para garantir a segurança daquela informação.

[4] P2P significa *peer-to-peer*, representa uma rede descentralizada onde o computador de cada usuário exerce função de cliente e de servidor simultaneamente.

- Integridade (da informação): é o que garante que a informação não foi adulterada por um terceiro não autorizado. Permite a inspeção dos dados, verificando, assim, a ocorrência de manipulação destes e, consequentemente, sua refutação.
- Autenticação: se subdivide em “autenticação da entidade” e “verificação da origem do dado (e sua procedência)”. A primeira é utilizada pelas partes para se identificarem no início da comunicação, abarcando protocolos de reivindicação de identidade e métodos de verificar essa reivindicação. No mesmo sentido, funciona a verificação da origem e procedência do dado, devendo a informação decorrente da comunicação ser autenticada quanto à origem, data de criação, conteúdo do dado, tempo de envio, etc. Esse conceito é importante para a compreensão das redes pública e privada no processo de autorização ou não de leitura e escritura na *blockchain*. No caso da rede pública de *blockchain*, não há necessidade de permissão de uma autoridade para escrever e ler na *blockchain*, porém é altamente resistente a censura, o que pode lhe conceder uma noção de imutabilidade.
- Disponibilidade (da informação ou de serviços): assegura o acesso das entidades autorizadas aos dados relevantes.

É mister ressaltar que o presente trabalho não possui o escopo de esgotar as definições de *Blockchain* e de seus aspectos intrínsecos e extrínsecos. Contudo, busca-se apresentar uma base razoável de conceitos que assegurem a compreensão da tecnologia de maneira mais simplificada e acessível aos não especialistas em TI.

3.3 Componentes da Blockchain

Para que se possa compreender a tecnologia *blockchain*, é necessário que destaquemos alguns de seus principais componentes, sendo estes elementos básicos que abrangem qualquer tipo de *blockchain*, como veremos a seguir. Notadamente que também se incluem, nesse “rol”, a rede e os nós que a integram.

3.3.1 Endereço ou chave pública

É a chamada criptografia assimétrica (BRAGA, 2017, p. 10). O endereço, numa *blockchain*, se assemelha a um e-mail, perante o qual se realizam as transações entre pessoas dentro do bloco. O endereço na rede *blockchain* é criptografado e, quando de sua criação, é concomitantemente gerada uma chave privada ou senha (ANTONOPOULOS apud LYRA, 2019, p. 20).

3.3.2 Chave privada ou senha

Segundo Lyra dispõe, a chave privada seria "a única forma de acesso para destravar os *tokens* e enviar para um determinado endereço" (LYRA, 2019, p. 20). Em caso de perda da chave, é impossível mover os *tokens* do endereço segundo o qual se encontram vinculados (LYRA, 2019, p. 20).

3.3.3 Token

Trata-se de uma unidade de troca ou transação de uma cadeia de blocos, podendo atuar como voto, registro, atestado, utilitário, direito de propriedade, ativo, moeda e identidade, por exemplo (ANTONOPOULOS; WOOD apud LYRA, 2019, p. 21). Quando o *token* assume mais de uma função, ele é considerado híbrido (LYRA, 2019, p. 21).

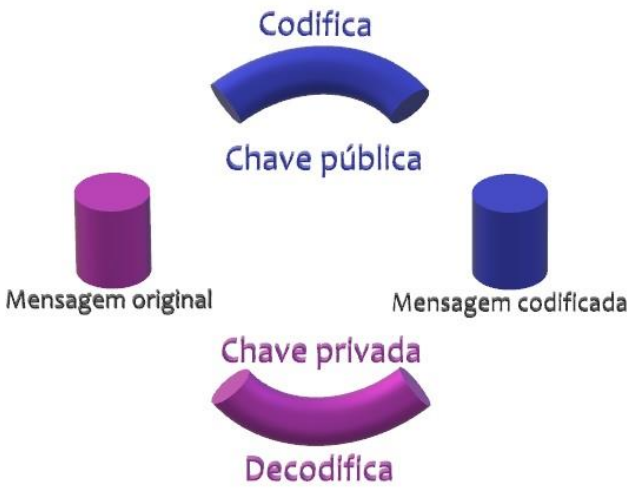
3.3.4 Criptografia

Frequentemente, as *blockchains* se utilizam de duas sequências criptográficas: a função *hash* ou "função de resumo criptográfico", para gerar endereços, "que consistem de valores *hash* calculados a partir das chaves públicas" (BRAGA, 2017, p. 10); e a assinatura digital, como garantia de autenticidade e confiabilidade da transação (BRAGA, 2017, p. 10).

O *hash* é um algoritmo que mapeia dados grandes e os comprime em dados de tamanhos mínimos e variáveis. Entende-se que a função de *hash* seria unidirecional em face de sua irreversibilidade, já que não se pode reaver o documento original através da sequência binária do *hash* (BRAGA, 2017, p. 10). Ademais, de maneira ideal, não seria possível gerar o mesmo valor de *hash* para mais de um documento (BRAGA, 2017, p. 10). Nesse caso, cada bloco que compõe a *blockchain* contém um conjunto de transações as quais, individualmente, possuem uma "impressão digital" criptográfica chamada "*hash*" (BERRYHILL et al, 2018, p. 15). O *hash* corresponde a uma chave exclusiva, portanto.

As chaves pública e privada são utilizadas de maneira conjunta, havendo a necessidade da combinação – mínima - de ambas para a garantia da segurança. Mougayar (2017) faz uma analogia a uma porta que precisa de duas chaves para ser aberta (MOUGAYAR, 2017, p. 12). A chave pública serve para o remetente codificar a informação que só será decodificada pelo proprietário da chave privada (MOUGAYAR, 2017, p. 12). A figura 2 ilustra, simplificadamente, o funcionamento da criptografia por meio das chaves pública e privada:

Figura 3 - processo criptográfico de chaves simplificado



Fonte: própria.

A assinatura digital, por outro lado, "[...] é uma computação matemática usada para provar a autenticidade de uma mensagem ou documento (digitais)" (MOUGAYAR, 2017, p. 12-13). A função da criptografia assimétrica - de chave pública - para assinatura digital – de chave privada - seria assegurar "integridade, autenticidade e irrefutabilidade" (BRAGA, 2017, p. 10). A assinatura digital é operacionalizada da seguinte forma, o titular da chave privada gera

a informação assinada, a qual pode ter sua autenticidade verificada por quem conheça da chave pública vinculada (BRAGA, 2017, p. 10). Tendo em vista que consta uma assinatura gerada por meio de chave privada, o assinante não pode negar sua autoria, sendo a assinatura, logo, irrefutável (BRAGA, 2017, p. 11).

A criptografia se fundamenta na hegemonia público-privada, ao passo que há visibilidade pública, contudo, a verificação se dá no âmbito privado (MOUGAYAR, 2017, p. 13).

3.3.5 Carimbo de tempo

Os carimbos de tempo ou *timestamps* são os registros de data e hora exatos da adição do bloco na *blockchain* e é adicionado a cada bloco para comprovar o momento de sua criação. Aos novos blocos, são adicionados dois carimbos de tempo em sua *hash*: um que ateste a sua origem e outro que comprove data e hora da criação do bloco anterior, reforçando os blocos anteriores (NAKAMOTO, 2008, p. 2).

3.3.6 Blocos

Os blocos são, cada um, um conjunto de transações validadas e agrupadas de forma que a informação esteja acessível, porém impossibilitando eventuais tentativas de adulteração (BERRYHILL et al, 2018, p. 15). Ademais, destaca-se que os blocos são dependentes entre si, relacionados intrínseca e linearmente, em ordem sequencial dos próprios *hashes* únicos, formando, portanto, uma corrente verificável e rastreável (BERRYHILL et al, 2018, p. 15).

Para que tenham validade, os blocos passam por processos predeterminados - conhecidos como mineração no caso da *Bitcoin* - que confirmem a legitimidade da transação. Todos os nós são informados do processo e, somente após passar por um processo de autenticação pelos nós participantes - utilizando-se as regras do protocolo de consenso definido -, o bloco é inserido na cadeia/corrente, ocorrendo, consequentemente, um novo processo de criação do bloco autenticado em cada um dos nós (FILHO et al., 2017, p. 9). Poderíamos considerar a estrutura semelhante ao panóptico de Foucault ao passo que todos os nós “vigiam” uns aos outros nesse processo de validação e autenticação dos blocos inseridos. Entretanto,

pode-se cogitar que a divergência entre o panóptico e a BC é que a BC não possui uma estrutura de vigilância oculta, há uma fiscalização mútua para assegurar a veracidade e integridade das informações transacionadas entre eles. Deste modo, pode-se entender a BC como uma eventual solução para a construção de uma sociedade mais democrática, com a necessidade de decisões conjuntas nas transações decorrentes dela e a possibilidade de um controle social mais eficiente.

3.4 Tipos de Blockchain

Pode-se afirmar que existem dois tipos de rede *blockchain*, podendo esta assumir uma estrutura de rede pública ou de rede privada. A *blockchain* pública ou não-permissionada não possui um proprietário única, permitindo, assim, que qualquer pessoa possa contribuir com dados, além de todos deterem cópias idênticas dela (FINCK, 2018, p. 670). Nesse caso, há maior resistência à censura e torna-se mais difícil de hackear, entretanto, também é mais complexo para se governar (FINCK, 2018, p. 670).

