Universidade do Minho
Escola de Direito

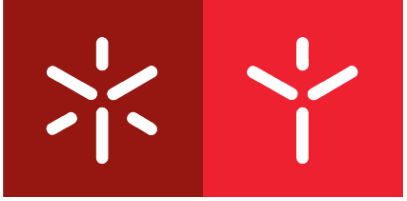
Lucas Silvestre Cortizo

A Blockchain à luz da Proteção de Dados na promoção de transparência contra a corrupção na Administração Pública

Novembro de 2020

A Blockchain à luz da Proteção de Dados na promoção de transparência contra a corrupção na Administração Pública
Lucas Silvestre Cortizo

UMinho | 2020



Universidade do Minho
Escola de Direito

Lucas Silvestre Cortizo

A *Blockchain* à luz da Proteção de Dados na promoção de transparência contra a corrupção na Administração Pública

Dissertação de Mestrado

Mestrado em Direito e Informática

Trabalho realizado sob a orientação dos Professores Doutores

Joana Covelo de Abreu

João Marco Cardoso da Silva

Novembro de 2020

Direitos de autor e condições de utilização do trabalho por terceiros

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos.

Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Licença concedida aos utilizadores deste trabalho

Atribuição-NãoComercial-SemDerivações
CC BY-NC-ND

https://creativecommons.org/licenses/by-nc-nd/4.0/

Universidade do Minho, Braga, 16 de Novembro de 2020.

Lucas Silvestre Cortizo

AGRADECIMENTOS

Primeiramente, e sempre, a Deus que é o centro da minha vida e é quem me ilumina cada dia para seguir os seus propósitos. Muitos são os desafios, principalmente por estar longe fisicamente da minha família, mas é através d'Ele que estou perto e jamais estarei sozinho.

À minha família que, desde o princípio, sempre fez o possível e impossível para que a educação fosse um dos meus alicerces. Agradecimento especial à minha mãe Dora, incansável em me ensinar que a educação é o bem mais valioso e minha maior inspiração para cursar este Mestrado; ao meu pai Fernando, pelo cuidado e apoio incondicional de sempre; aos meus avós, em especial Marizete e Espedito, que sempre investiram nos meus estudos e orgulhá-los é uma das minhas maiores alegrias; ao meu irmão Gabriel que sempre foi um companheiro e pudemos acompanhar o crescimento um do outro.

À minha namorada Mara que não cessou em me dar força e me apoiar em cada fase deste Mestrado, sendo ela a única testemunha do quão desafiador foi concluir esta dissertação e quantos finais de semana e noites passamos a trabalhar nas nossas respectivas teses.

Aos meus orientadores, Senhora Professora Joana Covelo de Abreu e Senhor Professor João Marco pela atenção e colaboração essenciais para o alcance dos objetivos propostos no presente trabalho, sem cuja orientação este trabalho não teria sido concluído.

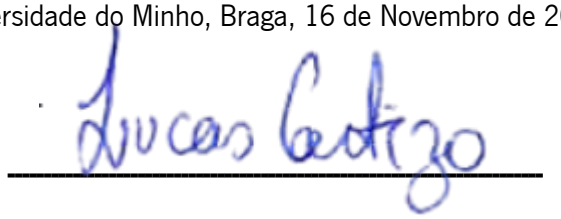
Aos meus colegas de trabalho da Comissão de Proteção de Dados de Malta, pelo imenso apoio e por sempre me envolverem nos debates da EDPB que vão resultar em diretrizes oficiais a nível europeu sobre a tecnologia *blockchain* à luz da proteção de dados pessoais, o que foi fundamental para meu auxílio neste trabalho.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

Universidade do Minho, Braga, 16 de Novembro de 2020.



Lucas Silvestre Cortizo

RESUMO

No contexto da sociedade da informação, cresce nos últimos anos a adoção das mais variadas soluções baseadas na tecnologia *blockchain.* Por ser uma tecnologia que promove registro e tratamento de dados de maneira descentralizada e distribuída, a presente dissertação averigua até que ponto a blockchain é juridicamente compatível com o arcabouço legislativo da proteção de dados – em especial, o Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

A partir das conclusões de quais modelos de *blockchain* apresentam características mais promissoras para uma eventual conformidade em relação ao direito fundamental à Proteção de dados, incluindo os princípios e diretos previstos no Regulamento (UE) 2016/679 que os usos desta tecnologia devem respeitar. A preocupação com atender as previsões normativas é enaltecida no contexto de oferecimento de soluções para a Administração Pública que deve obedecer ao princípio da legalidade. No contexto administrativo, são buscadas implementações práticas da *blockchain* sob o desígnio específico de utilizar esta tecnologia de registro para gerar mais transparência na Administração Pública, especialmente nas circunstâncias de combate à corrupção.

Palavras-chave: RGPD; Proteção de Dados; Blockchain; Tecnologia; Administração Pública; Transparência; Corrupção.

ABSTRACT

In the context of the information society, the adoption of the most varied solutions based on the blockchain technology has grown in recent years. As a technology that promotes the registration and processing of data in a decentralised and distributed manner, this thesis examines the extent to which blockchain is legally compatible with the legislative framework on data protection - in particular Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

From the findings of which blockchain models present the most promising features for possible compliance with the fundamental right of data protection, including which principles and data subject rights of such Regulation (EU) 2016/679 the uses of this technology must respect. The concern with meeting the regulatory requirements is foreseen by the specific context of providing solutions for Public Administration (which must comply with the principle of legality). In the administrative context, practical implementations of the blockchain are sought under the specific design of using this registration technology to generate more transparency in the Public Administration, especially in the circumstances of combating corruption.

Keywords: RGPD; Data Protection; Blockchain; Technology; Public Administration; Transparency; Corruption.

ÍNDICE

LISTA DE ACRÓNIMOS

Ab initio - Desde o princípio

ACBB - Anti-corruption blockchain backbone

Accountability – princípio da responsabilização

AEPD - Agencia Española de Protección de Datos

Apud.- Citado por

BID - Banco Interamericano de Desenvolvimento

CDFUE ou Carta - Carta dos Direitos Fundamentais da União Europeia

Cfe. - Conforme

Ciphertext – informação cifrada

Cleartext - informação em texto claro

CMI - Chr. Michelsen Institute (CMI

CNIL - Commission Nationale de l'Informatique et des Libertés, ou Autoridade de Controlo Francesa

Commit – comprometer

Commitment scheme - esquema de comprometimento

Corruption free – Isenta de corrupção

CRP - Constituição da República Portuguesa

Data vênia - com o devido respeito.

Design - Aspecto de um produto criado segundo certos critérios

Diretiva 95 - Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Double-entry bookkeeping - livro-razão das partidas dobradas , ou de entradas duplas

DPA - Autoridades de controlo

DPoS - Delegated-Proof-of-Stake

EDPB - Comité Europeu para a Proteção de Dados

e-residency – residência digital

Fork – subdivisão de cadeia

Guideline(s) – Diretriz(es)

Hash – operação informática de transformar aleatoriamente informação em um formato pré-definido. Resultado da operação é o hash digest.

Household exemption – Princípio de quando o tratamento de dados é exercido para atividades exclusivamente pessoais ou domésticas por pessoa singular

Ibid - latim ibidem, no mesmo lugar

ICO - Autoridade de Controlo do Reino Unido ou Information Commissioner's Office

Juris tantum – latim, diz-se da presunção legal que admite prova em contrário

KSI – blockchain desenvolvida pela Estônia

Lato sensu – latim, em sentido geral

Ledger - registro ou livro-razão

Membership - rede de relacionamentos aderidos

Mining – mineração, processo de validação (no contexto da blockchain)

n.º - número

NIIS - Nordic Institute for Interoperability Solutions

Node – nós

Nonce: número de utilização única

Offchain - armazenar dados em texto claro fora da blockchain

one-way hash – operação informática irreversível

Op. cit. – Obra citada

OSC - organização da sociedade civil

p. – Página

P2P - Peer-to-peer, rede ponto a ponto

Paper ou whitepaper – artigo técnico

Per si – latim, por si, de modo individual ou isolado.

Permissioned Blockchains - arquitetura permissionada, ou rede permissionada (que segue uma regulamentação de pré-seleção dos participantes)

Permissionless blockchain - blockchain não-permissionadas ou públicas

PKI - infraestrutura de chave pública

PoS - Proof-of-Stake

PoW - Proof-of-work

Privacy by design = proteção de dados desde a conceção

Res publica – coisa pública

Reveal – execução de revelar pelo receptor da mensagem

RGPD - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016

relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, ou o Regulamento.

Risk-based approach – abordagem de análise de risco

Scripts – lista de comandos que são executados por certo programa

Single point failure – falha de uma parte do sistema de informação

Smart contracts – comandos auto-executaveis baseados emu ma blockchain

Softwares – programas informáticos

Stakeholders – partes interessadas

Targeting – direcionamento

TFUE - Tratado sobre o Funcionamento da União Europeia

TFUE – Tratado sobre o Funcionamento da União Europeia

TI – tecnologia da informação

Timestamp - selo temporal

TJUE - Tribunal de Justiça da União Europeia, a Corte Europeia

TUE - Tratado da União Europeia

U4 - Grupo voltado ao desenvolvimento internacional contra a corrupção

UE - União Europeia

Ultima ratio – latim, o último recurso

Verifiers - entidades verificadoras

WEF - Fórum Econômico Mundial

World Wide Web – rede mundial de computadores

ZKP - zero-knowledge proof, ou prova de conhecimento zero

INTRODUÇÃO

O presente trabalho propõe-se analisar o arcabouço normativo referente à Proteção de dados pessoais como ponto de partida. De imediato, a Proteção de dados vai ser fruto de um longo processo que reflete uma evolução legislativa e uma maturação principiológica, elevando-a a preceito fundamental, de natureza universal, pertencente a todas as pessoas que se encontrem no âmbito territorial da moldura legislativa que a preveja. Para fins de melhor entendimento de todos os desdobramentos posteriores, é basilar estabelecer a relevância deste direito, sobretudo pela força da Carta dos Direitos Fundamentais da União Europeia (CDFUE), seja também pelo Tratado sobre o Funcionamento da União Europeia (TFUE), ou ainda pela Constituição da República Portuguesa a serem debatidos.

Não obstante, a evolução normativa deste primeiro momento precisa perceber o contexto de adoção e publicação do Regulamento geral sobre a proteção de dados (Reg. 679/2016, doravante RGPD ou Regulamento)[1]. Para fins de contextualização, já existia a Diretiva 95/46/CE, cuja vigência há décadas criava a importância do tema na União Europeia, entretanto restou esta Diretiva revogada pela adoção do RGPD.

O presente trabalho não se limita a pontuar estes dois marcos legislativos históricos, como um sendo o fim do outro. O objetivo é mostrar a Proteção de dados como um encadeamento de antecedentes jurisprudenciais e de diversas normas, a fim de evidenciar a matéria pela "pertinência, pelo grau de maturação e pela densificação dogmática e jurisprudencial"[2].

Para tanto, é necessário recorrer a uma sequência temporal de importantes institutos que ajudam na formação do ideal europeu que, por sua vez, deve ser cortejado com a conceção norte-americana, que há séculos desenvolve o princípio da privacidade. Diante desta comparação, entre Proteção de dados e privacidade, a natureza autônoma do primeiro indica um caminho para diferenciar os institutos e, sobretudo, elevar o RGPD a um patamar inédito. A evolução legislativa ocorre para aproximar a Proteção de dados, no contexto da UE, como sendo um dos pilares do atual Estado de Direito estabelecido (ou, no contexto jurídico-constitucional da União Europeia, do atual estado da União de Direito).

---

[1] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016

[2] Silveira, Alessandra; Marques, João. Do Direito a Estar só ao Direito ao Esquecimento. Considerações Sobre a Proteção de Dados Pessoais Informatizados no Direito da União Europeia: Sentido, Evolução E Reforma Legislativa. Revista da Faculdade de Direito – UFPR, Curitiba, vol. 61, n. 3, set./dez. 2016

O desafio deste trabalho não se resume a esta questão relativa ao papel do RGPD na construção de um Estado de Direito, uma vez que o tema central vai buscar desígnios práticos para entender, de forma materializada, o supracitado princípio da Proteção de dados em relação a alguma tecnologia (que dependa do tratamento de dados[3], na forma do RGPD). Tecnologias estas que possam potencialmente oferecer soluções a determinadas dificuldades. E o desígnio prático que vai analisado será o uso de soluções baseadas na *blockchain*[4] de forma a contribuir para um incremento da transparência e combate à corrupção na Administração Pública.

E diante deste ponto, é necessário fazer uma explicação detalhada da tecnologia *blockchain*. O presente trabalho sugere definições e detalhamentos sobre as possíveis características que acompanham as diversas formas que tal tecnologia pode assumir, bem como a forma como cada bloco está organizado e seus respectivos dados. Ainda é imperioso pensar se, e como, ocorre a validação e inserção de dados no registro, através de regras protocolares pré-estabelecidas, sem olvidar detalhes de possíveis caminhos de regulação da utilização da tecnologia associada à *blockchain*. Este último ponto é fundamental no debate que virá no capítulo posterior, a saber sobre a conformidade da *blockchain* em relação ao Regulamento.

Elementos trazidos nos dois primeiros capítulos vão ser resgatados e relacionados, numa perspectiva holística, no momento em que a *blockchain* for analisada à luz do RGPD. No escopo de averiguar adequação desta tecnologia, particularidades técnicas da *blockchain* vão ser um parâmetro do seu grau de flexibilidade, indicando até que ponto pode a Administração Pública adaptá-la para os fins almejados. O âmbito material do Regulamento deve ser trazido, junto às respectivas exceções, para justamente, através de particularidades da blockchain, se averiguar da possibilidade de uma solução baseada na cadeia de blocos poder implicar que o tratamento de dados extrapole a moldura de aplicação do RGPD. Uma suposição é tornar o RGPD inaplicável no caso concreto, nomeadamente partindo do exemplo das técnicas de cifragem e de pseudonimização a serem detalhadas ao longo da investigação.

Outrossim, sendo a normativa aplicável, cabe equacionar em que medida os direitos dos titulares, os princípios e a observância de, pelo menos, uma das bases legais do artigo 6 do RGPD

---

[3] Nos termos do RGPD: Tratamento de dados consiste na "operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição"

[4] Conforme será detalhado ao longo do trabalho, a *blockchain* é essencialmente uma base de dados distribuída ou um livro-razão descentralizado, onde vão ser inseridas todas as transações ou eventos a serem executados. A noção de distribuição decorre de que todos os participantes receberão uma cópia atualizada deste registro, e descentralização por via de regra, não possuir existir uma entidade centralizadora.

podem ser observados. Para fins de legalidade de soluções baseadas na *blockchain*, em especial as revestidas de interesse público, a presente investigação dispõe-se a analisar e propor soluções para quando algum princípio ou direito dos titulares suscitar alguma incompatibilidade aparente perante os atuais modelos pensados para a *blockchain*. E havendo este direcionamento, as bases teóricas do presente estudo restam interseccionadas, tendo em conta que o paradigma prático do trabalho é a adoção da tecnologia *blockchain* pela Administração Pública, a qual deve deferência ao interesse público, mas mormente ao princípio da legalidade (o que abrange a obediência ao RGPD).