Ainda, a rede *blockchain* não-permissionada pode ser definida como plataformas descentralizadas de livro-razão, de *software open source*[5], abertas a qualquer um que publique blocos, sem a exigência de autorização de alguma autoridade (YAGA et al, 2018, p. 5). O fato de a estrutura da rede não-permissionada ser aberta a todos os participantes pode propiciar que usuários mal intencionados tentem publicar blocos que subvertam o sistema, contudo, a rede previne esses tipos de ataques por meio do uso de acordo multipartidário ou o chamado sistema de "consenso", segundo o qual os usuários precisam gastar ou manter recursos no momento de tentativa de publicação de blocos (YAGA et al, 2018, p. 5).

Já no caso das redes privadas ou permissionadas, há um ou mais proprietários e, quando há um novo registro, a integridade do livro-razão é verificada por um processo de consenso limitado conduzido por atores confiáveis (FINCK, 2018, p. 670). A publicação de blocos, nesse caso, deve ocorrer com a permissão da autoridade responsável, seja ela centralizada ou descentralizada (YAGA et al, 2018, p. 5). Levando em consideração que apenas usuários autorizados são mantidos na *blockchain* permissionada, é possível restringir o acesso de leitura e de quem poderá realizar transações (YAGA et al, 2018, p. 5). A *blockchain*

[5] Software de fonte aberta.

permissionada porde ser originada e mantida utilizando-se código aberto ou fechado (YAGA et al, 2018, p. 5).

As redes permissionadas possuem a mesma capacidade de rastreabilidade de ativos digitais, além de o mesmo sistema distribuído, resiliente e redundante de armazenamento de dados que as redes não-permissionadas (YAGA et al, 2018, p. 5). Destarte, aqui também são usados modelos de consenso, entretanto, pode diferenciar-se das redes não-permissionadas, no caso da contrapartida monetária, em razão do estabelecimento da identidade dos participantes como membros da rede permissionada, bem como já existe um nível de confiança entre os integrantes entre si, visto que todos possuem autorização para publicar blocos e essa autorização pode ser revogada em caso de mal comportamento (YAGA et al, 2018, p. 5-6). O consenso, na *blockchain* permissionada, é normalmente mais rápido e de menor custo computacional que na rede não-permissionada (YAGA et al, 2018, p. 6).

Ainda, é possível realizar uma seletividade na transação de informação entre os participantes da rede permissionada de acordo com a identidade ou a credencial concedida, o que assegura um certo nível de privacidade nos casos em que a informação em si remete apenas a alguns dos participante e, não, a todos, ficando disponível a todos, porém a visualização do conteúdo restrita aos interessados na questão (YAGA et al, 2018, p. 6).

A principal diferença entre as *blockchains* pública e privada é que, apesar de sua caraterística de livro-razão distribuído sem a atuação do controle central de uma autoridade determinada, é possível, sim, ser estruturada como sistema fechado, como ocorre no caso da rede privada (FINCK, 2018, p. 670).

Acerca da rede permissionada ou privada, Martinovic destaca a existência de dois tipos principais: a "baseada em consórcio" e a "integralmente privada" (MARTINOVIC, 2017, p. 11, tradução livre). Em ambas, há um (ou mais) proprietário(s), o que permite que o processo de obtenção de consenso seja mais simples. Por outro lado, o direito de leitura da *blockchain* pode ser público ou restrito a um grupo de indivíduos, podendo a restrição, inclusive, possuir diferentes níveis de abstração (MARTINOVIC, 2017, p. 11-12). Esses tipos de redes *blockchain* são tidas como parcialmente descentralizadas, visto que membros do público podem fazer consultas limitas e receber prova do estado da *blockchain* (MARTINOVIC, 2017, p. 12). A rede integralmente privada é aquela na qual a permissão de escrever na *blockchain* se encontra centralizada e gerenciada por uma única organização, enquanto a permissão de leitura permanece pública (MARTINOVIC, 2017, p. 12).

Segundo dispõe Martinovic (2017, p. 12), as principais vantagens da *blockchain* permissionada são as seguintes:

- A autoridade gerenciadora da *blockchain* privada poder, facilmente e caso queira, alterar as regras da mesma, reverter transações, modificar dados, etc;
- O fato de os integrantes da *blockchain* serem conhecidos mitiga os riscos de possíveis ataques;
- São mais eficientes, visto que contam com a verificação das transações apenas por participantes conhecidos e com um alto poder de processamento;
- A infraestrutura da rede poder ser planejada e controlada;
- E, nos casos de utilização de permissões restritas, a rede pode gerar um grande nível de privacidade.

Por outro lado, a maior desvantagem da rede privada seria a ausência de imutabilidade, característica essa responsável pela garantia de não alteração de dados dentro da *blockchain*, não obstante, essa seria a maior vantagem das redes públicas (MARTINOVIC, 2017, p. 12). Ainda, a rede permissionada não garante a transparência para todos os cidadãos, dependerá do investimento do governo em determinado tipo de *blockchain*, sendo que esse investimento varia de acordo com a finalidade dessa rede. No que tange o bCPF, a cadeia de blocos deve realmente ser privada em face do caráter das transações a que se destina.

3.5 Smart Contracts

O conceito de *smart cotracts* ou contratos inteligentes foi desenvolvido por Nick Szabo, em 1994, porém somente retornou às discussões quando do surgimento da tecnologia Bitcoin, no ano de 2009, tendo se tornado um princípio elementar de *blockchain* (MOUGAYAR, 2017, p. 43).

Os contratos inteligentes (CI's) são códigos de execução automática, salvo se houver mecanismos que a previnam, por um sistema de computadores e serve para eliminar riscos de contrapartida (FINCK, 2018, p. 670). Todavia, não são considerados Inteligência Artificial – a qual exige resultado externo para determinar eventos do mundo real – e nem contratos legais (FINCK, 2018, p. 670). Os contratos inteligentes são escritos no código-fonte e têm como

função a criação de acordos digitais com a certeza de cumprimento em todos os bancos de dados das partes envolvidas (FINCK, 2018, p. 671).

Os nós dentro da rede *blockchain* são os executores do contrato inteligente, devendo todos eles auferir os mesmos resultados e estes serem devidamente registrados na *blockchain* (YAGA et al, 2018, p. 32). O usuário que queira realizar uma transação envia os dados para as funções públicas oferecidas pelo CI e o mesmo realiza o método mais adequado para a execução do serviço (YAGA et al, 2018, p. 32). Destarte, tendo em vista que o código se encontra dentro da *blockchain*, também é revestido de inviolabilidade, podendo ser utilizado como um terceiro participante, dentre outras alternativas (YAGA et al, 2018, p. 32).

O CI pode representar uma transação multipartidária, especialmente em processos de negócios, tendo como vantagens a confiabilidade dos dados, transparência, confiança, possibilitando um discernimento que gere em uma melhor tomada de decisão, reduzindo custos inerentes ao processo tradicional de negócios e o tempo gasto para completar a transação (YAGA et al, 2018, p. 32).

Ademais, os contratos inteligentes devem ser determinístico, uma vez que a definição de um *input* deve gerar sempre o mesmo *output*, não há margem para interpretações divergentes na execução do código (YAGA et al, 2018, p. 32). Portanto, o comportamento da transação é programado e, tão logo ocorra a transação, o contrato é executado automaticamente.

Tendo em vista que os contratos inteligentes operacionalizam as redes permissionadas, não há exigência de contrapartida monetária para a execução do código do contrato inteligente, diferentemente das redes não-permissionadas que utilizam dessa medida para fins de garantia de segurança contra ataques de usuários maliciosos, já que os participantes são conhecidos e há previsão de outros mecanismos de prevenção a maus comportamentos, como é o caso da revogação do acesso do determinado participante (YAGA et al, 2018, p. 32-33).

4 Aplicação prática de Blockchain no mundo

Apesar de haver pesquisas acerca do uso da *blockchain*, poucos a tratam de maneira acessível aos leigos em tecnologia da informação e menos ainda se trata de sua aplicabilidade ao setor público.

A aplicação concreta da tecnologia *blockchain* ainda não é muito extensa, entretanto, trata-se de uma grande inovação que deverá angariar mais adeptos a cada dia. *Blockchain* tem sido considerada como potencializadora de transformar a forma de prestação de serviços públicos e privados, bem como de aumentar a produtividade em face da gama de aplicações disponíveis (Matt Hancock & Ed Vaizey apud FINCK, 2018, p. 671-672).

No setor público, a *blockchain* tem a possibilidade de ser utilizada para a verificação de transações e mudanças de registros-chave, acordos e quaisquer outros que estejam categorizados como *data-at-rest* ou dados inativos armazenados, não se incluindo, logo, os *data-in-use* ou dados ativos ou em processo (MARTINOVIC, 2017, p. 14).

Tendo em vista os mecanismos de rastreamento de bens e pagamentos da *blockchain*, na África, desenvolveu-se o BitPesa, um banco que oferece serviços bancários móveis baseados em *blockchain*, possibilitando transferências de remessas rápidas e de baixo custo (FINCK, 2018, p. 672). Qualquer coisa pode ser representada por *tokens* e transacionada em um livro-razão distribuído, como é o caso do projeto entre uma *start-up* local e a empresa Siemens em Nova Iorque, nos EUA, tendo em vista que a *blockchain* desenvolvida facilita as operações de grades de energia inteligente urbana, na qual vizinhos vendem e compram energia uns dos outros (FINCK, 2018, p. 672).

A capacidade da *blockchain* de criar registros invioláveis tem sido o suficiente para se testar uma nova forma de administração oficial dos registros públicos, como certidão de nascimento, de casamento e escritura de imóvel, por exemplo. No estado de Georgia, EUA, tem-se iniciado um projeto-piloto sobre registro de imóveis (FINCK, 2018, p. 673).

Em termos de aplicação da tecnologia *blockchain*, a Estônia é o país pioneiro, sendo uma liderança no que tange o desenvolvimento das sociedades da informação (MARTINOVIC, 2017, p. 14). No ano de 2000, a Estônia declarou o acesso à Internet um direito humano, tendo desdobrado esse direito para atingir as áreas rurais e influenciado inovações no uso de tecnologia digital, tendo, inclusive, sua expertise digital reconhecida pela denominação de “e-Estônia” (MARTINOVIC, 2017, p. 14-15). Destarte, no mesmo ano, seu Parlamento aprovou

o Ato de Assinatura Digital, na qual a assinatura digital seria equiparada à manual (MARTINOVIC, 2017, p. 15).

Na Estônia há experimento de aplicação de livro-razão no governo, como o uso de *Keyless Signature Infrastructure* (KSI) para conceder aos cidadãos acesso a seus registros e bases de dados governamentais (FINCK, 2018, p. 673). Essa tecnologia está integrada a registros fundamentais de governo, como é o caso dos registros de negócios, de propriedade, de direito sucessório, de arquivos digitais judiciais e de anúncios oficiais (MARTINOVIC, 2017, p. 15).

Outra plataforma desenvolvida pelo governo da Estônia é o X-Road, a qual funciona interligando diferentes instituições governamentais, facilitando o exercício do governo por meio da utilização de tecnologia (MARTINOVIC, 2017, p. 16). Trata-se do principal meio de comunicação de serviços públicos e ampara a escritura de diversos bancos de dados, transmitindo grandes conjuntos de dados e realizando buscas em vários bancos de dados (MARTINOVIC, 2017, p. 16). Ademais, o X-Road garante a segurança por meio da autenticidade, integridade e não-repúdio da troca de dados, bem como da alta disponibilidade dos serviços e confidencialidade da troca de dados (MARTINOVIC, 2017, p. 16). Nesse sentido, poderíamos entender que o segredo no que tangem os dados pessoais dos cidadãos seria fundamental? A tecnologia BC colocaria limitações à teoria do Bobbio? Ou estamos falando de dois tipos diferentes de segredo? Bobbio afirma que o segredo não possui valoração de bom ou mau, dispondo que ele é conhecido ainda que seu conteúdo esteja reservado a alguns poucos indivíduos (BOBBIO, 2015, p. 78-79). Por outro lado, é importante destacar que os Estados não exercem todas as atividades sozinhos, fazendo uso de parcerias público-privadas para a prestação de serviços também, o que nos leva a questionar se o uso da BC no setor público não acabaria por tornar os dados dos cidadãos reféns de empresas privadas cujo único escopo é obter lucro.

Deste modo, concebe uma forma segura de gerenciamento de dados dos cidadãos por parte do Estado, tendo também representado o enxugamento da máquina estatal e dos seus serviços ineficientes, o que nos leva a concluir que o uso da tecnologia *blockchain* possui a capacidade de aumentar a eficiência do setor público, bem como aumentar a cooperação entre as organizações (JALAKAS, 2018, p. 39).

No Reino Unido, tem-se analisado a possibilidade de aplicação de tecnologia *blockchain* para coibir fraudes e erros no pagamento de pensões, o que poderia resguardar uma quantidade consideravelmente grande de perda de dinheiro público com o registro e

processamento de pagamentos e benefícios concedidos pelo governo dentro de uma *blockchain* (MARTINOVIC, 2017, p. 26).

Outrossim, cabe mencionar o caso do governo da Suécia, o qual, por meio de uma parceria com empresas privadas, pretende aplicar a tecnologia *blockchain* nos casos que envolvem transações imobiliárias, estando o projeto ainda em fase de teste (MARTINOVIC, 2017, p. 27). Martinovic destaca os pontos principais os quais o projeto almeja alcançar, são eles: aumento da transparência das transações, aumento da eficiência do processo de modo geral e diminuir a complexidade do processo de modo geral (MARTINOVIC, 2017, p. 27).

4.1 Desafios na adoção da Blockchain no governo

A tecnologia *blockchain* possui diversas vantagens no que tange à garantia da eficiência e da transparência no serviço público, bem como assegura a confiança e a verificabilidade deste. Todavia, vislumbram-se alguns obstáculos a sua aplicação de maneira generalizada. A maioria das aplicações concretas de *blockchain* são ainda experimentais, havendo pouquíssimos sistemas de produção em uso (DOMINGUE, 2018, p.11).

Domingue (2018, p. 13-14) destaca algumas barreiras conhecidas ao emprego da *blockchain* no sistema governamental, quais sejam:

- Interdependência: necessidade de adoção de um sistema de identidade confiável como base e a possibilidade de que, serviços interagentes utilizem de sistemas de identidade compatíveis coordenados, facilitando, deste modo, o perpasso pelos serviços. Esse é tido como a maior questão a ser superada.
- Harmonização do legado: integração entre a nova tecnologia e os sistemas de legado existentes. Sistemas de legado são sistemas de informação velhos e antiquados (IONITA et al, 2012, p. 127). No caso do setor governamental, a integração deve abarcar tanto de maneira técnica/operacional quanto a questão legal/jurídica.
- Interoperabilidade técnica e maturidade: coordenação integrada entre as iniciativas *blockchain* ao redor do mundo. Nesse caso, leva-se em conta que *blockchain* é uma tecnologia recente e de rápido desenvolvimento, estando sujeita a instabilidades, o que afeta a absorção da mesma e seus impactos.

Todavia, Domingue alerta para a possibilidade de se buscar sanar esse obstáculo tarde demais, em face do contexto de competitividade e desenvolvimento na qual a tecnologia se insere, podendo inviabilizar a harmonização.

- Proteção de dados e privacidade: em se tratando da *blockchain* pública, os dados são amplamente distribuídos entre os participantes, bem como existem várias formas de armazenamento de dados dentro da *blockchain*, o que impacta diretamente em regulamentações de proteção de dados e privacidade. O importante a se ressaltar é a aplicação da proteção fora das fronteiras estatais, visto que cada Estado possui soberania e suas próprias normas jurídicas. Contudo, Domingue não conjectura riscos de desconformidades e grandes conflitos entre regulações, dada a visibilidade do GDPR.

Notadamente que, em razão de se tratar de uma tecnologia nova e pouco explorada até o momento, não há como prever todos os possíveis e eventuais desafios de sua implementação, seja no setor privado, seja no setor público.

5 Discussão e análise de dados

Far-se-á uma apresentação do projeto bCPF analisado nessa pesquisa, bem como dos elementos intrínsecos ao compartilhamento de dados cadastrais e entes envolvidos. Depois, será realizada uma correlação dos dados obtidos por meio de duas entrevistas semi-estruturadas, uma com o Auditor-fiscal da RFB, e outra com o Assessor de Diretoria na Dataprev, com os construtos teóricos abordados previamente.

No primeiro tópico, será apresentado o panorama geral do bCPF, elencando sua previsão legal e regulamentação, aspectos intrínsecos e componentes inerentes à tecnologia *blockchain* aplicáveis ao projeto. Apresentar-se-ão os modelos de compartilhamento de dados da Administração Federal antes e com o bCPF, verificando suas vantagens e desvantagens.

No segundo tópico, far-se-á uma análise da *blockchain* como uma solução estratégica facilitadora do *doing business* e as implicações de sua implementação no setor público. Ainda, será tratada a questão da desburocratização possibilitada pelo uso da referida tecnologia.

No terceiro tópico, serão discutidos os aspectos inerentes ao tema da segurança e da proteção dos dados pessoais, os quais a utilização da *blockchain* pode ser capaz de solucionar de maneira eficiente, verificando as propriedades utilizadas no desenvolvimento do bCPF que se possibilitam assegurar esses pontos. Também será tratado o segredo como meio de garantia de segurança, a questão da confiança e dos elementos de transparência presentes na *blockchain* (open-source).

Por fim, no quarto tópico, tratar-se-á da auditabilidade proporcionada pela aplicação da tecnologia *blockchain* e de que maneira ela será realizada no âmbito do bCPF. Ademais, serão apresentados, como categoria de análise, os possíveis desafios de implementação do bCPF na Administração Pública Federal com base no que já foi estudado até agora e características do projeto e do setor público de modo geral.

5.1 O caso do bCPF

O compartilhamento dos dados cadastrais, como a base no Cadastro de Pessoas Físicas (CPF), é um dever das administrações tributárias da União, dos Estados, do Distrito Federal e dos Municípios, conforme dispõe o art. 37, inciso XXII, da Constituição Federal de 1988.