Ante o exposto, deve-se partir de premissas básicas que norteiam a evolução do pensamento e interligam os principais institutos do trabalho. O tratamento de dados deve observar o preceito fundamental trazido pelo RGPD, e também, os demais atos normativos de caráter supranacional. Se o tratamento de dados ocorre através de uma rede *blockchain*, o dever de observância existe (caso o âmbito de aplicação do RGPD não for afastado). Em se tratando de um tratamento de dados no seio da Administração Pública, a lógica permanece e o descumprimento tem efeitos na própria dinâmica do Estado[5].

Por fim, após certificar se a *blockchain* pode oferecer conformidade com toda esta estrutura normativa que protege o Direito fundamental à proteção de dados, é imperioso materializar a discussão para perceber como ocorre, na prática, a adoção e implementação da *blockchain* pela Administração Pública sob o desígnio específico de utilizar esta tecnologia para gerar mais transparência administrativa. Este instituto basilar do presente estudo tange os demais, ao passo que a adulteração de registros públicos deve ser um dos escopos na implementação governamental da tecnologia *blockchain*.

Portanto, o presente objetivo é averiguar até que ponto a *blockchain* é juridicamente compatível com o arcabouço legislativo da proteção de dados, para a partir de uma eventual conformidade, esta tecnologia ser analisada em casos concretos, no desígnio específico da Administração Pública. No contexto administrativo, para evitar um âmbito de pesquisa excessivamente largo, o foco deste estudo é buscar implementações práticas da *blockchain* que objetivem trazer mais transparência à Administração Pública, especialmente nas circunstâncias de combate à corrupção.

[5] Sobre a formação do Estado de Direito, veja-se Motta, Fabricio. Função normativa da administração pública, Editora Fórum, 2007.

CAPÍTULO I

1.1. Da Proteção De Dados Pessoais Como Direito Fundamental Reconhecido

Primeiramente, cumpre trazer os fundamentos e a teleologia inerentes ao RGPD. Esta norma é referência para o objeto de estudo, afinal representa um ditame à nível da União Europeia para ponderar a aplicação concomitante de certos princípios fundamentais, que no seio das relações que envolvem os dados pessoais, mostram-se relevantes a saber a Proteção de dados cumulada com a livre circulação de dados pessoais e ainda o interesse público.

A Proteção de dados vem prevista expressamente no artigo 8, nº 1, da Carta dos Direitos Fundamentais da União Europeia (CDFUE), e comentada na obra de SILVEIRA et al[6], cuja previsões não apenas determinam que é algo de natureza universal, de "todas as pessoas", mas também já adianta conceitos que vão ser basilares quando se falar em tratamento para fins específicos, as formas de obter uma base legal para o tratamento (sobretudo, o consentimento livre e específico do titular dos dados), sem prejuízo de anunciar que a fiscalização deverá ocorrer através de uma autoridade de controle independente.

Sobre esses termos, é importante trazer o artigo 8, nº 1, da CDFUE *ipisis litteris*: "Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente"[7].

Desde início, cumpre enaltecer o valor jurídico da CDFUE. No art. 6º, nº1, do Tratado da União Europeia (TUE) está atribuída força jurídica plena à Carta. Segundo CANOTILHO et al, a atribuição de força jurídica plena à CDFUE "soluciona o problema do valor jurídico das normas da Carta, sendo estas, a partir da entrada em vigor do Tratado de Lisboa, inequivocamente válidas e eficazes"[8]. Cria-se, segundo os autores, um catálogo próprio de direitos fundamentais "vinculativos para todos os órgãos e para as Instituições da UE, bem como para os EM, quando apliquem direito da União"[9]. É levantado

[6] Castro, Catarina Sarmento e. Comentário ao artigo 8.º. In: Silveira, Alessandra e Mariana Canotilho (Coord.). "Carta dos Direitos Fundamentais da União Europeia Comentada". Coimbra: Almedina, 2013.

[7] Europeia, União. "Carta dos Direitos Fundamentais da União Europeia (2010/c 83/02)". Diário oficial da União Europeia 30 (2010). Disponível em https://www.europarl.europa.eu/charter/pdf/text_pt.pdf Acesso em 19/02/2020

[8] Canotilho, José Joaquim Gomes e Mariana Canotilho. Comentário ao artigo 6º do Tratado da União Europeia in: Lopes Porto, Manuel e Gonçalo Anastácio. "Tratado de Lisboa, Anotado e Comentado" Coimbra: Almedina. 2012. P. 40/45

[9] Ibid.

ainda por CANOTILHO *et al* que, ao contrário da subordinação da União à CDFUE (que é inequívoca), os Estados-Membros devem observar os princípios da Carta por resultado jurisprudencial do Tribunal de Justiça da União Europeia (TJUE) que impõe uma vinculação alargada dos Estados em relação ao parâmetro de jusfundamentalidade provenientes da União.

Desta forma, o TJUE assumiu um "compromisso inequívoco"[10] com os direitos fundamentais no âmbito dos Estados-Membros, o que não se fez necessário a nível da União pelo caráter vinculativo da CDFUE. De qualquer forma, o padrão de jusfundamentalidade – sob o qual a Proteção de dados está inserida por força do artigo 8, nº 1, da CDFUE – foi previsto no artigo 6º, nº1, do Tratado da União Europeia e deve ser aplicado.

Ao trazer o padrão vinculativo e grau de importância da Proteção de dados e os demais direitos fundamentais em relação à UE, é importante detalhar esta evolução conceitual. Segundo SOUSA, mesmo antes do TUE o respeito pelos direitos fundamentais já era um mandamento da Constituição material da União. Entretanto, o Tratado "conseguiu elevar ainda mais o grau daquele respeito no acervo substantivo da Ordem Jurídica da União. De facto, o respeito pelos direitos fundamentais é erguido a valor em que se funda a União di-lo o já nosso conhecido artigo 2.° UE"[11]. Segundo o autor, esta evolução é obtida quer pela referência expressa ao respeito pelos direitos fundamentais, quer através da referência a outros valores. E é por isso que o respeito pelos direitos fundamentais, no contexto da UE, "tem de ser visto como um corolário"[12], incluindo a Proteção de dados e os demais princípios como respeito pela dignidade humana, a liberdade, o Estado de Direito, a justiça, dentre outros.

Sob a perspectiva da União, portanto, a jusfundamentalidade estabelece valores basilares. Mas, no âmbito dos Estados-Membros, ela também deve ser observada. No mesmo sentido da força vinculativa da CDFUE acima, SOUSA defende que os direitos fundamentais "não são apenas valores da União, são 'valores comuns' a todos os Estados-membros. Isto quer dizer que o respeito pelos direitos fundamentais (...) atinge o superior alcance ontológico dos valores que constituem o primeiro fundamento da União"[13]. E é inserido neste contexto que o valor jurídico da CDFUE merece ser percebido.

Cumpre reiterar o valor jurídico da CDFUE porque uma vez que a Proteção de dados está prevista no artigo 8, nº 1 da Carta, é importante vislumbrar este direito fundamental como originário da

[10] Ibid.
[11] Sousa, Domingos Pereira de. "Direito da União Europeia". Coimbra: Quid Juris. 2018. P. 189
[12] Ibid.
[13] Ibid

União e de força vinculativa. SOUSA[14] atenta a duas indagações possíveis a respeito do valor da Carta: (i) a CDFUE é um ato jurídico ou uma mera declaração política? (ii) a CDFUE obriga ou constitui um texto meramente facultativo? O autor afirma que ambas as questões foram resolvidas com a entrada em vigor do Tratado de Lisboa[15], passando a CDFUE a ter a força de um tratado internacional e a ser um acordo de natureza jurídica. Portanto, a Carta vincula nos mesmos moldes em que o TUE e TFUE vinculam, e por isso, a Proteção de dados assume o pressuposto de ser um direito fundamental por força do supramencionado artigo 8, nº 1 CDFUE.

Adicionalmente, o Tratado de Funcionamento da União Europeia (TFUE) também provisiona a Proteção de dados no artigo 16, pondo de lado qualquer dicotomia que possa ser aventada, que os dados pessoais estão sob proteção, mas que para o funcionamento da União Europeia é assegurada a livre circulação dos mesmos. Fica expressa a opção legislativa em trazer esses dois princípios no mesmo artigo, os quais são trazidos a seguir: "1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito; 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.o do Tratado da União Europeia".[16]

Nos comentários de GALVÃO *et al*, o artigo 16 TFUE estabelece pela primeira vez uma base jurídica expressamente aplicável ao tratamento de dados pessoais pelos Estados-Membros[17]. Segundo este autor, ao integrar o princípio da Proteção de dados nas "Disposições de aplicação geral" do Tratado, o legislador fez com que este princípio transcendesse "muito a mera dimensão económica do mercado interno"[18]. Não obstante, ainda é feita na obra uma relação entre o artigo 16º TFUE com a supramencionada CDFUE que consagra também o direito autônomo à Proteção de dados em seu artigo 8º. Ao mencionarem o artigo 8º da Carta, GALVÃO *et al* ainda fazem uma menção de que a

[14] Ibid

[15] Mesmo antes do Tratado de Lisboa, a força vinculativa da CDFUE já poderia ser interpretada à luz da prática da União e da jurisprudência constitucional dos próprios Estados-membros. Para aprofundar sobre, veja-se em Priollaud, François-Xavier, and David Siritzky. Le traité de Lisbonne: Commentaire, article par article, des nouveaux traités européens (TUE et TFUE). La documentation française, 2008.

[16] Tratado da União Europeia e do Tratado sobre o Funcionamento da União Europeia 2012/C. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:12012E/TXT&from=ES Acesso 19/02/2020

[17] Galvão, Luis Neto. Comentário ao artigo 16º do Tratado de Funcionamento da União Europeia in: Lopes Porto, Manuel e Gonçalo Anástácio. "Tratado de Lisboa, Anotado e Comentado" Coimbra: Almedina. 2012. Kindle Posição 5110.

[18] Ibid. Kindle Posição 5121.

CDFUE "passou a ter força vinculativa idêntica à dos tratados"[19] em virtude do artigo 6º do TUE, conforme explicado anteriormente.

Ante o exposto, já se consegue vislumbrar o quadro normativo sobre a Proteção de dados como um princípio vinculativo na UE, mesmo anterior ao RGPD, cujos termos elevam o assunto ao nível de direito fundamental reconhecido. Além desta noção basilar, o TFUE[20] declarou expressamente que esta proteção não deve coibir o livre fluxo do seu objeto protegido, por haver também assegurado o princípio da Livre circulação dos dados.

A indispensabilidade da livre circulação de dados foi bem anotada por SILVEIRA e FROUFE, em que seus termos: "A razão é simples: a livre circulação de dados é indispensável para o desenvolvimento da chamada economia digital. As soluções tecnológicas que permitem a utilização mais inteligente de recursos como energia e água, a redução de pesticidas na agricultura, a competitividade da indústria transformadora, bem como a redução de acidentes nas estradas, tudo depende do processamento de dados"[21].

Dito isto, merece destacar uma das ordens constitucionais que foi pioneira no que concerne a Proteção de dados, a saber o Estado-Membro português e a previsão no artigo 35 de sua Constituição.

1.2. Da Constituição Portuguesa

Não obstante o enquadramento transnacional, a Constituição da República Portuguesa (CRP) serve de paradigma no quesito da Proteção de dados ao ter sido uma das vanguardas neste assunto. A Carta Magna portuguesa, em seu artigo 35, foi uma das primeiras a tratar da chamada Autodeterminação informativa, pelo qual traz-se em seus termos: "Artigo 35: Utilização da informática; 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.; 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.; 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular,

[19] Ibid.
[20] Sobre este propósito: Silveira, Alessandra. Princípios de direito da União Europeia: doutrina e jurisprudência. Coimbra: Quid Juris, 2011.
[21] Silveira, Alessandra e Froufe, Pedro. Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos. UNIO - EU Law Journal. Vol. 4, No. 2, Julho 2018, p. 5.

autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.; 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.; 5. É proibida a atribuição de um número nacional único aos cidadãos.; 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.; 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei".[22]

No artigo 35, n.º 1, ressalta-se aquilo que vai ser transposto no entendimento do próprio RGPD, que este Direito a Proteção de dados vai além de apenas prever mecanismos de alteração de dados incorretos ou atualizar bases de dados. A Constituição portuguesa já mostrou entender que o mencionado direito pressupõe um poder por parte do titular dos dados, que possui o "direito de conhecer a finalidade" do tratamento de suas informações.

O artigo 35, n.º 3 é também um precursor da categoria especial de dados pessoais do artigo 9 do RGPD, denominados dados sensíveis e a sua consequente particular proteção. Na Carta Magna portuguesa, o tratamento sobre esta espécie de dados, apenas poderá ocorrer em três hipóteses: sob o consentimento expresso e mediante autorização legal (duas das bases legais previstas no Regulamento). E também traz uma permissão de tratamento para "dados estatísticos não individualmente identificáveis", o que não parece estar expressa nas hipóteses de base legal para tratamento de dados sensíveis do artigo 9 do RGPD, mas sim, prevista como circunstância fora do âmbito material do Regulamento.

Na realidade, o tratamento para fins estatísticos de dados anonimizados vem explicado no Considerando 26 do RGPD. O conceito desenvolvido retira a aplicação dos princípios, o que se entende pela retirada da aplicação do próprio Regulamento, sobre as chamadas informações anônimas. A partir do momento em que o dado for anonimizado, deixa de cumprir a definição do artigo 4, n.º 1 do RGPD que declarou o conceito de dado pessoal e, desta forma, a terceira hipótese de tratamento lícito de dado sensível (prevista na CRP) acaba por falar de uma hipótese onde não existe dado relacionado a pessoa individual, por definição do RGPD.

As noções de anonimização e âmbito material do RGPD serão importantes para os próximos capítulos em que os limites da Proteção de dados vão ser o parâmetro para determinar a conformidade

[22] Portugal. Constituição da República Portuguesa. Disponível em https://www.parlamento.pt/Legislacao/paginas/constituicaorepublicaportuguesa.aspx Acesso em 19 de fevereiro de 2020

da tecnologia *blockchain* com tal norma, afinal mesmo que exista um possível tratamento de dados pessoais, a investigação não se limita ao conceito e ir atrás das outras condições que dizem respeito à aplicabilidade do Regulamento.

Por ora, cumpre afirmar que, apesar de técnicas legislativas diferentes, existe uma similaridade conceitual entre a Carta Magna portuguesa e o Regulamento europeu, podendo citar como exemplo o n.º 7 do artigo 35 que estende a proteção seja para dados pessoais em formato de ficheiro físico ou eletrônico. Não obstante, o n.º 6 do artigo 35 da CRP lista de maneira expressa a questão que vem sendo trazida sobre a dialética dos dois princípios supramencionados, ao horizontalmente permitir os "fluxos de dados transfronteiras", mas com a preocupação da adequada Proteção de dados pessoais.

Em continuidade ao artigo 35 da CRP, há a previsão acerca de um número nacional único que por sua vez, se encontra inserido no contexto da Proteção de dados por, além de representar um cenário histórico, significa uma faceta do Direito da Privacidade que é mais abrangente, porém contorna os dados pessoais. A proibição constitucional do número nacional único remete a um projeto de um registro individual do cidadão[23] através da Lei n.º 2/73 que teve sua execução suspensa pelo I Governo Provisório de 1974, ocasionando posterior vedação constitucional.

O perigo mais apontado pelos estudos[24] seria que a instituição de uma chave única de acesso significaria o acesso simultâneo a vários ficheiros que, em conjunto e interrelacionados, reconstituiriam um perfil do indivíduo. A proibição ocorre diante de um contexto histórico[25] em que governos que não respeitem os direitos fundamentais e podem deter significativo poder sobre seus governados.

Em outras palavras, desenvolvido o Registo Nacional de Identificação, através da Lei n.º 2/73, a opção por posteriormente proibir tal unificador foi em nome da preservação dos direitos fundamentais. Sob o prisma de proteger privacidade e liberdades públicas do cidadão, o constituinte português adotou uma postura contemporânea de que os dados pessoais não são um 'bem' da Administração Pública, sem que ela possa dispor ao seu juízo e sem base legal para tanto[26]. Nota-se acima que existe uma tendência a aproximar a Proteção de dados ao direito da Privacidade.

---

[23] Canotilho, José Joaquim Gomes et al. "Constituição da República Portuguesa Anotada", Volume I, 4.º Edição, Coimbra: Editora Coimbra, 2007. p. 556.

[24] Castro, Catarina Sarmento. 40 anos de 'Utilização da Informática': O artigo 35. º da Constituição da República Portuguesa. e-Pública: Revista Eletrónica de Direito Público, vol. 3, n. 3, 2016, p. 84-99.

[25] Castro, Catarina Sarmento. Ibid.

[26] Ferreira, Rafael Freire. "Desafios em sede de tutela da personalidade: a autodeterminação informativa e a privacidade na sociedade da informação". Lisboa: Universidade Autónoma de Lisboa, Tese de Doutorado, 2016.

1.3. A Privacidade Norte-americana

No momento, é relevante trazer o entendimento de que a noção de privacidade norte-americana não constitui direito autônomo[27], diferente da ótica europeia, a qual - conforme já foi demonstrado - traz um direito autônomo, seja à nível nacional português consoante o artigo 35 da CRP, seja no nível europeu conforme a CDFUE e TFUE. As bases da privacidade não são novas, para as quais se atribui a autoria de WARREN e BRANDEIS[28].

Os autores ressaltaram que o mercado de notícias estava desenvolvendo-se de forma muito rápida e repararam que as atuações jornalísticas estavam cada vez mais invasivas, o que representava uma violação do direito de intimidade. Deste paradigma, a obra partiu da doutrina do juiz THOMAS COOLEY que, em 1888, na obra *A Treatise on the Law of Tort sor the Wrongs Which Arise Independent of Contract*, cunhou o chamado "*right to be let alone*" ou direito de estar sozinho[29].

E a partir desta noção de construção doutrinária, os autores do "*Right to Privacy"* examinaram, em sua obra, diversos antecedentes jurisprudenciais para entender qual era, de fato, a motivação para a ausência de um direito à privacidade. De uma análise detalhada da jurisprudência norte-americana - considerando, por certo, o período histórico - esses juristas notaram que o "direito à propriedade era capaz de proteger manuscritos e obras de arte, essencialmente por conta da sua natureza. No entanto, o mesmo não era suficiente quando o ponto em questão fossem bens imateriais, tais como a paz de espírito e a possibilidade de proibição de publicação de fatos ou informações indesejadas que dissessem respeito tão somente à própria pessoa"[30].

Neste sentido, surgiu o entendimento que a privacidade decorre da própria pessoa e a doutrina americana passou a seguir esse marco histórico que é a obra de WARREN e BRANDEIS[31]. O direito à Proteção de dados, para o sistema americano, acaba por indicar algo que inexiste por si só, mas decorre da privacidade. Conforme se depreende da doutrina de MILLS[32], cuja contribuição é tratar a proteção da informação pessoal como uma esfera da privacidade, cujo conceito de *"The Personal-*

---

[27] Ruaro, Regina Linden. "A tensão entre o Direito Fundamental à proteção de dados pessoais e o livre mercado". Brasília: Repats, v. 4, 2017, p. 389-423

[28] Warren, Samuel D. Brandes, Louis D. The Right to Privacy. In: Harvard Law Review, v. 4, n. 5, Dec. 15, 1890, p. 193-220. Disponível em: <http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>. Acesso em: 19 de fevereiro de 2020.

[29] Ruaro, Regina Linden. Ibid.

[30] Ruaro, Regina Linden. Ibid. p. 7.

[31] Warren, Samuel D. Brandes, Louis D. The Right to Privacy. Ibid.

[32] Privacy: the lost right. New York: Oxford University Press, 2008. Rabelo, Iglesias Fernanda de Azevedo e Garcia, Filipe Rodrigues. O direito à autodeterminação informativa. Disponível em <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10473>. Acesso em: 19/02/2020

Information Sphere: Protecting Personal Data" traz essa noção da Proteção de dados pessoais enquanto uma derivação da privacidade.

O contexto europeu, conforme foi exposto, acaba por tratar a Proteção de dados como direito autônomo e não uma esfera (apesar de que, em diversas circunstâncias, seja possível identificar pontos em comum entre esses dois conceitos). A separação do contexto europeu parece evidente quando se fala em sigilo da informação pessoal. Se a Proteção de dados for entendida como derivada da privacidade e, por sua vez, a privacidade for voltada para a vida privada e opção de sigilo da informação, o descumprimento de um direito, acarretaria o dos demais, a exemplo da clássica lição do autor RICHARD POSNER que define a privacidade como uma "forma de omitir informações acerca de si, as quais podem ser usadas por terceiros em seu prejuízo"[33]. O problema deste conceito é seu caráter limitante. Ao traçar uma linha, qual seja o sigilo, a partir do momento que este limite é ultrapassado, pressupõe o fim do próprio direito.

Exemplificando, se a privacidade for sigilo de informação pessoal, caso ocorra uma divulgação ou ao acesso não autorizados (no formato do artigo 32, n.º 2 do RGPD), a Proteção de dados encerraria nesta violação, e qualquer uso do dado pessoal divulgado estaria além da conceção da privacidade. Ou ainda, na ótica inversa, só haveria ofensa à privacidade e Proteção de dados caso houvesse acesso não autorizado ou divulgação ilícita, o que não corresponde ao modelo e à conceção adotados pelo RGPD. Por isso que soa ultrapassado na doutrina europeia falar que há ainda uma pequena tentação de caracterizar o sigilo como direito de privacidade[34].

Esta visão é bastante elucidada pelo autor SOLOVE ao explicar o problema de tratar sigilo como privacidade, pois retiraria de toda informação não mais sigilosa a proteção jurídica. Em seus termos: "Em diversos contextos legais, a visao da privacidade com sigilo normalmente leva a conclusão de que uma vez que o fato for publicamente divulgado – não importa o quão limitado ou estreito seja esta divulgação – este fato não pode mais ser considerado privado"[35].

A visão americana da privacidade é reflexo inclusive da jurisprudência da "*Fourth Amendment*" da Suprema Corte dos Estados Unidos que sustenta a ideia de que se uma questão apresenta completa ausência de sigilo, ela deixa de ser privada. O próprio WILLIAM STUNTZ[36] analisa que, de acordo com esta quarta emenda, a privacidade decorre do interesse em guardar segredos, todavia acaba por deixar de lado questões fundamentais como a atuação policial desarrazoada ou outras

[33] Posner, Richard A. "The economics of justice", Cambridge Massachusetts: Harvard University Press, v. 5, 1983, p. 271. (Tradução livre)
[34] Thompson, Paul B. "Privacy, secrecy and security", Ethics and Information Technology 3.1, 2001, pp. 13-19.
[35] Solove, Daniel J. "Understanding privacy", Massachusetts: Harvard University Press, 2010. pp. 22–23. (Tradução livre)
[36] William J. Stuntz, "Privacy's Problem and the Law of Criminal Procedure," 93 Michigan Law Review, 1995, pp. 1016-1022

questões que envolvam a dignidade da pessoa humana, a exemplo da devassa de informações pessoais (mesmo que públicas) por parte do Estado.

Caso seja adotado um conceito limitante para a privacidade, a tendência será, além de causar uma impressão de que ela não mais existe, relativizar e enfraquecer a própria proteção jurídica. Conforme SOLOVE[37], a doutrina da privacidade traz diversos tipos de visão, seja a do filósofo THOMAS NAGEL que, há duas décadas, já alertava para a "desastrosa erosão da preciosa, porém frágil"[38] privacidade. Doutro lado, visões mais radicais acompanham a doutrina há anos com opiniões terminativas. Vários livros e artigos trazem termos como destruição, morte e fim da privacidade, podendo citar NELSON que entendeu que a privacidade não apenas está morta, como está morrendo repetidamente[39].

Dependendo do ponto de vista, a mencionada crise da privacidade pode ser maior ou menor. E conforme foi visto, a visão limitante do direito à privacidade poderá conduzir a uma interpretação de inexistência do próprio direito, e por conseguinte, afetar o direito à proteção de dados.

Apesar de se pregar o contrário, a privacidade ainda existe por ser amplamente reconhecida por normas em vigência e, por isso, precisa ser aplicada. Uma das primeiras tutelas internacionais foi assumida através da Declaração Americana dos Direitos e Deveres do Homem de 1948 que determinava que toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar[40]. Logo em seguida, foi aprovada a Declaração Universal dos Direitos do Homem que, no seu artigo 12, propugnou a proteção da privacidade.

1.4. Proteção de dados no contexto europeu

Diante deste cenário, é válido equacionar o contexto jurídico da União Europeia que, de forma particularizada, passou a tratar a Proteção de dados em separado da privacidade e a buscar efetivar tal direito fundamental universal e autônomo através de padrões próprios.

No entanto, vale mencionar, nessa moldura e a título prévio, a Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais de 1950[41], que, em seu artigo 6, fala no direito à

[37] Solove, Daniel J. "Understanding privacy". Ibid, pp. 22–23.
[38] Nagel, Thomas. "The Shredding of Public Privacy" Times Literary Supplement, 1998, p. 95. Tradução livre
[39] Nelson, Deborah. "Pursuing Privacy in Cold War America xii-xiii". Nova York: Columbia University Press, 2002. Tradução livre
[40] Organização Dos Estados Americanos. Declaração Americana dos Direitos e Deveres do Homem de abril de 1948. Disponível em https://www.cidh.oas.org/basicos/portugues/b.Declaracao_Americana.htm Acesso em 19/02/2020
[41] Europa. Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais de 1950. Roma, 4.11.1950. Disponivel em https://www.echr.coe.int/Documents/Convention_POR.pdf Acesso em 27/02/2020

intimidade e vida privada. Na década seguinte, no ano de 1968, foi elaborada a Recomendação 509 da Assembleia Consultiva do Conselho da Europa, cujo destaque foi dado aos direitos da personalidade, e trazendo de forma inovadora questões acerca da vida privada em relação às interceptações telefônicas e à captura de imagens sem autorização, com um debate que se mantém até os dias atuais sobre os limites entre autonomia privada e interesse público[42] (todavia, agora com a mesma essência, voltada às novas tecnologias, a exemplo do reconhecimento facial).

Duas décadas depois, desenvolve-se a ideia jusfundamental inerente à autodeterminação informativa por parte do Tribunal Constitucional Federal alemão na decisão BVerfGE 65, 1130 – *Volkszählung* (Censo), através da qual foi declarada parcialmente inconstitucional, em 15 de dezembro de 1983, a Lei do Censo daquele mesmo ano[43]. Resumidamente, a lei obrigava a população a responder a perguntas censitárias para fins estatísticos e para alimentar um banco de dados governamental, onde foi invocado o direito fundamental de se autodeterminar sobre a liberação e uso dos próprios dados pessoais.

Este caso concreto consegue ser relacionado justamente com as exceções do artigo 35 da CRP para a autodeterminação informativa, uma vez que seria para fins de estatísticas, desde que seja garantida a anonimização, nos termos legais. No precedente alemão, perante o conflito entre fim estatístico e autodeterminação, foi proferido entendimento que a lei do censo era compatível com a dignidade da pessoa humana, porém não poderia ser exercida sem garantir a autodeterminação da informação. Percebe-se que o direito à autodeterminação informativa (*Recht auf Informationelle Selbstbestimmung*) foi reconhecido e elevado ao justo status constitucional[44].

A decisão alemã é um marco na privacidade europeia, e ainda toca no quesito do anonimato, separando-o do direito à privacidade. Isto significou uma ampliação do conceito da privacidade, um aumento de dimensão que influenciou a formação da cultura da privacidade na Europa até os dias atuais, compatibilizando a autodeterminação informativa para ser considerada um direito constitucional. Portanto, nas palavras de PINHEIRO: "a ampliação do conceito de privacidade ultrapassa o conceito de intimidade, abrangendo a pessoa inserida nas comunicações verbais ou não, que pode se traduzir em informações pessoais (individuais), não necessariamente secretas" [45].

---

[42] Dotti, René Ariel. "Proteção da vida privada e liberdade de informação: possibilidade e limites". São Paulo: Revistas dos Tribunais, 1980. p. 183

[43] Pinheiro, José Alexandre Guimarães de Sousa. Tribunal Constitucional Federal Alemão: decisão constitucional BVerfGE 65, 1. Disponível em http://www.servat.unibe.ch/dfr/bv065001.html#Opinion Acesso em 19/02/2020.

[44] Ferreira, Rafael Freire. Ibid.

[45] Pinheiro, José Alexandre Guimarães de Sousa. "A vida na sociedade de vigilância: privacidade hoje". Rio de Janeiro: Renovar, 2008. p. 94.

Em outras palavras, a decisão dos Censos de 1983 supracitada lançou as bases da teoria da autodeterminação informativa[46] pois, na sua decisão, a Corte Constitucional foi traçando um marco referencial para a proteção dos dados pessoais, como direito autônomo aos direitos de personalidade, o que foi seguido pela Carta Magna portuguesa, bem como pelas normas europeias subsequentes.

Por conseguinte, cabe, equacionar o caminho jusconstitucional e normativo trilhado pela ordem jurídica da União Europeia, a compreender de que forma a proteção internacional de direitos humanos (como resulta da Convenção Europeia dos Direitos Humanos) e a proteção de direitos fundamentais decorrente das tradições constitucionais comuns aos Estados-Membros promoveram a construção do direito à proteção de dados neste ordenamento jurídico.