O CPF é um número de identificação de utilização recorrente no país, não somente pelas administrações tributárias, havendo em torno de 800 convênios de compartilhamento de informações entre a Receita Federal e as várias entidades de todos os níveis federativos e poderes, segundo dados da própria Receita Federal (Receita Federal, on-line)[6]. O auditor-fiscal da RFB prevê centenas de atores envolvidos, mas não sabe ao certo precisar quem são ainda, visto que os convênios ainda estão em fase de negociação. Contudo, num primeiro momento, não vislumbra a possibilidade de inclusão de empresas privadas. Conforme o Assessor de Diretoria da Dataprev, o credenciamento dos entes autorizados se dá da seguinte maneira: "Os entes autorizados são identificados pela RFB, a qual firma um convênio formal. Após o convênio ser firmado o ente está apto a contratar o serviço da Dataprev".

O compartilhamento de dados dessa base cadastral deve obedecer a parâmetros de proteção de dados, sendo importante trazer atenção à possibilidade de rastreamento dos dados sem obstaculizar demais o acesso a eles pelas entidades autorizadas (Receita Federal, on-line)[7].

Nesse sentido, a nova tecnologia *Blockchain* possui como principal característica a capacidade descentralizadora, permitindo a disponibilização de um conjunto de dados complexos de maneira comprimida, distribuída, imutável e facilitando seu rastreamento quanto a qualquer tentativa de alteração de dados, o que assegura maior confiança e segurança no tratamento dos dados (Receita Federal, on-line)[8].

A Receita Federal publicou no Diário Oficial da União, a Portaria RFB nº 1.788/2018 - que altera a Portaria RFB nº 1.639/16 - sobre a disponibilização de dados no âmbito da administração pública federal envolvendo a tecnologia *blockchain*.

---

[6] **Receita Federal publica norma sobre compartilhamento de dados utilizando tecnologia Blockchain**. Receita Federal, publicado em 21/11/2018, com última alteração em 04/04/2019. Disponível em: <https://receita.economia.gov.br/noticias/ascom/2018/novembro/receita-federal-publica-norma-sobre-compartilhamento-de-dados-utilizando-tecnologia-blockchain>. Acesso em 28/05/2019.

[7] **Receita Federal publica norma sobre compartilhamento de dados utilizando tecnologia Blockchain**. Receita Federal, publicado em 21/11/2018, com última alteração em 04/04/2019. Disponível em: <https://receita.economia.gov.br/noticias/ascom/2018/novembro/receita-federal-publica-norma-sobre-compartilhamento-de-dados-utilizando-tecnologia-blockchain>. Acesso em 28/05/2019.

[8] **Receita Federal publica norma sobre compartilhamento de dados utilizando tecnologia Blockchain**. Receita Federal, publicado em 21/11/2018, com última alteração em 04/04/2019. Disponível em: <https://receita.economia.gov.br/noticias/ascom/2018/novembro/receita-federal-publica-norma-sobre-compartilhamento-de-dados-utilizando-tecnologia-blockchain>. Acesso em 28/05/2019.

A Dataprev, criada pela Lei nº 6.125/74, é uma empresa pública vinculada ao Ministério da Economia, que provém soluções de Tecnologia da Informação e Comunicação para o aprimoramento e a execução de políticas sociais do Estado. Teve seu primeiro estatuto aprovado pelo Decreto nº 75.463/75 e sua instalação pela Portaria Ministerial nº 189/75. Sua composição acionária se dá na seguinte proporção: 51% de participação da União e 49% do INSS (Dataprev, on-line)[9].

O chamado solução bCPF (*Blockchain* do Cadastro de Pessoas Físicas) é uma solução G2G (*Government to Government* – Governo para Governo) desenvolvida pela Dataprev para a Receita Federal buscando simplificar o processo de disponibilização da base de dados CPF sem comprometer os mecanismos de segurança, integridade e a eficiência. O projeto piloto conta com a participação do Conselho de Justiça Federal (Receita Federal, on-line)[10].

Essa implementação da tecnologia *Blockchain* pela Receita Federal conta com uma abordagem de rede permissionada, ou seja, apenas as entidades autorizadas terão acesso à cadeia de informações objeto do bCPF. Toda a tecnologia está fundamentada em software livre de código fonte aberto e auditável (Receita Federal, on-line)[11].

Ademais, a solução bCPF também prevê, inclusive, a figura dos *smart contracts* (contratos inteligentes[12]), também utilizador da tecnologia *blockchain* para prever funcionalidades e controles adicionais que tornam o bCPF seguro e possível (Receita Federal, on-line)[13].

---

[9] **Dataprev desenvolve solução com tecnologia Blockchain para compartilhamento da base CPF**. Dataprev, 22/11/2018. Disponível em: <https://portal.dataprev.gov.br/dataprev-desenvolve-solucao-com-tecnologia-blockchain-para-compartilhamento-da-base-cpf>. Acesso em 28/05/2019.

[10] **Receita Federal publica norma sobre compartilhamento de dados utilizando tecnologia Blockchain**. Receita Federal, publicado em 21/11/2018, com última alteração em 04/04/2019. Disponível em: <https://receita.economia.gov.br/noticias/ascom/2018/novembro/receita-federal-publica-norma-sobre-compartilhamento-de-dados-utilizando-tecnologia-blockchain>. Acesso em 28/05/2019.

[11] **Receita Federal publica norma sobre compartilhamento de dados utilizando tecnologia Blockchain**. Receita Federal, publicado em 21/11/2018, com última alteração em 04/04/2019. Disponível em: <https://receita.economia.gov.br/noticias/ascom/2018/novembro/receita-federal-publica-norma-sobre-compartilhamento-de-dados-utilizando-tecnologia-blockchain>. Acesso em 28/05/2019.

[12] Contratos inteligentes são códigos, inscritos no código fonte da BC, que estabelecem regras de cumprimento automático nos bancos de dados.

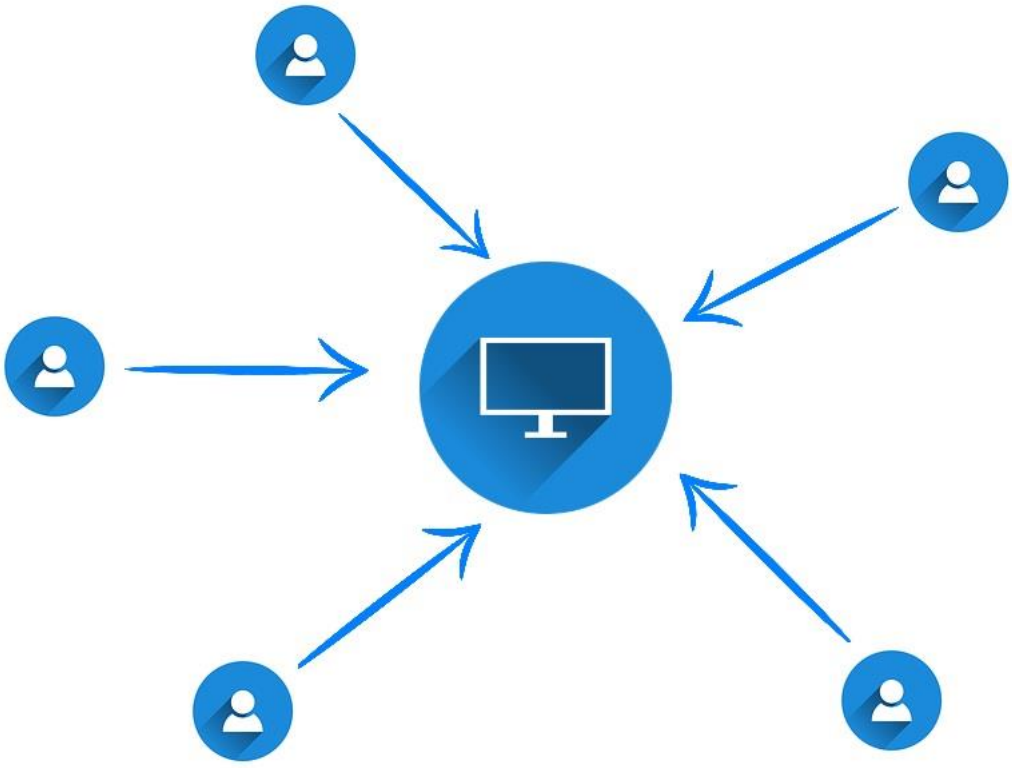
[13] **Receita Federal publica norma sobre compartilhamento de dados utilizando tecnologia Blockchain**. Receita Federal, publicado em 21/11/2018, com última alteração em 04/04/2019. Disponível em: <https://receita.economia.gov.br/noticias/ascom/2018/novembro/receita-federal-publica-norma-sobre-compartilhamento-de-dados-utilizando-tecnologia-blockchain>. Acesso em 28/05/2019.

O modelo de *Blockchain* da Receita Federal prevê os seguintes tipos de participação[14]:

> (i) a participação apenas para consumo dos dados;
>
> (ii) a participação para contribuição sobre um campo do dado e;
>
> (iii) a participação para alteração do dado, esta última a ser realizada pela entidade com as prerrogativas legais para esta ação prevista em contratos inteligentes.