Na realidade, reitera-se a previsão do já mencionado artigo 6.º, n.º 3 do Tratado da União Europeia, onde foi estabelecido que "[d]o direito da União fazem parte, enquanto princípios gerais, os direitos fundamentais tal como os garante a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais e tal como resultam das tradições constitucionais comuns aos Estados-Membros"[47].

A União Europeia consagra princípios gerais de direito na sua ordem jurídica, uma vez que os Estados-Membros devem estar vinculados pelos direitos fundamentais. Seja a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, sejam os princípios constitucionais comuns aos Estados-Membros que são os princípios gerais do direito da União.

Reiterando o que sublinha CANOTILHO et al, a consideração das tradições comuns aos Estados-Membros, "quer como fonte de direitos fundamentais, quer enquanto critério interpretativo dos direitos consagrados na Carta permite afastar uma abordagem rígida de 'menor denominador comum', permitindo a densificação das normas do padrão comunitário de jusfundamentalidade de forma a proporcionar um elevado nível de protecção dos direitos, adequado ao Direito da União e em harmonia com o direito constitucional dos EM"[48]. Densificar direitos fundamentais no âmbito da União é, portanto, uma forma de proteger direitos básicos e gerar harmonia entre os Estados-Membros.

Ante todo o exposto, pode-se afirmar que a Proteção de dados é direito originário da União, fruto de um amadurecimento jurisprudencial e uma evolução legislativa que conduziram a este padrão

[46] "À proteção de dados pessoais relacionado com o princípio da dignidade humana foi forjado no espaço jurídico germânico" in: Pinheiro, José Alexandre Guimarães de Sousa. "Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional". Lisboa: AAFDL, 2015. p. 778.

[47] Para uma melhor compreensão quanto à relevância do Tratado da União Europeia neste processo, ver Porto, Manuel Lopes; Anastácio, Gonçalo et al. Ibid. pp. 252-256.

[48] Canotilho, José Joaquim Gomes e Mariana Canotilho. Comentário ao artigo 6° do Tratado da União Europeia in: Lopes Porto, Manuel e Gonçalo Anástácio. Ibid. p. 42.

de jusfundamentalidade imposto. Antes de se pensar em um regulamento sobre a Proteção de dados, tal princípio já havia recebido *status* de direito fundamental e previsão expressa nos termos do artigo 16º do TFUE, bem como no artigo 8º da CDFUE (ao qual foi atribuída força vinculativa idêntica aos tratados em virtude do artigo 6º do TUE)[49].

Em um viés mais específico, cabe equacionar a Diretiva que antecedeu o RGPD. Embora tenha sido revogada pelo RGPD, cabe ressaltar que a Diretiva 95/46/CE[50] tem caráter pedagógico reconhecido, além de ser um marco histórico. Isso é dito com base no próprio considerando 9 do RGPD que retirou dúvidas sobre a importância da Diretiva 95, mesmo ao fim de sua vigência.

Segundo o considerando 9 do RGPD, os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, o que indica que a opção legislativa passou por, tendo bebido influências decorrentes da vigência da Diretiva, ir mais além, criando um quadro diretamente aplicável aos diversos Estados-Membros, tendo a capacidade de uniformizar o regime atinente à proteção de dados no contexto jurídico da União enquanto a Diretiva 95 tinha como finalidade apenas promover a harmonização "[d]a defesa dos direitos e das liberdades fundamentais das pessoas singulares em relação às atividades de tratamento de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros"[51].

O contexto de edição da Diretiva 95 é resultado da necessidade de permitir o fluxo de informações pessoais no mercado interno em condições de segurança para os titulares dos dados, na senda do próprio desígnio inerente à literalidade do artigo 16.º do TFUE. A fim de que as legislações ficassem mais homogêneas, foi idealizado que a causa seria um nível de proteção equivalente. E sobre este contexto, SILVEIRA bem elucida o paradigma europeu para desenvolvimento de uma normativa em busca do nível adequado de proteção: "É neste contexto que surge a Diretiva 95/46/CE i impondo aos Estados-Membros a obrigação de adotarem legislação interna que oferecesse garantias de proteção semelhantes em todo o espaço europeu [...] estipulando os procedimentos e os comportamentos-regra relativamente ao fluxo de dados pessoais a transferir para Estados terceiros (os quais passaram a ser classificados pela Comissão Europeia de um modo diferenciado, consoante oferecessem, ou não, um 'nível de proteção adequado' em matéria de dados pessoais"[52]

---

[49] Neste sentido, veja-se Galvão, Luis Neto. Comentário ao artigo 16º do Tratado de Funcionamento da União Europeia in: Lopes Porto, Manuel e Gonçalo Anástácio. Ibid. Kindle Posição 5121.

[50] Portugal. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. Disponível em http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pt:HTML Acesso 20/02/2020.

[51] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid. Considerando 3.

[52] Silveira, Alessandra e Froufe, Pedro. "Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos". UNIO - EU Law Journal. Vol. 4, No. 2, Julho 2018, pp 4-20.

Harmonizar, pelo curso dos fatos, não foi suficiente. Decorrendo de uma fragmentação da Proteção de dados pelos diversos regimes nacionais resultantes das mais diversas transposições da Diretiva 95/46, surgiu a necessidade de um passo além na proteção de dados, para que, em nome da segurança jurídica, fosse dada uma certa singularidade ao regime vigente. Destas circunstâncias, calhou ao legislador europeu adotar um Regulamento[53].

Se os objetivos e princípios, apesar de repaginados, mantiveram-se na sua essência geral semelhantes, às razões de ser adotada uma nova espécie normativa foram, da mesma forma, cuidadosamente explicadas nas considerações do RGPD. Nota-se uma atualizada demanda e a adoção de um Regulamento em vias de promover uma adequada coerência e uniformidade. Na obra de PIÑAR MAÑAS[54], tudo fica mais evidente, ao entender que o conflito aparente de princípios suscitado anteriormente não foi resultado de uma inexistente incompatibilidade principiológica, mas sim a tentativa fracassada de harmonização dos regimes nacionais deveriam levar em conta, tanto a livre circulação de dados pessoais entre os Estados-Membros, mas também a tutela de um Direito Fundamental. O que acabou não acontecendo de forma uniforme.

Vincular sobretudo o nível de proteção, a fim de mitigar riscos de maneira mais efetiva e evitar sentimento de insegurança jurídica, demonstrou ser uma das motivações no RGPD. Sobre seus exatos termos, o Considerando dispõe sobre os esforços envidados ainda no âmbito da vigência da revogada Diretiva: *"*(...) não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União"[55].

O dispositivo elucida uma dicotomia levantada no início, acerca do conflito aparente entre Proteção de dados e o livre fluxo de dados pessoais. Todavia, o próprio Regulamento sobre a Proteção de dados usa como motivações da sua adoção a garantia da livre circulação de dados. Afinal, a partir do momento em que se vislumbra um Mercado Único Digital, presume-se a observância de atos

[53] General Report - XXVIII FIDE Congress in: Vilaça, José Luís da Cruz; et al. "The internal market and the digital economy". Vol. 1, Lisboa: Almedina, 2018

[54] Mañas, José Luis Piñar. Transparencia y protección de datos: las claves de un equilibrio necesario. In: "Derecho administrativo de la información y administración transparente". Madri: Marcial Pons, 2010. pp. 81-102.

[55] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid Considerando 9

vinculantes aos Estados-Membros. Conforme ABREU leciona acerca deste ponto: *"A UE avançou a estratégia para a prossecução do Mercado Único Digital que, a fim de promover o acesso e o exercício em linha de atividades de cidadãos e empresas, pretende promover um clima de livre concorrência enquanto observa padrões mais elevados de proteção de dados e do consumidor, sob pena de criar, sistemicamente, um retrocesso dos valores europeus quando não deve ser esse o caminho a calcorrear"*[56]

Para a doutrina no assunto, a coexistência dos dois princípios fortalece e potencializa ambos, entretanto a busca do motivo para que a Proteção de dados tenha sido convertida na questão jusfundamental identitária dos tempos atuais não pode se resumir a isto. De acordo com SILVEIRA[57], a centralidade que foi adquirida pela Proteção de dados não se resume apenas ao fato de o Mercado Único Digital ter sido convertido em um interesse público primário na UE, potencializando a inevitável circulação de pessoas, mercadorias, serviços e capitais com o consequente aumento do fluxo transfronteiriço de dados. Nesta visão, Proteção de dados é a questão jusfundamental atualmente "para que o projeto do humanismo não se torne irrelevante"[58].

Apesar das instâncias não se esgotarem entre si, ambos princípios parecem caminhar pela necessidade de uma proteção homogênea. A uniformidade viabiliza objetivos que existem desde a formação do grupo econômico europeu, qual seja estabelecer mecanismos que reforcem a posição da União Europeia como um dos paradigmas dominantes, assegurando a sua coesão, a estabilidade monetária e as vantagens do mercado único[59]. Portanto, a preocupação pela coesão dos Estados-Membros é encarada como elemento comum ao sucesso do Mercado Único[60] desde a formação do bloco econômico.

Inclusive, no processo de integração da União Europeia tomaram-se os direitos fundamentais como elemento de coesão[61], na medida em que se deixa de vislumbrar temas - a exemplo da proteção de dados - apenas como questões econômicas e comerciais, passando a ser vislumbradas como um

---

[56] Abreu, Joana Rita Covêlo de. "Digital Single Market as the new world to the European Union: repercussions in social and institutional regulatory structure–the universal service and the Body of European Regulators for Electronic Communications'(BEREC) redefinition". UNIO–EU Law Journal, v. 4, n. 2, 2018, pp. 48-60,

[57] Silveira, Alessandra e Froufe, Pedro. "Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos. UNIO - EU Law Journal". Vol. 4, No. 2, Julho 2018, pp 4-20.

[58] Silveira, Alessandra e Froufe, Pedro. Ibid.

[59] Stelzer, Joana. "União Européia e Supranacionalidade: Desafio ou Realidade?". Curitiba: Juruá, 2000. p.37

[60] Veja-se em Cortizo, Lucas. Cap. "Blockchain e e-Government (paradigmas e perspectivas)" in: Silveira, Alessandra, Joana Rita Sousa Covelo Abreu, and Larissa Coelho. "UNIO Ebook Interop 2019: O Mercado Único Digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir", Braga: Universidade do Minho, 2019.

[61] Vasconcelos, Álvaro de et al. "Portugal no centro da Europa". Lisboa: Quetal Editores, 1995. p. 36.

arcabouço legislativo em defesa de bens jurídicos basilares e culturalmente intrínsecos ao bom funcionamento da sociedade, dentre os quais, insere-se a Proteção de dados pessoais.

Diante do exposto, diferenças entre os níveis de proteção foram geradas por disparidades na execução e aplicação da Diretiva 95/46/CE, e com isso o Parlamento Europeu e o Conselho entenderam por necessário adotar o Regulamento, cuja força é de ato normativo vinculativo e diretamente aplicável em todos os Estados-Membros[62]. Disto decorre a lógica de que a revogação da Diretiva 95 pelo RGPD foi uma ação para garantir a aplicação cogente do Direito Fundamental da Proteção de dados pessoais numa perspectiva uniformizada.

Isto se deve ao fato de que o regulamento é um ato capaz de promover uma uniformidade de regime jurídico aplicável[63]. Tendo em vista as competências partilhadas e os atos jurídicos europeus previstos no artigo 288 do TFUE, a União Europeia adota regulamentos e diretivas. Sobre a diferença dos dois atos, SILVEIRA et al explicam que "residindo a diferença entre ambos no facto de que as diretivas apenas harmonizam as normas aplicáveis nos distintos Estados-Membros da UE, enquanto os regulamentos uniformizam o direito aplicável num dado domínio, sem necessidade de intermediação legislativa das autoridades nacionais"[64].

E, seguindo esta diferenciação, quando se opta por substituir uma diretiva por um regulamento da mesma matéria, fica perceptível que é buscada uma proteção equivalente em todos os Estados-Membros. Equivalência de proteção que fez com que uma legislação inicialmente harmonizada passasse a ser "agora tendencialmente uniformizada em todos os Estados-Membros"[65]. Esta evolução fez-se necessária para assegurar a livre circulação de dados no mercado interno.

A uniformização da execução pretendida pelo RGPD foi instrumento para alcançar a garantia de segurança jurídica, e desta, existe uma relação direta com a facilitação da atividade econômica sem entraves, com regramentos vinculantes, permitindo assim uma livre concorrência. Conforme bem observa a doutrina: *"O RGPD revogou a Diretiva 95/46/CE, que visava a proteção das pessoas no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados entre os Estados-Membros (Parlamento Europeu e Conselho da União Europeia, 1995), que foi transposta para a ordem jurídica portuguesa pela Lei n.º 67/98. O RGPD tem como objetivo uma uniformização da execução e*

---

[62] União Europeia. Regulamentos, diretivas e outros atos legislativos. Disponível em https://europa.eu/european-union/eu-law/legal-acts_pt Acesso em 20.02.2020

[63] Para aprofundar sobre a uniformidade do regulamento, veja-se em Camisão, Isabel; Abreu, Joana, et al. "Enciclopédia da União Europeia". Editora Petrony. 2017.

64 Silveira, Alessandra e João Marques. Ibid. p. 91–118

65 Ibid. p. 91–118

aplicação da legislação no que se refere ao tratamento dos dados pessoais, garantindo segurança jurídica e a atividade económica, sem entraves e uma livre concorrência"[66].

Entretanto, seguindo a evolução legislativa, ainda foram editadas algumas normas relevantes entre a Diretiva 95 e o RGPD, relacionadas ao tema. Cita-se a Diretiva 97/66/CE[67] que confirma o *modus operandi* de preservar a livre circulação dos dados pessoais seria uma forma de respeitar o direito fundamental da Privacidade.

Em seguida, a Diretiva 2002/58 CE, de 12 de dezembro de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas[68]. Dentre as determinações, trouxe temas que permanecem atuais na égide do RGPD, a saber "utilização das *cookies* é legítima, desde que se prestem informações claras e precisas sobre a sua finalidade, sendo indispensável o consentimento do utilizador; (...) A divulgação dos dados pessoais em listas deve ser autorizada pelo seu titular;" ou ainda "(...) São necessárias medidas de segurança em relação às chamadas não solicitadas para fins de comercialização que invadem a privacidade" [69].

Como vem sendo demonstrado, diversas das questões trazidas pelo RGPD já vinham sendo construídas pelo Ordenamento Europeu, mas atingiram um marco temporal relevante no dia 25 de maio de 2018, com a entrada em vigor do Regulamento Geral sobre a Proteção de Dados[70].

1.5. O RGPD Como Grau de Maturação

De acordo com a evolução normativa acima debatida, nota-se que o RGPD foi resultado de um grau de maturação, conforme explanam SILVEIRA e MARQUES, na qual se repara uma evolução doutrinal aliada a um arcabouço jurisprudencial que vão dar significância ao Regulamento. Nota-se não ser uma norma editada de súbito, mas sim, uma construção cultural europeia que permeia o Ordenamento e gera uma importância internacional, pois "o quadro normativo da União Europeia em matéria de proteção de dados, pela sua pertinência, pelo grau de maturação e pela densificação

66 Balinha, Hélio, et al. "O RGPD: a articulação entre a gestão de informação e a gestão de segurança da informação." Actas do Congresso Nacional de Bibliotecários, Arquivistas e Documentalistas. No. 13, 2018. p. 2.

67 Européia, União. Diretiva 97/66/CE do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das telecomunicações. Disponível em http://eur-lex.europa.eu/legalcontent/PT/ALL/?uri=CELEX%3A31997L0066 Acesso em 20/02/2020.

68 Européia, União. "Diretiva 2002/58 CE, de 12 de dezembro de 2002. Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas)." Diário Oficial das Comunidades Europeias, Bruxelas 31, 2002.

69 Salom, Javier Aparicio; Sergio Sanfulgencio Tomé. "El régimen jurídico de las cookies y su aplicación por la agencia española de protección de datos." Revista Aranzadi Doctrinal 11, 2014, pp. 217-235.

70 Europeia, União. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Ibid.

dogmática e jurisprudencial de que dispõe, constitui-se como um padrão globalmente respeitado e, por isso mesmo, replicado em vários pontos do mundo"[71].

Resumidamente, esta norma é aplicada aos responsáveis pelo tratamento de dados (denominados controladores) e aos subcontratantes que realizam alguma ação entendida por tratamento. O RGPD será aplicado às operações de processamento sobre dados pessoais europeus, independentemente se o tratamento esteja ou não localizado na União Europeia[72].

É imperioso, neste momento, traçar os devidos parâmetros normativos que serão utilizados no prosseguimento da investigação para debater sobre a tecnologia *blockchain* em relação à Proteção de dados. O RGPD vai ser um desígnio padrão, afinal como foi visto, existem dezenas de normas e antecedentes jurisprudenciais que tratam do Direito à Privacidade e Proteção de dados, precisando a análise de algum guia jurídico-principiológico concreto.

Apesar do RGPD ter entrado em vigor apenas em maio de 2018, sua aprovação ocorreu em 2016, e quem analisa a conjuntura política do momento, tenta relacionar algumas opções legislativas, a exemplo do âmbito material do Regulamento. Diante de uma série de atentados terroristas na Europa, como o de Bruxelas no dia 22 de março de 2016, o Parlamento Europeu passou a se preocupar com a devida prossecução criminal e foi por esta razão, segundo FERREIRA[73], que o artigo 2.º foi enfático ao determinar que está fora do âmbito legal o tratamento de dados pessoais voltado "prevenção, investigação, deteção e repressão de infrações penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública".

Entretanto, é impreterível mencionar a obra de MAÑAS que traz um entendimento sobre o novel Regulamento que vem sendo adotado pelas Autoridades de controlo, a saber uma recomendação de gestão de dados pessoais por parte do responsável, uma completa análise de riscos pelo responsável, observância dos princípios do RGPD desde a conceção e por defeito do produto que envolva tratamento, dentre outros. Sob termos exatos: *"Un nuevo modelo que podemos decir que pasa de la gestión de los datos al uso responsable de la información. Este es seguramente el más profundo cambio que el Reglamento va a imponer y que se aprecia en cuestiones como el principio de accountability traducido por «responsabilidad proactiva» (artigo 5.2 del Reglamento), los principios de privacidad desde el diseño y por defecto, la aproximación a la protección de datos basada en el análisis de riesgos, la figura del Delegado de protección de datos, el fortalecimiento de los códigos de conducta,*

[71] Silveira, Alessandra; Marques, João. Ibid. p. 116
[72] Jordan A. & Sowerby M. "Preparing for the General Data Protection Regulation – Digest", Information Security Forum Limited. 2016
[73] Ferreira, Rafael Freire. Ibid. p. 123

la exigencia de llevar un registro de las actividades del tratamiento, la regulación de las medidas de seguridad, y un largo etcétera"[74].

Seguindo este entendimento doutrinário que o RGPD inova em certos conceitos, não apenas se resumindo a uma Diretiva 95 repaginada, gozando de aplicabilidade direta, pode-se citar BOARDMAN[75] cuja contribuição é vislumbrar os princípios e direitos previstos no RGPD como uma valorização de ações e papéis na proteção e tratamento dos dados pessoais, que embora já viessem previstos na Diretiva 95, no Regulamento apresentam definições e âmbitos mais alargados. Acerca deste alargamento, o autor enumera aspectos que demonstram tal abrangência legal: Forma de obter o consentimento do titular dos dados (inclusive os menores de idade), maior rigor ao definir o tratamento para fim específico (em ordem de considerá-lo lícito), inclusão de categorias especiais de dados, a saber os dados sensíveis (dados genéticos, biométricos e sobre a saúde).

Ante o exposto, tem-se um Regulamento de força vinculante e com aplicabilidade direta, mas é imperioso debater seus limites. O âmbito normativo, seja material e formal, é fundamental para qualquer análise de conformidade, sobretudo no caso da presente investigação, uma vez que será buscada conformidade dos usos de uma tecnologia em especial, a *blockchain*, nos desígnios de uma possível implementação pela Administração Pública, em especial no combate à corrupção[76].

1.6. O Âmbito Material Do RGPD

Acerca do âmbito material de aplicação do RGPD, a estrutura geral segue a lógica estabelecida na Diretiva 95/46, uma vez que o n.º 1 do artigo 2º dispõe que o Regulamento se aplica aos tratamentos total ou parcialmente automatizados, bem como ao tratamento não automatizado de dados pessoais constantes, ou que venham a constar em ficheiros ou bancos de dados. Ao se depreender o conceito de tratamento do artigo 4, n.º 2 nota-se um âmbito material amplo, pois esta definição abrange diversos tipos de ação enquadrados sob a definição legal.

E para evitar que a aplicação da norma se perca na vastidão do conceito, o n.º 2 do artigo 2 elenca hipóteses nas quais irá haver tratamento de dados pessoais, mas que foram legalmente excepcionadas do enquadramento da norma: *"a) Efetuado no exercício de atividades não sujeitas à*

[74] Mañas, José Luis Piñar. I. "Introducción. Hacia Un Nuevo Modelo Europeo De Protección De Datos". Revista del Consejo General de la Abogacía, n. 98, 2016, p. 14.
[75] Boardman, Ruth; Mullock, James; Mole, Ariane – Bird & Bird & guide to the General Data Protection Regulation. Bird & Bird, 2017. apud Balinha, Hélio, et al. Ibid. pp. 2-3.
[76] Cortizo, Lucas. Cap. Blockchain e e-Government (paradigmas e perspectivas) in Silveira, Alessandra; Joana Rita Sousa Covelo Abreu; Larissa Coelho. Ibid. p. 16.

aplicação do direito da União; b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública."[77]

Em outras palavras, a alínea "a" expressa uma perspectiva que insere o caso concreto fora do âmbito da UE. Não obstante, a alínea "b" excepciona o "título V, capítulo 2, do Tratado da União Europeia" que diz sobre "Disposições específicas relativas à política externa e de segurança"[78]. Como também, a alínea "d" traz expressamente a questão da "prevenção de ameaças à segurança pública", assunto de caráter transnacional e extracomunitário[79]. O ponto em comum destas três alíneas é a presença de temas que demandam a adoção de normas específicas para tais domínios, atentas às suas especificidades.

Ao contrário das 3 alíneas (a, b, d) do artigo 2 n.º 2 que trazem exceções do âmbito material do RGPD, ora porque se extravasa o âmbito de aplicação do próprio direito da União, ora porque as matérias demandavam atos normativos adequados às suas especificidades, a alínea "c" demonstra uma hipótese em que o tratamento do dado pessoal não ultrapasse o âmbito da própria pessoa natural. A já denominada, antes mesmo da vigência do RGPD, "*household exemption*"[80] significa que o RGPD não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma atividade profissional ou comercial.

De acordo com a doutrina sobre o assunto, nem mesmo o alcance desta exceção ao âmbito normativo é uma contenda resolvida. Conforme WARSO[81] observa, a Proteção de dados além de um direito fundamental, possui importante papel ao mediar o equilíbrio entre outros direitos, por isso é que a aplicação da "*household exception*" deve ser estendida para incluir as atividades *online* que sejam privadas. Para o autor, esse papel vai-se refletir no complexo trabalho de definir a "*online privacy*",

---

[77] Europeia, União. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Ibid.

[78] Europeia, União. Tratado da União Europeia, versão consolidada. Disponível em https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF Acesso em 21.02.2020

[79] Neste sentido, Nesser, Petter; Stenersen, Anne; Oftedal, Emilie. "Jihadi terrorism in Europe: The IS-effect. Perspectives on Terrorism". V. 10, n. 6, 2016, p. 3-24.

[80] Warso, Zuzanna. "There's more to it than data protection–Fundamental rights, privacy and the personal/household exemption in the digital age.". Computer Law & Security Review 29.5, 2013, pp. 491-500.

[81] Warso, Zuzanna. Ibid.

uma vez que o ecossistema da rede é repleto de atores e atividades que estão a moldar os territórios e limites da Web.

Para socorrer quem interpreta o âmbito legal e suas exceções, os antecedentes jurisprudenciais ajudam na percepção. Afinal a interpretação terminológica não existe no Regulamento que, por opção legislativa, possui um largo âmbito material em ordem de assegurar um elevado nível de proteção[82].

1.7. Âmbito Formal Do RGPD

Por outro lado, no que concerne à aplicação territorial, nota-se uma alteração na definição de competência em relação à Diretiva 95/46. O Regulamento furtou-se de adentrar na questão de qual seria o direito nacional aplicável, em sentido diverso do que fora decidido pelo Grupo de Trabalho do artigo 29 em 2010 na opinião do "Dictamen 8/2010"[83]. Conforme este documento, o direito nacional do Estado-Membro se aplica quando o responsável pelo tratamento detém estabelecimento em algum Estado-Membro e recorre a meios de tratamentos situados neles.

O entendimento sofreu uma reviravolta no memorável acórdão do TJUE de maio de 2014, "Google Spain" (Google Spain SL, Google Inc. v AEPD[84], Mario Costeja González, C-131/12), que envolve a temática do direito ao esquecimento "ou direito à desindexação"[85]. Sem entrar no mérito por enquanto, o procedimento tratava da aplicação da Diretiva 95/46 sobre os motores e ferramentas de busca da internet, tendo de um lado da lide o Google (Google Spain e Google Inc.) e de outro a AEPD e Mario Costeja González[86].

Acerca do julgado, o Tribunal firmou entendimento que, mesmo que o estabelecimento comercial que se encontre dentro da União Europeia não seja o responsável pelo tratamento de dados pessoais ou por qualquer atividade diretamente relacionada a esse, não se deve ignorar o fato de existirem operações pelo estabelecimento exterior à UE. Uma vez que o estabelecimento fora da União

---

[82] Neste sentido, veja-se Voigt, Paul; Von Dem Bussche, Axel. "The EU general data protection regulation (GDPR). A Practical Guide". V. 1, Cham: Springer International Publishing, 2017. p.17.

[83] "mientras que ahora se pone el foco en las personas en cuanto destinatarias de los servicios o cuyo comportamiento es objeto de control (la orientación hacia las personas de la que hablaba el citado Dictamen 8/2010)" in: Vaquero, Juan Pablo Aparicio. "La protección de datos que viene: el nuevo Reglamento General europeo." AIS: Ars Iuris Salmanticensis 4.2, 2016, pp. 27-34.

[84] *Agencia Española de Protección de Datos.*

[85] O direito à desindexação pode ser entendido como sinônimo do direito ao esquecimento, ou ainda como um novo direito distinto daquele. Nesse sentido, veja-se: Ruaro, Regina Linden; Machado, Fernando Inglez de Souza. Ensaio a propósito do direito ao esquecimento: limites, origem e pertinência no ordenamento jurídico brasileiro. Revista do Direito Público, Londrina, v. 12, n. 1, 2017, p. 204-233.

[86] Carulla, Santiago Ripol. Cap "Aplicación territorial del reglamento". In: Piñar Mañas, José Luis (Coord.). "Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidade". Madrid: Editorial Reus, 2016. p. 77-186

Europeia poderia financiar a atividade que ocorre dentro do grupo econômico, o entendimento foi atualizado para interpretar a Diretiva 95 como aplicável mesmo que o tratamento fosse fora da EU.

Seguindo a construção jurisprudencial acerca do âmbito territorial, cumpre trazer o caso Weltimmo v NAIH (C-230/14), decidido pelo TJEU. Nesta decisão, a Corte Europeia determinou a noção de estabelecimento que deve ser estendido a qualquer real e efetiva atividade empresarial, mesmo que seja mínima. A fim de determinar se uma entidade estabelecida fora da União tem um estabelecimento em um Estado-Membro, o grau de estabilidade dos acordos e o exercício efetivo das atividades nesse Estado-Membro devem ser considerados à luz da natureza específica da situação econômica cumulado com atividades e prestação de serviços no caso concreto. Na própria decisão, foram citados os casos cinzentos das empresas que oferecem serviços exclusivamente através da Internet.

A decisão fala que o limiar para um "arranjo estável"[87] pode realmente ser bastante estreito quando a atividade principal seja a prestação de serviços em linha. E em consequência disto, em determinadas circunstâncias, a presença de um único funcionário ou agente da empresa não pertencente à União Europeia pode ser suficiente para constituir um acordo se esse funcionário ou agente agir com um grau suficiente de estabilidade.

Conforme foi visto, houve uma verdadeira construção jurisprudencial até a definição das regras territoriais no corpo e nos considerandos do RGPD. Saliente-se que a preocupação em atender as demandas tecnológicas permeou este processo e o Regulamento irá refletir este discernimento. Além do antecedente do *Google Spain SL, Google Inc. v AEPD, Mario Costeja González (C-131/12) e Weltimmo v NAIH* (C-230/14), merecem ser citados os casos do *Verein für Konsumenteninformation v Amazon EU* (C-191/15) e *Wirtschaftsakademie Schleswig-Holstein* (C-210/16).

Sobre o acórdão da Amazon[88], a questão da Proteção de dados foi expressamente suscitada para definir se uma empresa, estabelecida em um país (Luxemburgo neste caso), mas que dirigia suas atividades para outro país (Áustria[89]), deveria cumprir exclusivamente a lei de Proteção de dados do Estado-Membro em que estava estabelecida ou se também deveria cumprir as regras de Proteção de dados do Estado-Membro ao qual suas atividades comerciais são direcionadas.

[87] Nos seus termos: "The threshold for 'stable arrangement' can actually be quite low when the centre of activities of a controller concerns the provision of services online." In: Acórdão TJEU, Weltimmo v NAIH, de 1 de Outubro de 2015, processo C-230/14.