Faz-se necessário diferenciar os modelos de compartilhamentos de dados anterior e atual, com o bCPF. Segundo expõe o Auditor-fiscal da RFB, o modelo anterior seguia um paradigma centralizado, o qual contava com um computador central funcionando no SERPRO e os órgãos que quisessem informações precisariam solicitar a esse computador central, conforme ilustra a figura a seguir.

Figura 4 - modelo de compartilhamento de dados centralizado da RFB



Fonte: própria.

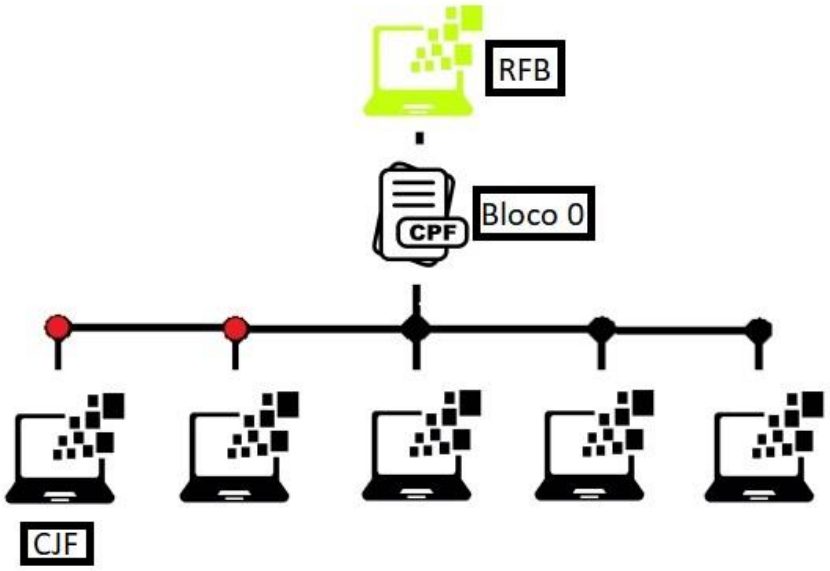
[14] **Receita Federal publica norma sobre compartilhamento de dados utilizando tecnologia Blockchain**. Receita Federal, publicado em 21/11/2018, com última alteração em 04/04/2019. Disponível em: <https://receita.economia.gov.br/noticias/ascom/2018/novembro/receita-federal-publica-norma-sobre-compartilhamento-de-dados-utilizando-tecnologia-blockchain>. Acesso em 28/05/2019.

No caso do bCPF, houve uma transformação do paradigma centralizado num paradigma paralelizado *peer-to-peer*. Sendo assim, o Auditor-fiscal da RFB afirma o seguinte:

> Então a Receita, quando ela escreve, graças ao paradigma de banco de dados distribuído, todo mundo recebe automaticamente e [...] se eu sair do ar, esse cara replica pros outros camaradas. [...] Tem o problema de confiança ou de desconfiança. [...] Aqui é uma rede permissionada, aqui eu tenho o paradigma centralizado onde só eu escrevia e todo mundo consome a informação. Aqui eu criei um *smart contract* e gravei no bloco 0, no primeiro bloco do *blockchain*, quando ninguém tava existindo, [...] só tinha eu no *blockchain*, a Receita [...], só a Receita escreve, ninguém mais escreve. [...] Quando eles vieram, o *smart contract* foi copiado e tá gravado no bloco 0. Só quem escreve, portanto, é a Receita, a pessoa só consome. Então o problema de confiança aqui não é um problema [...] tão óbvio, é [...] como fazer troca de informação com confiança contra, em antagonismo, em diferença ao modelo centralizado, que é confiável por ser centralizado. Aí a gente resolveu o problema.
>
> [...]
>
> A gente fez uma coisa revolucionária. Aqui, nesse modelo, a CEB consumia a informação, mas ela não podia escrever. [...] Nós fizemos o seguinte, [...] a CEB escreveu sugestão Juliana Asa Norte. [...] No dia seguinte, a NET falou ela mudou da Asa Sul para a Asa Norte, sugestão NET Asa Sul Asa Norte. A Juliana não alterou a base CPF dela, mas eu "tô" recebendo um monte de gente sugerindo que ela mudou de endereço. No modelo centralizado, eu não consigo fazer isso, mas aqui, graças à onerosa guarda de todos os bloquinhos [...], 10 falaram que ela mudou, "tá" aí, ela mudou.

Logo, há um compartilhamento automático das informações constantes do banco de dados, sendo que foi criado um contrato inteligente estabelecendo que somente a Receita Federal poderá escrever na *blockchain* e os outros integrantes apenas consumirão o conteúdo – ressalva-se que, no contrato inteligente do bCPF, há previsão de que os demais membros possam fazer sugestões apenas e nenhuma alteração. Com base nas informações coletadas, o modelo bCPF pode ser ilustrado da seguinte maneira:

Figura 5 - modelo de compartilhamento de dados do bCPF



Fonte: própria.

Na figura acima, podemos observar o contrato inteligente gravado no Bloco 0, a Receita Federal como controladora da *blockchain* e os membros conectados, sendo os pontos vermelhos exemplos de quem poderia fazer as sugestões e os pontos pretos de quem apenas pode observar. A grande vantagem do bCPF é justamente essa integração maior entre os órgãos, permitindo aos mesmos, dentro das regras estabelecidas, auxiliar de maneira mais eficiente na gestão pública.

O Auditor-fiscal da RFB informa que o modelo centralizado é o mais rápido, mais econômico e mais confiável de todos. Todavia, o modelo paralelizado da *blockchain* acaba sendo mais barato financeiramente, apesar de ser caro tecnologicamente, porque o pagamento se dá de maneira distribuída. O modelo do bCPF é necessariamente lento porque “tem que minerar o dado, tem que encadear os blocos, tem que propagar os blocos. É claro que é lento em segundos, mas é lento”. Ainda, ele “é mais fácil de colocar uma aplicação no ar, usa as 500.000 linhas que tão prontas. Mas a alteração é caríssima, às vezes, você tem que derrubar a rede e começar de novo. Tem que refazer tudo”. O fato de as linhas de códigos já estarem prontas significa que há um molde padrão, que pode ser utilizado por qualquer pessoa, no qual as especificidades mínimas decorrentes do caso concreto poderão ser acopladas a ele para criar a rede, havendo uma redução enorme de força de trabalho.

5.2 Blockchain como uma solução estratégica

A partir das informações obtidas na entrevista com o Auditor-fiscal da Receita Federal, a *blockchain* vai muito além da criptomoeda. Ele menciona que a *blokchain* é uma solução estratégica que influencia o chamado *doing business*, ou seja, a capacidade de facilitar o negócio. A implicação dessa característica da *blockchain* seria ofertar uma solução para que governos ou empresas possam resolver problemas. Nesse sentido, ele explana o seguinte:

> *Blockchain* não é mais a questão física de cabo de rede interligando computadores, *blockchain* é uma solução lógica, não é do mundo físico, tangível, é do mundo da lógica, do *software*. É uma solução *software*, uma solução lógica que permite um próximo passo que o cabo de rede permitiu, ele permite integração. E aí ele facilita o *doing business*.

Desta maneira, a integração deixa de ser tangível e passa a ser lógica. É importante fazer um destaque na correspondência entre a sociedade e a máquina realizada por Deleuze, segundo a qual as sociedades antigas faziam uso de máquinas simplórias, as sociedades disciplinares, de máquinas energéticas, e as sociedades de controle, de máquinas de informática e computadores, não representando apenas uma evolução de cunho tecnológico, mas, principalmente, desenvolvimento do próprio capitalismo (DELEUZE, 1992, p. 223). A forma como nos conectamos em nossas relações sociais não é a mesma de antigamente, com o advento da *internet* e das redes sociais, bem como as relações comerciais sofreram suas devidas modificações e adequações aos modelos tecnológicos que vem surgindo com o tempo. Todavia, deve-se endereçar um problema muito recorrente nas relações jurídicas, que é o da confiança. Nesse sentido, o Auditor-fiscal da RFB dispõe:

> A *blokchain* é composta por três aspectos tecnológicos principais: é um banco de dados distribuído – todos os participantes compartilham da informação -, tudo o que é feito é gravado em pedra - nunca mais é apagado -, e *smart contracts*, isto é, "um programa de computador que é executado dentro do próprio *blockchain* e esse programa de computador está gravado em pedra dentro do próprio *blockchain* [...]".

Outra vantagem da implementação da *blokchain* no setor público é a sua característica *open-source*, visto que, além de mais uma vez garantir a confiança em virtude da disponibilidade de acesso e leitura do código fonte, as 500.000 linhas de código básicas já estão prontas, podendo o desenvolvedor acrescentar apenas algumas linhas de código para criar a rede BC pretendida, o que resulta em menor tempo gasto em trabalho.

Acerca da desburocratização, o Auditor-fiscal da RFB dispõe que "Na hora que você cria uma camada lógica que integra órgãos ou países, você desburocratizou já. Se você tem um

número de CPF, por que precisa fornecer o endereço? Precisa porque não está integrado". Logo, o setor público pode atuar de maneira mais eficiente e mais rápida com a utilização do bCPF, visto que não há mais a necessidade de solicitar a informação e aguardar o trâmite, o banco de dados fica disponível, haverá maior coordenação e integração entre os órgãos públicos federais.

5.3 Da segurança e da proteção de dados pessoais

A questão de não inclusão de empresas privadas é um fator que contribui para o aumento de confiança no projeto, visto que, em virtude do mercado crescente de dados pessoais e do capitalismo de vigilância de Zuboff (2015), a concessão de acesso a empresas privadas à base CPF seria de um risco enorme à segurança desses dados pessoais. Então, ainda que o Estado atue de maneira mais restrita acerca dos dados pessoais da base CPF, este é um procedimento fundamental para assegurar a sua proteção.

Conforme o Auditor-fiscal da RFB, o maior problema a ser enfrentado é o da confiança, vide:

> Qual é o único problema essencial que caracteriza a necessidade de você usar *blockchain*? [...] É o problema da confiança. Esse problema é gritante quando você fala de dinheiro e na criptomoeda [...] mas você tem outros tipos de problema de confiança e aí agora eu vou te dar um exemplo: suponha que esse é o mapa da América do Sul [...] nós temos computadores no data center que rodam os programas da Receita, você acha que se eu virasse pra Argentina e falasse: "- Argentina, coloca seus dados de Comércio Exterior no computador brasileiro, não coloca na Argentina não", o senhor (Secretário da Receita) acha que ela iria aceitar? "- Não". Então vamos fazer o seguinte, por que o senhor não abre mão e põe lá na Argentina? "Não vou aceitar". É um problema explícito que [...] a Argentina vai sacanear o Brasil? Não é, é um problema implícito. Não vou entregar a confiança disso pra você, eu tenho minha soberania. O problema de confiança está associado a um problema político, às vezes realmente de desconfiança, pessoas que não se conhecem. [...] Se eu tiver um banco de dados distribuído que quando eu escrevo, escreve lá, é bacana, mas pera aí, ele pode escrever lá e pode depois alterar. Um banco distribuído que quando eu escrevo aqui, escreve lá e guarda uma cópia do anterior, resolveu o problema de confiança. Dá pra usar *blockchain* pra resolver um problema que eu tô tendo hoje em dia de Comércio Exterior entre Brasil e Argentina. [...] Eu tenho mais um problema, eu não quero que os outros países do Mercosul entrem, só Brasil e Argentina. Não se preocupa, vamos fazer uma rede permissionada. Não, mas eu tenho mais um problema, eu quero que só o Presidente da República ou o Secretário da Receita estabeleça [...]. como você vai materializar a legislação dentro da tecnologia? [...] Vamos usar *Smart Contracts*!

Portanto, é possível que a *blokchain* venha a solucionar questões de desconfiança entre atores envolvidos de maneira eficiente, assegurando uma maior integração, de maneira lógica, entre eles. Outro aspecto importante do bCPF é o fato de sua estrutura ser de rede permissionada ou fechada, o que significa que apenas entes autorizados terão acesso a essa rede. O Auditor-fiscal da RFB afirma que a garantia da proteção de dados no bCPF decorre da estrutura permissionada da rede. Nesse sentido, o Assessor de Diretoria da Dataprev destaca o seguinte:

> O bCPF é um serviço o qual tem o objetivo de descentralizar a base do CPF de forma ágil, segura e econômica. O serviço foi concebido utilizando a tecnologia mais moderna de descentralização de informação, a tecnologia blockchain. Assim uma rede permissionada foi criada e através dela é descentralizada as informações de movimentação na base CPF, assim o participante mantém sua base do CPF sempre sincronizada com a base oficial garantindo a integridade e inviolabilidade dos dados.
>
> O termo permissionada é utilizado para demonstrar que a rede é privada e que existe um ente que detém o poder de permitir novos entrantes. A rede é baseada em modelo "Proof-of-authority" e cada bloco é gerado a cada 15 segundos em média, em cada bloco é armazenado um conjunto de transações de atualização da base CPF. A expectativa é que a rede supere os 500 nós e sua conexão será via Internet utilizando protocolos de criptografia do canal de transmissão.

Ainda, ele continua mencionando que a garantia da proteção dos dados que serão compartilhados por meio do bCPF se dá em face de criptografia e *hash's*, os quais asseguram que a informação armazenada permaneça imutável. Finck também aponta como métodos de garantia da segurança a criptografia, as chaves e as assinaturas que determinem a função e os limites de cada participante na *blockchain* (FINCK, 2018, p. 668). O Assessor de Diretoria da Dataprev afirma, ainda, que "apesar de ser elementos simples, a mecânica de cadeia de blocos e validações da rede garantem a integridade dos dados". A criptografia está diretamente ligada à noção de segredo, visto que apenas quem detenha de conhecimento acerca das chaves conseguirá ter acesso ao conteúdo decifrado. Para Bobbio, segredo é sinônimo de poder (BOBBIO, 2015, p. 47). Segundo estabelece Gomes, o segredo pode exprimir um valor democrático, dos pontos de vista utilitarista – para proteção do bem maior - e kantiano - privacidade, reserva e confidencialidade pendem de segredo e estão a cargo da liberdade (GOMES, 2018, p. 15).

Vivendo em uma sociedade informacional, comparada a máquinas de informática por Deleuze (1992), não há como olvidar a existência de eventuais riscos a ataques cibernéticos que ameaçam a segurança da rede e dos dados. Para tanto, em resposta ao questionamento sobre a importância do uso de certificação digital e restrição da faixa de endereços IP para a segurança

da rede, bem como de que forma poderia ser evitados ataques de *hackers*, o Assessor de Direção da Dataprev informou que

> O uso de tecnologias adicionais de segurança trazem uma camada adicional de segurança ao serviço, certificado digital é um exemplo disso. Já a restrição de faixas de IPs que podem acessar o serviço garantem que tráfegos de rede não legítimos são rejeitados antes de chegarem ao serviço propriamente dito. Com isso a resposta a um ataque DDos, por exemplo, se torna mais eficiente.

Conforme as informações apresentadas, podemos observar que a tecnologia *blockchain* possui mecanismos de garantia de segurança eficientes que podem mitigar eventuais ataques de entes maliciosos. Entretanto, no caso da rede não-permissionada ou pública, existem alguns riscos e muitas incertezas acerca das consequências de uso no setor público, visto que a escalabilidade pode resultar em um processo natural cada vez mais centralizador do poder computacional da rede (ATZORI, 2015, p. 16). Ainda, no caso da rede pública, a *blockchain* possui um alto grau de volatilidade, podendo ser bifurcada ou rejeitada pelos usuários a qualquer tempo (ATZORI, 2015, p. 16). Outra questão levantada por Atzori (2015, p. 17), é a dependência dessa rede pública na conectividade dos usuários, ou seja, caso a rede digital seja terminada ou os usuários migrem para outras redes, não há garantias de *backup* das informações. Esses são apenas alguns dos riscos técnicos que essa rede pode apresentar, visto que não há como precisar todas as possibilidades, ainda mais em virtude de se tratar de algo novo.

Todavia, não há como dizer que os riscos são os mesmo no que diz respeito à rede permissionada ou privada, visto que sua estrutura é diferenciada e, logicamente, mais restritiva tanto do ponto de vista subjetivo – em face dos sujeitos que a integram – quanto do ponto de vista objetivo – referente ao seu conteúdo. Portanto, há que se entender a escolha do modelo de rede do bCPF uma de suas maiores características, ainda mais em se tratando de conteúdo de base de dados pessoais, que são necessários para a gestão administrativa interna e a prestação dos serviços públicos e que exigem uma maior proteção por parte do Estado.

5.4 Da auditabilidade

O Auditor-fiscal da RFB aponta que o controle do bCPF é feito pela Receita Federal porque só ela escreve e isso se dá por conta da previsão no contrato inteligente. Ademais, o Assessor de Diretoria da Dataprev destaca que

> O bCPF por essência permite realizar a auditoria, pois na *blockchain* existe todas as transações de atualização da base CPF e essas transações são imutáveis. Assim se houver dúvidas quanto a integridade de uma informação basta que ela seja validada perante a *blockchain*.

Essa é uma característica fundamental da *blockchain* que a diferencia de outras tecnologias, visto que a auditoria é feita conjuntamente por meio do processo de validação dos blocos pelos integrantes da *blockchain*. Ainda que Bobbio entenda que não há democracia sem a opinião pública, do direito à informação acerca de decisões a serem tomadas de cunho coletivo e de exprimir críticas quanto a elas (BOBBIO, 2015, p. 41), a rede BC não vai de encontro à Democracia, podendo contribuir com ela na medida em que a auditoria dos processos decorrentes do bCPF conta com ferramentas eficientes e seguras, bem como tudo fica registrado na rede, não podendo o responsável malfeitor se eximir de responsabilidade.

A rede permissionada adotada pelo bCPF não assegura a transparência dos bancos de dados CPF, o que por si só já representa uma medida de segurança dos dados pessoais. Entretanto, não se pode dizer que não aumentou a transparência entre os órgãos da Administração Pública Federal, podendo contribuir para uma melhora e maior celeridade na prestação dos serviços públicos que dependem das informações contidas nesse banco de dados.