[88] Müller, Michael F. "Amazon and Data Protection Law–The End of the Private/Public Divide in EU conflict of laws?." Journal of European Consumer and Market Law 5.5, 2016. pp. 215-218.

[89] Neste caso, constatou-se este *hyperlink* com determinação diferente, indicando as atividades não estavam sendo dirigidas na Austria.

Por tudo isso, o atual Regulamento definiu sua aplicação territorial para ocorrendo o tratamento dentro ou fora da União. Sob os termos[90]: *"Artigo 3 1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União. 2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares que se encontrem no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com: A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; O controlo do seu comportamento, desde que esse comportamento tenha lugar na União. 3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público".*

O n.º 2 do artigo 3 RGPD clarifica a possibilidade de atuação por atitudes extra-europeias e centraliza a atenção no titular dos dados, uma vez que define "aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União".

Nota-se que não se fala, em momento algum, de "filial", que pressupõe uma decisão por parte da matriz em desenvolver um estabelecimento separado[91]. O próprio considerando 22 estipulou que não interpreta termos empresariais com rigor formal, ao definir que, para o legislador, no contexto da Proteção de dados pessoais, o "estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável. A forma jurídica de tal estabelecimento, quer se trate de uma sucursal, quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto"[92].

Quando o artigo 3. º, n.º .2, a) trata de "oferta de bens ou serviços"[93], precisa-se definir em quais hipóteses estará abrangido esta definição legal. Essas definições tornam-se cada vez mais relevantes no contexto da sociedade da informação, na qual temos a ubiquidade tecnológica e redes complexas de relacionamento entre empresas, o que dificulta a simples definição territorial da mesma.

[90] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid

[91] Para o conceito do Direito Empresarial de filial, vem em Negrão, Ricardo. Direito Empresarial-Estudo Unificado. Saraiva Educação SA, 2008.

[92] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid.

[93] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid.

Ante o exposto, a fim de determinar se o responsável pelo tratamento ou subcontratante oferece ou não bens ou serviços aos titulares dos dados que se encontrem na União, o Considerando 23 recomendou que o caminho seria "determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União"[94].

E partindo de um contra exemplo, o Considerando 23 RGPD ainda define que a mera disponibilização de um site acessível por um sujeito dentro da UE, ou até usar a língua oficial de algum Estado-Membro, por si só, não constitui a intenção prevista no artigo 3.º, n.º.2, a) RGPD. Entretanto, ao analisar o caso concreto, o conjunto de fatores como uso da língua, moeda corrente, possibilidade de entrega de bens e serviços no Estado-Membro e etc. serão levados em consideração para determinar o âmbito territorial[95].

Em outras palavras, o artigo 3 do RGPD define o âmbito territorial do Regulamento baseado em dois critérios: o critério do estabelecimento (artigo 3 n.º 1) e o critério do *targeting* (artigo 3 n.º 2)[96]. Basta que um desses critérios seja atingido que a proteção da normativa será aplicada. Além do mais, o artigo 3 n.º 3 determina a aplicação do RGPD inclusive quando a lei do Estado-Membro seja aplicada por força do Direito Internacional Público.

Neste desenvolvimento proposto, detalhou-se uma evolução legislativa que culminou no RGPD como um grau de maturação, norma esta que estabelece um âmbito material e territorialmente definido. Dentro deste escopo, há coexistência de princípios complementares e direitos subjetivos dos titulares dos dados, assentando-se assim as bases do RGPD como um guia jurídico e paradigma em face da tecnologia *blockchain,* cuja essência é registro de dados, conforme a seguir detalhado.

[94] Considerando 23 em Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid.

[95] Neste sentido, as orientações do Comité Europeu para a Proteção de Dados são no sentido da jurisprudência decorrente dos processos Peter Pammer contra Reederei Karl Schlüter GmbH & Co. KG e Hotel Alpenhof GesmbH contra Oliver Heller (processos apensos C-585/08 e C- 144/09, Acórdão TJEU), a fim de sugerir uma análise da existência de uma oferta de bens ou serviços a um titular dos dados na União. Ver mais em: União Europeia. Diretrizes 3/2018 sobre o âmbito de aplicação territorial do RGPD (artigo 3.º). Comité Europeu para a Protecao de Dados. p. 19.

[96] União Europeia. Diretrizes 3/2018 sobre o âmbito de aplicação territorial do RGPD (artigo 3.º). Ibid.

CAPÍTULO II

2.1. Da Tecnologia Blockchain

Neste capítulo, é necessário definir a tecnologia *blockchain*, trazendo características singulares da mesma, a fim de entender suas particularidades para, no capítulo seguinte, buscar analisar os aspectos de compatibilidade entre tal tecnologia e o Regulamento Geral sobre a Proteção de Dados. Para tanto, definir-se-á *blockchain* a partir do ensinamento de CROSBY[97] que definiu a *blockchain* como sendo – essencialmente – uma base de dados distribuída, ou ainda, uma "*public ledger*" (um registro ou livro-razão público). Segundo o autor, neste registro vão ser inseridas todas as transações ou eventos digitais a serem executados, e a noção de distribuição decorre de que todos os participantes receberão uma cópia atualizada deste registro.

Na definição, o autor explica o que a limita, uma vez que, na própria definição, utiliza-se o protocolo e o formato público que, posteriormente, este estudo demonstrará ser uma das possíveis formas da *blockchain*. Por isso, para fins de simplificar a conceptualização, explica-se que a *blockchain* é uma forma de inserção de dados. Inserção esta que, por sua vez, vai seguir um critério de verificação, a exemplo do consenso da maioria dos participantes.

Esta noção mais ampla de que a *blockchain* tem natureza de inserção de dados vem nos ensinamentos de MATZUTT[98], cujo contributo permitiu enxergar que, no paradigma da Bitcoin, além da intenção manifesta de registrar transações financeiras, se viabilizou a possibilidade de inserção de dados não financeiros, até pequenas mensagens através de tipos de transação especial, ou inclusive a introdução de ficheiros completos programando dados arbitrários como transações padrão. Para evitar possíveis códigos maliciosos, a Bitcoin adotou modelos-padrão e os *nodes*[99] da rede acabam descartando os *scripts* que não estão em conformidade[100].

O termo cadeia foi devidamente pensado porque, como será explanado, existe uma relação de parentesco entre os blocos que, interligados, numa análise *lato sensu*, constituem uma verdadeira *timeline chain*, uma cadeia em que cada componente obedece a uma ordem casual, temporalmente registrada. Em outros termos, o registro distribuído tem os dados de cada transação realizada e os

---

[97] Crosby, Michael et al. "Blockchain technology: Beyond bitcoin". Applied Innovation, v. 2, n. 6-10, 2016. p. 71.

[98] Matzutt, Roman et al. "A quantitative analysis of the impact of arbitrary blockchain content on bitcoin". International Conference on Financial Cryptography and Data Security. Springer, Berlin: Heidelberg, 2018. p. 420-438.

[99] *Nodes* são pontos de comunicação e redistribuição no contexto de uma rede. Para maior aprofundamento neste ponto, ver em Cortizo, Lucas. Cap. Blockchain e e-Government (paradigmas e perspectivas) in Silveira, Alessandra, Joana Rita Sousa Covelo Abreu, and Larissa Coelho. Ibid. p. 16

[100] Matzutt, Roman et al. Ibid

blocos são tecnicamente interligados (o bloco posterior é suposto possuir um código *hash*[101] referente ao bloco anterior), tornando o registro resistente a violação ou apagamento, devido à forma com que as propriedades criptográficas e a sua própria conceção distribuída de rede são utilizadas.

A doutrina, bem como a aplicação do entendimento da UE, mostra que, apesar de a Bitcoin, a conhecida moeda *peer-to-peer* digital, ser o caso pioneiro ao usar uma das facetas da *blockchain*, a tecnologia que lhe subjaz pode ser percecionada de forma bem mais ampla que a sua primeira execução prática, sendo aplicável ao mundo financeiro e fora dele. Em estudo do Parlamento Europeu sobre "*Cryptocurrencies* and *blockchain*"[102], os autores deixam clara a separação dos dois institutos: apesar de estarem claramente ligados, um não deve ser confundido com o outro.

A *blockchain* é um tipo de tecnologia de *ledger* distribuída que forma a base do cripto-mercado, é a tecnologia por trás de diversas criptomoedas já em circulação, fato que não a limita. Por isso é que a *blockchain* pode ser aplicada em vários setores e possui uma maior gama de possibilidades que ultrapassam o contexto financeiro das criptomoedas. "Precisa-se traçar uma evidente linha entre *blockchain* e criptomoedas"[103].

Voltando ao defendido por CROSBY[104], a abordagem fica sob outro prisma, no qual a *blockchain* acaba por ser capaz de estabelecer um sistema para criar e distribuir consenso digitalmente. O que resulta em entidades participantes cientes dos acontecimentos de forma atualizada e simultânea, dotando-as de cópia irrefutável daquele registro. Este conceito promete abrir as portas para desenvolver uma relação democrática e escalável, rompendo com o paradigma de centralização que foi transposto inclusive na *World Wide Web,* que mesmo descentralizada e aberta ainda passa pelo controle de um oligopólio[105]. Por isso, defende-se que há uma tecnologia disruptiva, centro de uma revolução que acaba de começar[106].

Apesar de o primeiro uso mundialmente conhecido da *blockchain* ter ocorrido publicamente em 2008, através do lançamento da Bitcoin, para criar um contexto histórico do seu surgimento, precisa-se voltar alguns séculos na História. Apesar do senso comum de que basta envolver tecnologia que haverá inovação, esta afirmação, além de falaciosa, não surge como suficiente para justificar a

---

[101] De acordo com Mackenzie, Donald. "Pick a nonce and try a hash". London Review of Books, v. 41, n. 8, p. 35-38, 2019: o hash apanha uma mensagem (ou outro texto qualquer), mistura de forma aleatória e condensa em um formato de tamanho fixo correspondente chamado de digest.

[102] Houben, R.; Snyers, A. "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion". Europe Parliament, 2018. p. 24

[103] Houben, R. et al. Ibid. p.24

[104] Crosby, Michael et al. Ibid.

[105] Smyrnaios, Nikos. "Internet oligopoly: The corporate takeover of our digital world". Emerald Group Publishing, 2018.

[106] Crosby, Michael et al. Ibid.

utilização do termo disrupção. É o que se pode depreender da explicação de PORTER et al[107] que definem a inovação disruptiva como uma decorrência do estabelecimento que seja resultado de fatores tecnológicos ou não tecnológicos. E ainda vai além em analisar se a tecnologia atua de forma considerável para o alcance da inovação disruptiva, o que traria a noção de tecnologia disruptiva.

2.2. Aspectos Introdutórios Sobre A Blockchain

A fim de perceber o contexto de surgimento e utilização atual da *blockchain*, deve-se discernir um período bem anterior ao lançamento da Bitcoin que, apesar de ter sido o primeiro grande evento de divulgação concreta daquela tecnologia, mostra-se apenas um evento no curso de um processo evolutivo.

Diante da natureza de "*ledger*", consegue-se identificar desde os primórdios da civilização humana a presença dos livros e registros. A junção entre escrita, dinheiro e registros tornou possível, ao ser humano, fazer negócios, e por conseguinte, estabelecer-se em maiores grupos e desenvolver mais complexas organizações político-sociais. VIGNA[108] identifica que a primeira *ledger* remonta a 3.000 A.C., na antiga Mesopotâmia, cuja contribuição para as civilizações posteriores é justamente o aparecimento de registros de impostos, pagamentos, pagamento de trabalhadores – e um dos mais relevantes historicamente – o sistema da Lei Babilônica, o famoso Código de Hamurabi[109], que está escrito e conservado em um desses registros. Então, se a troca de bens e serviços tem definido a expansão da sociedade, isto só restou possível porque os indivíduos puderam, através da escrita, registrar tais trocas. Sem registros, não existe sequer crédito e o comércio se limita ao câmbio de produtos.

Os registros, apesar de oferecerem dados de algum evento, podem ou não oferecer veracidade, nem conseguem cabalmente garantir que aquele conteúdo está intacto. Para ilustrar o problema, cita-se o histórico atavio relativo à demarcação territorial que encontra um inimigo na falsificação de registros públicos, a denominada tática de grilagem de terra[110]. Neste processo de grilagem, há a utilização de um título de propriedade falso, cujo resultado foi proveniente de um mecanismo de apropriação ilegal de terras públicas, cujo título era um papel comprado ilicitamente dos

[107] LI, Munan; Porter, Alan L.; Suominen, Arho. "Insights into relationships between disruptive technology/innovation and emerging technology: A bibliometric perspective". Technological Forecasting and Social Change, v. 129, 2018. p. 285-296.
[108] Vigna, Paul; Casey, Michael J. The truth machine: the blockchain and the future of everything. Picador, 2019.
[109] Thornton, Ann-Marie. "Hammurabi, Babylonian law". Topic 1, Secondary Source, 2017.
[110] Brasil, Ministério do Meio Ambiente. "A grilagem de terras públicas na Amazônia brasileira". Instituto De Pesquisa Ambiental Da Amazônia, 2006.

cartórios ou de terceiros; ora, e para dar "uma certa aparência de autenticidade, o documento era colocado em uma gaveta com alguns grilos. Passado algum tempo, os grilos iriam alimentar-se das bordas da escritura, expelir excrementos no documento e auxiliar na transformação do papel de cor branca para uma cor amarelada, ficando com um aspecto envelhecido"[111]. Assim, o título de propriedade passaria maior credibilidade ao seu possuidor, apesar de que, nos dias atuais, já se usem tecnologias mais eficazes para conseguir burlar os registros públicos e falsificar documentos.

Mas o problema reside na maneira como a verdade está formatada. Segundo VIGNA[112], por quase sete séculos, os livros foram, no senso comum, a equação da verdade, mesmo que de forma individual e inconsciente. A adoção do livro-razão ao nível de dogma aconteceu através de um processo, sobretudo no mundo ocidental de mudança de perspectiva.

Historicamente, a influência da política face à usura e à ausência de instrumentos contábeis e matemáticos adequados acarretou a mitigação da expansão do crédito e empréstimos em um primeiro momento, e atividade bancária e advento do capitalismo em consecução lógica. E a Europa Ocidental praticamente não possuía conhecimento sobre a matemática, sendo apenas durante o século XII que as Cruzadas da Igreja Católica abriram caminho para o mundo oriental e viram o quanto eles já eram mais avançados com números e equações[113].

Até o século XIII, o conhecimento matemático europeu resumia-se aos monges que tinham um calendário para celebrar a Páscoa. E, neste contexto, um mercador italiano chamado Fibonacci viajou por Grécia, Egito e Sicília, coletando destes vários povos inúmeros papéis de conhecimento matemático. Em sua memorável obra, o Liber Abaci – considerado um dos livros mais importantes da Idade Média[114] - ele trouxe conceitos desconhecidos até então, a exemplo das integrais, frações, raiz quadrada e álgebra.