Acerca dos desafios decorrentes da implementação do bCPF, o Auditor-fiscal da RFB não vislumbrou nenhum, todavia serão revisitados alguns obstáculos mencionados em tópicos anteriores. Domingue (2018, p. 13-14) apresenta algumas barreiras à implementação da *blockchain* no setor público, são elas:

- Interdependência: pressupõe um sistema confiável e coordenado. No caso do bCPF, esse não seria um desafio, tendo em vista que a estrutura *blockchain* adotada já possui uma coordenação entre os participantes, bem como, em se tratando de rede permissionada, todos os membros são conhecidos, o que implica em uma noção de confiança. Além do mais, há registro de tudo na rede e processos de validação, o que também reforçam a confiança.
- Harmonização do legado: integração entre a nova tecnologia e os sistemas de legado existentes. No caso do setor governamental, a integração deve abarcar tanto de maneira técnica/operacional quanto a questão legal/jurídica. Não há informação suficiente para afirmar que esse não seria um desafio de implementação, visto que houve uma troca de modelo centralizado para paralelizado com a adoção do bCPF.

- Interoperabilidade técnica e maturidade: coordenação integrada entre as iniciativas *blockchain* ao redor do mundo. O projeto bCPF trata de base de dados pessoais, não podendo se encaixar nessa hipótese.
- Proteção de dados e privacidade: em se tratando da *blockchain* permissionada, os riscos de violação de direitos de privacidade e proteção de dados é quase nula.

Ainda, não se pode deixar de elencar como um desafio a resistência dos servidores frente às novas tecnologias, seja em razão de dificuldade cognitiva e de adaptação a novas tecnologias, seja porque não desejam alterar a maneira como exercem o serviço há tanto tempo. Ademais, conforme destaca Pedrosa (2019), a rotatividade dos gestores é um fator que implica em grande obstáculo aos projetos de cunho inovativos, já que dependem da boa vontade governamental para que tenham continuidade e, sendo o bCPF ainda um projeto-piloto, está ainda mais vulnerável a esse tipo de situação.

Notadamente, os desafios a serem enfrentados pelo bCPF ainda não são totalmente conhecidos, havendo mera especulação de possibilidades frente ao que se observa quando a Administração Pública implementa inovações em sua gestão. Sendo o bCPF um instrumento voltado somente à base de dados cadastrais e havendo o devido treinamento e incentivo a sua aplicação pelos servidores autorizados, poderão ser superadas essas barreiras.

6 Conclusão

Não é novidade que a Internet é a materialização da sociedade informacional, permitindo o compartilhamento de informações de forma aberta; em tese, não possui dono; e é desenvolvida de maneira colaborativa, se caracterizando em uma "teia de conexões" (SILVEIRA, 2017, p. 20 e 23-24). Esse desenvolvimento da sociedade também alterou as relações jurídicas e sociais, fazendo emergir uma nova forma de mercado, o de compra e venda de dados pessoais (SILVEIRA, 2017, p. 11).

Shoshana Zuboff (2013) correlaciona o Panóptico de Bentham com a era informacional, denominando-o de Panóptico da Informação, o qual possui três regras: necessidade de mecanização de tudo, necessidade de informatização de tudo e que toda aplicação digital que tiver como ser usada para vigilância e controle, a deverá ser, independente da razão da coleta. Ela verifica o surgimento de uma nova forma de economia a qual chama de "Capitalismo Distribuído", sendo o usuário o bem econômico. Nesse contexto, ela apresenta o "Capitalismo de Vigilância", segundo o qual, não apenas há a coleta arbitrária de dados, como também o uso de algoritmos para modular o comportamento dos usuários.

As sociedades disciplinares são meios de confinamento, representando o molde enquanto as sociedades de controle representam a modulação (DELEUZE, 1992, p. 221). A disciplina é forma de exercício de poder, sendo a vigilância enraizada socialmente e constante, na qual cada indivíduo é responsável por vigiar os próprios atos e os dos outros.

Ainda que entenda ser o segredo uma expressão de poder, Bobbio não defende que todos os atos devam ser públicos (BOBBIO, 2015, p. 47 e 62-63). O segredo, contudo, difere de mistérios, sendo o primeiro decorrente de tomada de decisão e passível de contestação e, o segundo, limitador da razão e da vontade (BOBBIO, 2015, p. 78).

Levando em consideração as evoluções tecnológicas, surge a tecnologia *Blockchain*, a qual representa um banco de dados distribuído e descentralizado, que se utiliza de uma estrutura *peer-to-peer*, isto é, sem a necessidade de um ente intermediário. Nesse sentido, destaca-se que "a tecnologia foi construída tendo em mente quatro principais características arquiteturais: segurança das operações, descentralização de armazenamento/computação, integridade de dados e imutabilidade de transações" (FILHO et al., 2017, p. 6).

Trata-se de uma inovação tecnológica bastante recente, logo, ainda não há instrumentos regulatórios específicos de *blockchain*, havendo, inclusive poucos estudos e

compreensão total sobre suas implicações. As pesquisas existentes ainda são meramente introdutórias. Todavia, a própria Administração Pública já vem desenvolvendo projetos que utilizam a tecnologia *blockchain*, como é o caso do bCPF, objeto de estudo da presente pesquisa.

O objetivo dessa pesquisa é verificar de que maneira o bCPF poderia assegurar a confiabilidade da proteção de dados no compartilhamento da base de CPF's por meio do levantamento de possíveis vantagens e desvantagens do uso da tecnologia *Blockchain* pela Administração Pública Federal, bem como pela revisão da literatura sobre os aspectos intrínsecos a tecnologia, proteção de dados e gestão pública. Para tanto, utilizou-se o método de pesquisa qualitativo, descritivo e exploratório, por meio da análise de documentos escritos, como obras literárias e artigos, bem como pela realização de duas entrevistas semi-estruturadas com representantes da Receita Federal e da Dataprev.

A tecnologia *blockchain* possui diversas vantagens do ponto de vista da garantia de eficiência e transparência dentro do setor público, por exemplo. Contudo, também possui barreiras a sua implementação. No caso do bCPF, verifica-se a possibilidade de obstaculização de implementação em face de resistência dos servidores à inovação e de rotatividade de gestores, por exemplo.

A *blockchain* possui diversos métodos que garantem a segurança das informações contidas nela, podendo representar, inclusive, uma solução à violação da proteção de dados pessoais, podendo mitigar a captura ostensiva e arbitrária dos mesmos. O fato de o bCPF ser uma rede permissionada, existir um contrato inteligente com as normas de funcionamento e não incluir empresas privadas no rol de participantes já são vantagens enormes desse projeto, visto que isso acaba por aumentar a confiança no serviço e garante uma proteção aos dados da base CPF tratados por ele.

O tema *blockchain* ainda é muito recente e pouco se sabe sobre. Logo, o estudo é meramente introdutório, tendo se limitado a compreender a adoção da tecnologia *blockchain* na gestão pública, cabendo aprofundamento e estudos futuros sobre o tema. Existem algumas iniciativas *blockchain* no setor público brasileiro já em vigor, contudo optou-se por um estudo inicial do bCPF em razão do objeto, que é o compartilhamento de dados pessoais.

REFERÊNCIAS

ARENDT, Hannah. **A condição humana**. Tradução de Roberto Raposo. 10. ed. Rio de Janeiro: Forense Universitária, 2005.

ATZORI, Marcella. **Blockchain Technology and Decentralized Governance: Is the State Still Necessary?** University College of London - Center for Blockchain Technologies. Dezembro de 2015. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713>. Acesso em: 28/06/2019.

BRASIL. **Decreto nº 9.690, de 23 de janeiro de 2019**. Altera o Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9690.htm>. Acesso em: 27/06/2019.

BRASIL. **Lei de Acesso à Informação nº 12.527, de 18 de novembro de 2011**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 29/09/2018.

BRASIL. **Lei Geral de Proteção de Dados Pessoais nº 13.709, de 14 de agosto de 2018**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 29/09/2018.

BRASIL. **Marco Civil da Internet nº 12.925, de 23 de abril de 2014**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 29/09/2018.

BARDIN, L. **Análise de Conteúdo**. Lisboa, Portugal; Edições 70, LDA, 2009.

BATTISTELLI, Juliana. **Os principais conceitos de back-end para começar a desenvolver para a web**. Blog Mastertech. 2017. Disponível em: <https://blog.mastertech.com.br/tecnologia/os-principais-conceitos-de-back-end-para-comecar-desenvolver-para-web/>. Acesso em: 11/07/2019.

BENTHAM. **Panóptico – Memorial sobre um Novo princípio Para Construir Casas de Inspeção e, principalmente, Prisões**. Rev. Bra. de Hist. v.07 n 14, Mar/Ago. 1987.

BERRYHILL, J., T. BOURGERY e A. Hanson, **Blockchains Unchained: Blockchain Technology and its Use in the Public Sector**, OECD Working Papers on Public Governance, nº 28, OECD Publishing, Paris, 2018.

BOBBIO, N. **Democracia & Segredo**. São Paulo: Editora Unesp, 2015.

BRAGA, Alexandre Melo. **TECNOLOGIA BLOCKCHAIN: Fundamentos, Tecnologias de Segurança e Desenvolvimento de Software**. Campinas: CPQD, 2017, p. 3. Disponível em: <https://www.cpqd.com.br/wp-content/uploads/2017/09/whitepaper_blockchain_fundamentos_tecnologias_de_seguranca_e_desenvolvimento_de_softwar_FINAL.pdf>. Acesso em: 11/06/2019.