Entretanto, a grande contribuição (até levando em consideração a finalidade profissional de Fibonacci), era a aplicação comercial destas operações. A noção do "algarismo 0 (zero)", por exemplo, é a base da disrupção da matemática comercial, pois cria terreno para expansão, aumenta as proporções de lucro, faturamento, organização e volume.

Todavia, o Liber Abaci apenas criou uma espécie de "combustível" aos comerciantes europeus, faltando algum mecanismo para utilizar todo esse potencial. E a engenharia foi, justamente,

---

[111] Brasil, Ministério do Meio Ambiente. p. 11

[112] Vigna, Paul et al. Ibid

[113] Lyons, Jonathan. "The house of wisdom: How the Arabs transformed Western civilization". Bloomsbury Publishing USA, 2011.

[114] Neste sentido, veja-se em: Sigler, Laurence. "Fibonacci's Liber Abaci: a translation into modern English of Leonardo Pisano's book of calculation". Springer Science & Business Media, 2003.

[114] Sangster, Alan. "The genesis of double entry bookkeeping". The Accounting Review, v. 91, n. 1, 2016, p. 299-315

a "*double-entry bookkeeping*"[115] (o livro-razão das partidas dobradas, ou de entradas duplas, conforme as mais diversas traduções) que representou o prelúdio das Ciências Contábeis. E ocorreu em 1494, alguns anos após a importação de Fibonacci; desta vez, o método foi desenvolvido por um Frei Franciscano chamado de LUCA PACIOLI[116]. Esta obra foi pensada desde o princípio em ser acessível e bastante utilizada, visto que foi escrita em italiano, ao invés de latim[117].

A importância da contribuição do Frei foi além do que outra já tivesse feito, porque trouxe técnica contábil com aplicação prática. Ela surge porque, sendo a usura proibida, era necessário voltar a inteligência envolvida para a viabilização da posição do mercador que tinha de demonstrar, perante a Igreja, que a riqueza havia revertido em benefícios para a humanidade. O obstáculo residia, na visão de pensadores como AHO[118], na sua incompatibilidade com o facto de uma pessoa ser cristã porque se entendia que não podia, ao mesmo tempo, buscar o lucro, o que foi relativizado por uma passagem da própria Escritura Sagrada: nesta, encontrava-se uma alegoria relativa ao julgamento final após a morte, na qual o resultado vai ser a comparação do livro da vida (nas mãos de Deus) e o livro da morte. Nota-se a presença de dois livros, que vão ser comparados com a finalidade de obter um julgamento final. Todo registro que não constar simultaneamente em ambos livros será descartado.

Neste contexto, o sistema do livro-razão de partidas dobradas permitiu que surgisse o mercador cristão e apenas solicitava que o comerciante registrasse, com a data *Anum Dominnem*, todas as transações que forem feitas, lembrando-se sempre de adotar uma postura ética e trabalhadora e atuando em nome d'Ele[119].

Com esta nova conceção cultural, o crédito e débito passaram a ser permitidos na Europa Ocidental e o livro-razão das partidas dobradas passou a ser uma forma eficiente de registrar ambos institutos econômicos. Este marco histórico impulsionou a atividade bancária, a qual foi bem explorada inicialmente pelos membros da família Medici de Florença sendo intermediários de uma relação de crédito e débito que passou a ser possível[120].

Se um vendedor em Roma resolvesse vender um bem a um comprador em Veneza, o intermediário entre os dois utilizava a técnica do registro de partidas dobradas, na conta do vendedor creditava um valor, que deveria ser exatamente igual ao valor debitado na conta do comprador. E

---

[115] Carqueja, Hernâni O. "O livro de 'm. Barrême (1721)', em francês, e os dois primeiros livros em português sobre
116 Pacioli, Luca et al. Summa de Arithmetica geometria proportioni: et proportionalita. Tokyo: Yushodo Co, 1989
117 Vigna, Paul. Et al. Ibid
[118] Aho, James A. "Rhetoric and the invention of double entry bookkeeping". Rhetorica: A journal of the History of Rhetoric, v. 3, n. 1, 1985. p. 21-43.
[119] Vigna, Paul. Et al. Ibid.
[120] Parks, Tim et al. "Medici money: banking, metaphysics, and art in fifteenth-century Florence". Nova York: WW Norton & Company, 2005.

assim surgia uma forma de pagamento à distância entre partes que não precisavam confiar entre si, mas confiavam que a instituição financeira intermediária iria usar as partidas dobradas para, respectivamente, creditar e debitar as partes da transação.

Neste sentido, CARRUTHERS[121], para explicar a atuação da família Medici, categorizou-a como um banco internacional, cujas principais características assentavam numa demonstração de fidelidade, honestidade e capacidade. Para citar como exemplo, os Medici usavam auditorias para monitorar as diversas áreas de gerenciamento, e de maneira similar aos lordes ingleses - cujo principal critério para atuação de um gerente era estar interessado na honestidade dos subordinados – agiam de forma a estimular a confiança na sua instituição.

A confiança era o cerne central das relações: os comerciantes precisavam acreditar em certos fatores, porque transações ocorriam em distantes localidades[122], e esses fatores eram os livros de partida dobrada. A partir do momento que as partidas dobradas criaram a contabilidade, ainda segundo CARRUTHERS[123], a figura do contador deixou de ter a conotação de simples ajudante e passou a ser a principal fonte de uma informação privada.

Todo esse contexto histórico demonstra o surgimento da contabilidade e dos inevitáveis intermediários (que vinham a ser os grandes bancos do mundo), instalação das bases para permitir a expansão comercial, a Renascença e a emergência do próprio capitalismo. "Permitiu-se o estabelecimento de uma prática de 500 anos das instituições financeiras que criaram para si a função de portadores da confiança de forma centralizada da sociedade"[124]. E este conceito do livro-razão de partidas dobradas, conforme será explicado, estava no fundamento do Estado-nação surgido na Modernidade após o fim do contexto feudal da Idade Média.

Quem defende que a *blockchain* representou uma disrupção, normalmente vislumbra no *paper* de SATOSHI NAKAMOTO[125] de 2008 uma ruptura similar à obra de LUCA PACIOLI de 1494. O ano de 2008 inclusive foi marcante para o mundo. No início do ano, em 29 de Janeiro, a empresa Lehman Brothers apresentou um relatório financeiro sobre o ano anterior e o resultado tinha sido espetacular: com uma receita de 59 mil milhões de dólares e ganhos acima de 4 mil milhões de dólares, a conta

[121] Carruthers, Bruce G.; Espeland, Wendy Nelson. "Accounting for rationality: Double-entry bookkeeping and the rhetoric of economic rationality". American journal of sociology, v. 97, n. 1, 1991, p. 31-69.
[122] Ramsay, G. D; John Isham. "Mercer and Merchant Adventurer: Two Account Books of a London Merchant in the Reign of Elizabeth I". Durham: Northamptonshire Record Society, 1962. p.53
[123] Carruthers, Bruce G. Ibid.
[124] Vigna, Paul. Et al. Ibid
[125] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019.

era simples, os registros e livros daquela empresa estavam em alta[126]. Mas, apesar de ser uma das bases do *Wall Street* e do seu nível de confiança ser elevado, a verdade era que as *ledgers* da Lehman Brothers estavam sendo adulteradas, evidenciando uma falta de transparência ligada à contrafação de registros pelas empresas da bolsa de valores.

Após trilhões gastos por governos e bancos centrais a fim de consertar a quebra da bolsa pelo despencar da confiança dos investidores, a ordem antiga foi reestabelecida. O bem mais valioso, a confiança, apesar de trincado com o *crack*, permanecia no ideal da sociedade em relação aos registros contábeis[127]. Mas, no mesmo ano, em 31 de outubro de 2008, foi lançado um curioso "*White paper*"[128], assinado por alguém desconhecido publicamente, chamado Satoshi Nakamoto. Em resumo, ele descrevia uma moeda chamada Bitcoin, uma versão digital do dinheiro que não precisava de Estado ou de instituições financeiras, já que, afinal, essa moeda iria ser registrada num diverso conceito de livro-razão, um registro distribuído.

Alguns conceitos semelhantes são prévios ao da *blockchain*. NICK SZABO, proveniente do movimento *cyberpunk*, já havia desenvolvido algo semelhante na década de 90[129]. Um protocolo, criado por ele, tinha como alicerce uma tabela executada em uma máquina virtual, que nada mais era que um conceito de rede com computadores interligados e acessível por múltiplas partes. SZABO[130] ainda previu as bases da tecnologia dos *smart contracts,* uma vez que se desejou traduzir cláusulas contratuais em código, transformando-as em um software executável de forma automatizada, e assim conseguindo reduzir os terceiros de confiança entre as transações, tecnologia a qual pode utilizar a forma de registro baseada na *blockchain*.

Já em 2005, pode-se mencionar GRIGGS que desenvolveu, ao trabalhar na Systemics, um sistema protótipo de um livro-razão de entradas triplas[131]. E, neste projeto, o cientista utilizava a criptografia para assinar e tornar fraudes mais difíceis de serem cometidas. O terceiro livro-registro continha a sequência assinada dos recibos que poderia ser verificado de forma pública e em tempo real, muitos dos conceitos similarmente trazidos pela *blockchain*.

---

126 Bloomberg. Lehman Brothers resurrected? Well almost. Disponível em https://economictimes.indiatimes.com/lehman-brothers-resurrected-well-almost/articleshow/6562620.cms?from=mdr Acesso em 03/04/2020

127 Vigna, Paul. Et al. Ibid

128 Nakamoto, Satoshi. Ibid.

129 Szabo, Nick. "Smart contracts: building blocks for digital markets". Extropy: The Journal of Transhumanist Thought, v. 18, n. 6, 1996. p. 2,

130 Christidis, Konstantinos; Devetsikiotis, Michael. "Blockchains and smart contracts for the internet of things". Ieee Access, v. 4, 2016, p. 2292-2303.

131 Grigg, Ian. "Triple entry accounting". Systemics Inc, 2005.

Os exemplos precursores ao da *blockchain* mostram ideias de mesma natureza, mas que adotam arquiteturas diversas. Natureza esta que buscava remodelar o conceito de confiança e centralização. Por isso, a partir de agora, parte-se a uma detalhada análise do conceito estrutural adotado na *blockchain,* vendo os aspectos de design e arquitetura que ajudarão a entendê-la e a pensá-la para fins de conformidade com a Proteção de dados de forma a antever a possibilidade de encontrar solução para questões específicas da Administração Pública.

2.3. Organização de blocos e dados

Pode-se definir a *blockchain* como uma sequência de blocos, a qual reúne uma linha de todas as transações/registros que se queira inserir. Os blocos não estão individualmente registrados, eles são um conjunto de informações, no qual estão escritos dados referentes a este bloco em si, mas também ao seu bloco imediatamente anterior. Apesar de se falar em bloco, a *blockchain* representa uma estrutura holística, porém, para fins teóricos, pensar em um conjunto de blocos ajuda no entendimento da ligação forte da cadeia e na inserção temporal das transações. Em outros termos, a *blockchain* trata-se de uma cadeia de registros organizados em blocos, e mecanismos criptográficos fortes entre os blocos faz com que exista uma intensa relação da cadeia como um todo.

Tecnicamente, a representação informática do que se chama bloco seria um "'Énuplo" ou "Tupla": uma estrutura de dados (com restrição de adição, alteração, remoção), um "conjunto finito"[132], ou ainda, uma sequência imutável. Quando utiliza o termo "*tuple*", YANG explica de forma visual como o bloco poderá ser visualizado, a partir das informações que contém: "*a tuple of \{{<}hash, parent hash, number, miner, nonce, timestamp, transactions{>}\}*"[133]. De forma gráfica, importante trazer à baila a seguinte representação didática:

[132] Nguessan, Desire; Jose Sidnei Colombo Martini. "Framework for security and privacy Management for Mobile Middleware Based on tuple.". IEEE Latin America Transactions, vol. 13, n.8, 2015. pp. 2757-2762.

[133] Li, Yang, et al. "EtherQL: a query layer for blockchain system." International Conference on Database Systems for Advanced Applications. Springer, Cham, 2017. p. 150-250

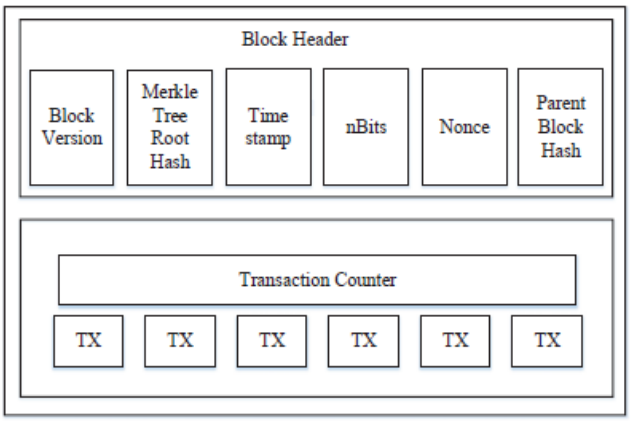


Figura1: Estrutura do bloco por ZHENG et al[134]

Uma vez que cada bloco aponta para o bloco anterior, através de uma referência numérica única (o já denominado *digest* do código *hash*), os blocos estão logicamente dispostos numa cadeia, em uma sequência improvável de ser adulterada, e esta resiliência da ligação entre blocos vizinhos é importante para entender porque a *blockchain* é aventada como solução de segurança no armazenamento de dados. Nas palavras de ZHENG[135], essa ligação entre blocos cria um parentesco entre eles, por isso é que o bloco anterior vai ser chamado de pai em relação ao bloco posterior que irá armazenar seu correspondente código *hash*. E em decorrência lógica desta relação, o primeiro bloco não terá bloco pai. De acordo com BUTERIN[136], o primeiro bloco será chamado de bloco *Genesis*, pois promove a abertura do registro e não tem nenhum antecedente.

No que tange ao bloco em si, apesar de, em conceitos mais superficiais, declararem que apenas existe o registro da transação, de um olhar mais detalhado é possível depreender mais alguns pormenores. Primeiramente, o bloco vai conter a versão, indicando quais as regras de validação que devem ser seguidas naquele contexto. Como já foi dito, encontrar-se-á o código *hash* referente ao bloco exatamente anterior, mas além disso, o "Merkle tree root hash" com um *hash* de todas as transações que forem registradas naquele bloco. Ou seja, cada bloco conterá, numa espécie de cabeçalho

[134] Zheng, Zibin et al. "An overview of blockchain technology: Architecture, consensus, and future trends". IEEE international congress on big data (BigData congress), IEEE, 2017. p. 558

[135] Zheng, Zibin et al. "Blockchain challenges and opportunities: A survey". International Journal of Web and Grid Services, v. 14, n. 4, 2018. p. 352-375.

[136] Buterin, Vitalik et al. "A next-generation smart contract and decentralized application platform". Ethereum White paper, v. 3, n. 37, 2014. Disponível em https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf Acesso em 25/04/2020.