BRITO, J. A. P. **Cibercidadania: a virtualização na Comunicação Pública contemporânea**. Revista Brasileira de Comunicação, Organização e Relações Públicas. São Paulo. Ano 3, n. 4, p. 107-123, jan-jul, 2006.

CACHAPUZ, Maria Cláudia**. Intimidade e vida privada no novo código civil brasileiro**: uma leitura orientada no discurso jurídico. Porto Alegra: Sergio Antonio Fabris Ed., 2006.

CANCELIER, Mikhail V. de L. **O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro**. Sequência (Florianópolis). Agosto de 2017, Páginas 213-240. Disponível em: <http://www.scielo.br/pdf/seq/n76/2177-7055-seq-76-00213.pdf>. Acesso em: 11/11/2018.

CHAHIN et. al. **E-Gov a próxima revolução brasileira: eficiência, qualidade e democracia: o governo eletrônico no Brasil e no mundo**. São Paulo: Prentice Hall, 2004.

Dataprev desenvolve solução com tecnologia Blockchain para compartilhamento da base CPF. Dataprev, 22/11/2018. Disponível em: <https://portal.dataprev.gov.br/dataprev-desenvolve-solucao-com-tecnologia-blockchain-para-compartilhamento-da-base-cpf>. Acesso em 28/05/2019.

DELEUZE, Gilles. **Post-scriptum sobre as sociedades de controle. In: Conversações: 1972-1990**. Tradução de Peter Pál Pelbart. Rio de Janeiro: Ed. 34, 1992.

DLA Piper. **Data Protection Laws of the World**. Disponível em: <https://www.dlapiperdataprotection.com/index.html?c=IL&c2=&t=definitions>. Acesso em: 10/11/2018.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006.

DUTRA, Deo Campos. **Método(s) em Direito Comparada**. Revista da Faculdade de Direito – UFPR, Curitiba, vol. 61, n. 3, set./dez. 2016, p. 189 – 212. Disponível em: <https://revistas.ufpr.br/direito/article/download/46620/29831>. Acesso em: 23/11/2018.

FILHO, José Reynaldo Formigoni; BRAGA, Alexandre Mello; LEAL, Rodrigo Lima Verde. **Tecnologia Blockchain: uma visão geral.** Campinas: CPQD, 2017, p. 3. Disponível em: < https://www.cpqd.com.br/wp-content/uploads/2017/03/cpqd-whitepaper-blockchain-impresso.pdf>. Acesso em: 13/06/2019.

FINCK, Michèle, **Blockchains: Regulating the Unknown.** German Law Journal, volume 19, nº 4, 2018.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**; tradução de Raquel Ramalhete. Petrópolis, Vozes, 1987. 288p.

GODOY, Arilda Schmidt. **Pesquisa Qualitativa Tipos Fundamentais**. Revista de Administração de Empresas, São Paulo, v. 35, n.3, p, 20-29, 1995.

HABERMAS, Jürgen. **Mudança estrutural da esfera pública**: investigações sobre uma categoria da sociedade burguesa. Tradução de Denilson Luís Werle. São Paulo: Editora Unesp, 2014.

IONITA, Anca Daniela; LITOIU, Marin; LEWIS, Grace. **Migrating Legacy Applications: Challenges in Service Oriented Architecture and Cloud Computing Environments**. USA, PA: IGI Publishing Hershey, 1 ed., 2012.

JALAKA, Parol. **Blockchain from Public Administration Perspective: Case of Estonia**. Estonia, Masters Thesis. Tallinn University of Technology, 2018. Disponível em: <https://digi.lib.ttu.ee/i/file.php?DLID=10173&t=1>. Acesso em 22/03/2019.

KLUMB, Rosangela; HOFFMAN, Micheline Gaia. **Inovação no Setor Público e Evolução Dos Modelos de Administração Pública: O Caso do TRE-SC**. Cadernos Gestão Pública e Cidadania, São Paulo, v. 21, n. 69, Maio/Ago. 2016.

KOCH, Per; HAUKNES, Johan. **Innovation in the Public Sector**. Publin Report n. D20. Oslo: NIFU STEP, 2005. Disponível em < http://www.aviana.com/step/publin/reports/d20-innovation.pdf> Acesso em 15/06/2019.

LUCENA, A. U.; HENRIQUES, M. A. A. **Estudo preliminar sobre o uso dos blockchains de Bitcoin, Litecoin, Ethereum e Namecoin em gestão de identidades**. In: XVI SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS. 16. 2016, Niterói. Anais eletrônicos... RJ: Sociedade Brasileira de Computação. Disponível em: <http://sbseg2016.ic.uff.br/pt/files/anais.pdf>. Acesso em: 23/04/2019.

LÜDKE, Menga; ANDRÉ, Marli E.D.A. **Pesquisa em educação: abordagens qualitativas**. São Paulo: EPU, 1986.

LYRA, João Guilherme. **Blockchain e Organizações Descentralizadas**. Rio de Janeiro: Brasport, 2019.

MARCONI, M., LAKATOS, E. M. **Técnicas de Pesquisa**. São Paulo: Atlas, 2006.

MARTINOVIC, Ivan. **Blockchains: Design Principles, Applications, and Case Studies**. Working Paper No.7 (DRAFT). Supporting material for the Training Session No. 5: Cyberspace, Politics, and Society. Oxford, 2017. Disponível em: <http://www.egov.ee/media/1374/martinovic-blockchains-design-principles-applications-and-case-studies.pdf>. Acesso em: 14/06/2019.

MARTINOVIC, Ivan, KELLO, Lucas e SLUGANOVIC, Ivo. **Blockchains For Governmental Services: Design Principles, Applications, And Case Studies.** Working Paper Series No. 7. Oxford: Centre for Technology and Global Affairs, 2017. Disponível em: <https://www.ctga.ox.ac.uk/sites/default/files/ctga/documents/media/wp7_martinovickellosluganovic.pdf>. Acesso em: 14/06/2019.

MOUGAYAR, William. **Blockchain para negócios: promessa, prática e aplicação da nova tecnologia da internet**. Rio de Janeiro: Alta Books, 2017.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em 12/05/2019.

PEDROSA, Tamires. **Os caminhos para a inovação no setor público**. Administradores.com, 2019. Disponível em: <https://administradores.com.br/artigos/os-caminhos-para-a-inovacao-no-setor-publico>. Acesso em: 15/06/2019.

Receita Federal publica norma sobre compartilhamento de dados utilizando tecnologia Blockchain. Receita Federal, publicado em 21/11/2018, com última alteração em 04/04/2019. Disponível em: <https://receita.economia.gov.br/noticias/ascom/2018/novembro/receita-federal-publica-norma-sobre-compartilhamento-de-dados-utilizando-tecnologia-blockchain>. Acesso em 28/05/2019.

RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

RUBINSTEIN, I. **Big Data: The End of Privacy or a New Beginning? International Data Privacy Law**, Volume 3, Issue 2, 1 May 2013, Pages 74–87. Disponível em: <https://doi.org/10.1093/idpl/ips036>. Acesso em: 29/09/2018.

SILVEIRA, Sérgio Amadeu da. **Tudo sobre tod@s**: redes digitais, privacidade e venda de dados pessoais. São Paulo: Edições Sesc São Paulo, 2017.

SILVA, Maria O. S. et al. **Pesquisa Avaliativa: aspectos teóricos-metodológicos**. São Paulo: Veras Editora, 2013.

UNIÃO EUROPEIA. **Diretiva 95/46/CE**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em: 09/10/2018.

UNIÃO EUROPEIA. **General Data Protection Regulation 2016/679 (GDPR).** Disponível em: <http://www.privacy-regulation.eu/pt/index.htm>. Acesso em: 09/10/2018.

VEIGA, Armando; RODRIGUES, Benjamin Silva. **A monitorização de dados pessoais de tráfego nas comunicações electrónicas**. Raízes Jurídicas, Curitiba, v. 3, n. 2, jul/dez, 2007. Páginas 59-110. Disponível em: <http://ojs.up.com.br/index.php/raizesjuridicas/article/viewFile/168/140>. Acesso em: 12/11/2018.

VERASZTO, E.V., SILVA, D., MIRANDA, N. A., SIMON, F. O. **Tecnologia: buscando uma definição para o conceito**. Revista PRISMA.COM, nº 7, 2008, p. 60-85. Disponível em: <http://revistas.ua.pt/index.php/prismacom/article/view/681/pdf>. Acesso em 12/05/2019.

YAGA, D., MELL, P., ROBY, N., e SCARFONE, K. **Blockchain Technology Overview.** NIST, U.S. Department of Commerce, 2018.

ZUBOFF, S. **THE SURVEILLANCE PARADIGM: Be the friction - Our Response to the New Lords of the Ring**. In: Frankfurter Allgemeine Zeitung, 2013. Disponível em: < https://www.faz.net/aktuell/feuilleton/the-surveillance-paradigm-be-the-friction-our-response-to-the-new-lords-of-the-ring-12241996.html>. Acesso em: 18/08/2018.

ZUBOFF, S. **Big Other: Surveillance Capitalism and the Prospects of an Information Civilization**. In: Journal of Information Technology. 30, 75-89, 2015.