(*header*), os metadados e as transações que vão ser representadas por essa "*Merkle tree*"[137], cujo root vai estar inserido, com a simples finalidade técnica de provar que a transação registrada é parte daquele bloco específico. E no mesmo cabeçalho do bloco, o espaço do *hash* do bloco anterior, interligando os blocos entre si e criando a relação de parentesco já explicada.

Não suficiente, haverá a *timestamp*[138]: selo temporal de quando o bloco foi validado. Consoante SZALACHOWSKI, são carimbos que servem de *input* para a aumentar a dificuldade do processo de validação, e com isso impede que um atacante manipule a *blockchain*, tendo em conta que registros vão necessariamente ser feitos de forma cronológica.

O selo temporal pode ser traduzida para um carimbo de tempo, para que o bloco seja inserido na cadeia de forma cronológica, tanto de data, como de hora. O formato do carimbo pode seguir esta lógica, por exemplo: *1970-01-01T00:00* UTC. Por isso que CHRISTIDIS[139] conceitua a *blockchain* sendo um registro temporal e autenticado da atividade de uma rede, afinal os *nodes* desta rede seguem passos pré-definidos e vão inserir dados de maneira linearmente organizada.

E por fim, ainda incluso em um único bloco, vai ser encontrado o "nBits", o atual e online objeto para *hashing*, salvo em um formato compacto; mas também pode ser utilizado o *Nonce:* um espaço de 4 byte que usualmente inicia com vários zeros que vão aumentando a cada cálculo do *hash*. O processo que envolve o *nonce*, segundo bem detalhado por MACKENZIE[140], é que a entidade validante não precisa validar apenas a transação, mas também valida os *nonces* referentes, ressalvando que esta estrutura não é transversal a todas *blockchain* e oferece apenas uma possibilidade.

Definido pelo autor como um número arbitrário, na definição citou inclusive Hamlet para explicar que a palavra é um antigo termo sinônimo de ocasião[141], e disto decorre que a única maneira de achar o *hash* com a quantidade de zeros iniciais é aleatoriamente "apanhar um *nonce* e testar um

[137] Ver conceito em Merkle, R. C. "A digital signature based on a conventional encryption function". Berlin: Springer, Heidelberg Proceedings of Advances in Cryptology, CRYPTO 1987, vol. 293, 1988.
[138] Szalachowski, Pawel. "Towards More Reliable Bitcoin Timestamps". 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018. p. 101-104.
[139] Christidis, Konstantinos; Devetsikiotis, Michael. "Blockchains and smart contracts for the internet of things". Ieee Access, v. 4, p. 2293. 2016.
[140] Mackenzie, Donald. Ibid. p. 7.
[141] Nos termos de Mackenzie, Ibid: "'nonce', na arbitrary number. (It's an old word, found for example in Hamlet; 'for the nonce' meant 'for the occasion'".

hash"[142]. Probabilisticamente afirmando, falhar-se-á em produzir o resultado desejado e o caminho será apanhar um outro *nonce* e testar novamente[143].

No momento em que finalmente se encontra o *hash*, com ao menos o número de zeros requerido, é importante mencionar a intensidade computacional que pode ser envolvida no processo de validação da transação para ser registrada na *blockchain*. Apesar de matematicamente não ser correto afirmar que este sistema é plenamente seguro, pois sempre existe uma possibilidade, do ponto de vista jurídico, os institutos precisam oferecer segurança jurídica que vai ser pensada observando demandas de proporcionalidade.

Ante todo o exposto, um bloco não se resume a dado, ou dado pessoal diretamente relacionado, havendo diversas propriedades e recursos técnicos dentro da estrutura pensada para cada bloco. Mas por ser um registro, é natural que seja avaliado não apenas à luz da sua conformidade jurídica, mas também quanto à sua própria capacidade técnica. Um dos parâmetros de capacidade é o máximo de transações que cada bloco pode conter. Isto vai depender, então, do tamanho do bloco e do tamanho de cada transação a ser registrada. Inclusive, de acordo com GREVE, o tamanho do bloco é um dos requisitos a ser analisado no âmbito do processo de validação, a fim de averiguar se "o seu tamanho está dentro do limite aceito pela rede"[144].

A *blockchain* usa o chamado mecanismo de criptografia assimétrica para validar os seus registros e, a partir disso, cria um ecossistema que não depende da confiança em intermediários. A ausência de autoridade é trazida pelo conceito desenvolvido no elucidativo estudo feito pelo Nomura Research Institute a pedido do Ministério da Economia, Comércio e Industria do Japão[145], o qual, nas conclusões, define a *blockchain* como um mecanismo usando uma plataforma *peer-to-peer* que permite o registro de transações cuja autenticidade é garantida, através do qual se promove a prevenção de duplicidade.

Além disso, ainda assegura que os dados registrados serão rastreáveis, o que garante transparência das transações, uma vez que a falsificação é dificultada por essa particularidade. Não obstante, menciona a potencial resistência do sistema contra ataques por utilizadores maliciosos,

---

[142] Mackenzie usa a expressão "the only way to find a hash with the requisite number of initial zeros is randomly to pick a nonce and try a hash". p. 7.

[143] De acordo com Mackenzie, Ibid: este ato vai demonstrar o trabalho de validação, caso a blockchain assim esteja estruturada, cujo tempo necessário para alcançar o resultado será diretamente proporcional à capacidade computacional, afinal se os nonces possuírem 32 dígitos binários, fala-se em mais de 4 bilhões de números, e vários *nonces* a serem testados

[144] Greve, Fabíola et al. "Blockchain e a Revolução do Consenso sob Demanda". Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), 2018. p. 16.

[145] Survey on Blockchain Technologies and Related Services FY2015 Report. Nomura Research Institute. 2016. Disponível em https://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf Acesso em 20/04/2020

atribuindo à ausência de uma autoridade central para dificultar um ataque direcionado uma das suas finitudes.

O estudo[146] ainda define de forma ampla a *blockchain* como um simples protocolo para mutualmente aprovar informação de valor através da internet. E esta noção, apesar de resumida, traz as essências da *blockchain*, que ao ser entendida como um protocolo, vai expor um acordo, um jogo de regras definidas que pressupõe a atuação de utilizadores. Sem detalhar a personalidade jurídica dos diversos participantes, cada um deles vai possuir uma chave pública e outra privada. Segundo ZHEN[147], a típica assinatura digital envolve duas fases: primeiramente, a assinatura, e posteriormente, a verificação. No exemplo trazido na obra, os autores explanam que primeiro o utilizador gera um código *hash* derivado da transação que ele deseja assinar. Em seguida, deve-se cifrar o *hash* utilizando a chave privada e mandar para outro utilizador o *digest* cifrado. O receptor vai averiguar a transação pela comparação do *hash* decifrado (usando para tanto a chave pública do emissor) com o *hash* derivado dos dados recebidos.

E dentre essas propriedades criptográficas basilares, vale mencionar que a *blockchain* pode utilizar a criptografia de curva elíptica para viabilizar a assinatura digital, o que segundo JOHNSON et al[148], corrobora um desígnio de segurança no registro de transações na rede, uma vez que permite ao participante guardar um conhecimento secreto (a chave privada), ao publicar um enigma (a chave pública) preservando a informação confidencial.

Além disto, tendo em vista que haverá uma espécie de "ciclo de vida"[149] de um registro, consoante GREVE, uma fase prévia inerente precisa acontecer antes que o *node* "assine" um registro a ser inserido na *blockchain*, qual seja uma pré-validação, na qual se autentica o certificado de transação, verifica-se a assinatura do certificado de transação incluído na operação e, não obstante, averígua-se caso a transação não é repetida.

Não esgotada, porém devidamente apresentada a questão da arquitetura, acredita-se ser relevante trazer características que tornam a *blockchain* um conceito único, mas ao mesmo tempo flexível, por poder adotar vários formatos. Por isso, as características da *blockchain* serão pilares da investigação e junto com a arquitetura adotada serão objetos de investigação para saber os desígnios da cadeia de blocos, sob o prisma da Proteção de dados pessoais.

---

[146] Survey on Blockchain Technologies and Related Services FY2015 Report. Ibid.

[147] Zheng, Zibin et al. "Blockchain challenges and opportunities: A survey". International Journal of Web and Grid Services, vol. 14, n. 4, 2018. p. 352-375.

[148] Johnson, D.; Menezes, A.; Vanstone, S. "The elliptic curve digital signature algorithm (ECDSA)", International Journal of Information Security, vol. 1, n. 1, 2001. pp.36–63.

[149] Greve, Fabíola, et al. Ibid. p.30

2.4. Principais Características Da Blockchain

Diante da evolução histórica e diante de sua arquitetura concebida, é preciso eleger algumas características da *blockchain* que servirão para os desdobramentos da presente investigação. E por isso, as primeiras características listadas são a descentralização[150] e desintermediação[151]. Conforme já foi dito, o que é comum aos sistemas tradicionais centralizados é o facto de que cada transação precisar de ser validada através de uma terceira parte, ou entidade de confiança, como, por exemplo, um Banco Central. Esta característica comumente encerra em si duas expectativas: i) desde logo que, ao retirar a participação de terceiros intermediários, o registro passará a ser diretamente validado pela própria plataforma, determinando que os custos caiam[152]; ii) a outra razão diz respeito à segurança, já que, ao não existir um "alvo" apenas para ser atacado, a *blockchain* permite uma conquista de maior confiança já que assenta no pressuposto de "dividir para conquistar".

A rede P2P (*peer-to-peer*), de acordo com JÍMENEZ[153], permite a desintermediação, afinal cada um dos integrantes funciona como uma entidade de confiança autônoma por si só. E a noção de que a *blockchain* permite a interação entre os pares autônomos, somada com a dispensa da presença da figura de um terceiro de confiança, segundo GONÇALVES E CAMARGO[154], só se torna possível pela própria arquitetura do sistema. Para os autores, os componentes do sistema e como eles interagem entre si proporciona maior fluidez nas relações, assim como um rol praticamente inesgotável de utilizações.

E o fato de descentralizar será bastante explorado nos capítulos seguintes quando o escopo vai ser o de pensar a *blockchain* ao serviço de uma administração pública que se pretende mais transparente. Afinal, historicamente, os registros centralizados são realizados através de agentes / órgãos públicos que oneram o Erário público sob a cátedra de se poderem reputar como um terceiro

---

[150] Zheng, Zibin et al. Ibid. p. 352-375.

[151] Significa "*several copies of the Blockchain coexist on different computers*", conforme definido em Ramos, Luis Felipe M.; Silva, João Marco C. "Privacy and Data Protection Concerns Regarding the Use of Blockchains in Smart Cities". Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV2019), Melbourne, VIC, Australia, 2019.

[152] Fala-se em "custos de monitoramento, fiscalização e de liquidação caem significativamente". Para aprofundar neste tema: Valle, Daniel. Blockchain e o mercado da música. Diss. Pontifícia Universidade Católica Do Rio De Janeiro.

[153] Jiménez, María Nieves Pacheco. "Criptodivisas: del bitcoin al MUFG. El potencial de la tecnología blockchain." Revista Cesco de derecho de consumo, vol. 19, n. 7, 2016.

[154] Gonçalves, Pedro Vilela Resende; Rafael Coutinho Camargos. "Blockchain, Smart Contracts e "Judge as a Service" no Direito Brasileiro". II Seminário Governança das Redes e o Marco Civil da Internet: globalização, tecnologias e conectividade. Belo Horizonte: Instituto de Referência em Internet e Sociedade-IRIS, 2017. pp. 207-212.

de confiança investido do poder estatal para validar transações por eles armazenadas, e é neste processo que a corrupção pode acontecer.

De maneira diversa, a transação na *blockchain* pode ser conduzida de forma direta pelos *nodes*. Não existe agência centralizadora para autenticar o registro, e esta característica aventa a possibilidade de a *blockchain* oferecer uma implementação, na perspectiva da Fazenda Pública, que ofereça menos custos (sobretudo de agentes públicos a serem contratados), bem como quanto aos custos de manutenção a partir do momento que não demanda criação de instituições inteiras apenas para manter registros estatais e declarar a existência de transações.

A outra característica possível acaba por decorrer da mencionada descentralização que é a resiliência do sistema[155]. A resiliência decorre de como é desenvolvida a estrutura para fins de evitar alterações não desejadas. MYLREA et al[156] associam a referida característica ao fato dos registros poderem ser submetidos e votados por toda a rede, assim como de a versão final deste registro ter de estar na posse simultânea de todos os nodes do sistema. E é por isso que a descentralização torna a *blockchain* resiliente, dificultando a observância de uma violação do sistema. Em uma base de dados centralizada, o atacante precisa aceder ao controle central para conseguir adulterar e / ou deletar dados, e quem não possui acesso a esse poder central fica à mercê do tempo em obter resposta sobre algum dado específico.

Mesmo que a *blockchain* seja "permissionada"[157], apesar da hierarquia entre *nodes*, o registro vai estar descentralizado na rede e cada outro *node* possui uma cópia simultânea. Em outras palavras, cada bloco é divulgado (em *broadcast*) para outros *nodes* que seguem o protocolo do consenso para inserção de um novo bloco na cadeia. E neste conceito em que, se o registro individual for alterado, os outros acusam a violação e putativas falsificações tornam-se mais facilmente detectáveis.

Nas palavras de ZHENG, uma vez que as transações estão espalhadas através da rede e a validação envolve diversos *nodes*, segundo o autor, resta "praticamente impossível de adulterar"[158]. E essa dificuldade propositalmente criada é que ilustra a resiliência do sistema, que de uma maneira geral conceitua a capacidade de alguma entidade voltar ao seu estado normal depois de ter sido tensionado. Se a ameaça pode ser gerada pelo atacante na *blockchain*, o estado normal garante que ele superará o ataque e não abalará seu suposto funcionamento. E indo além, há autores que

---

[155] Mylrea, Michael; Sri Nikhil Gupta Gourisetti. "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security." 2017 Resilience Week (RWS), IEEE, 2017.

[156] Ibid.

[157] Tradução adotada majoritariamente para "*permissioned*". Neste sentido, Moraes, Juliana Moreira. "Blockchain e o compartilhamento de dados na esfera da administração pública federal brasileira: análise do bCPF". Universidade de Brasília. 2019.

158 Zheng, Zibin et al. Ibid. p. 352-375.

classificam a verdadeira resiliência, natural à *blockchain*, como a capacidade de operar em face de condições adversas, o que acaba por ser mais amplo e abranger as ameaças causadas por interações humanas indesejáveis[159].

Outra característica eleita, e útil para as discussões posteriores, é a possibilidade de anonimização. Esta propriedade permite que os *nodes* interajam entre si através de um endereço único gerado, específico para a rede baseada na *blockchain*. A mesma pessoa individual e coletiva por trás daquele endereço pode criar vários para evitar que sua identidade seja exposta, então o endereço é um possível identificador único[160]. E se vão ser expostos aparentes conflitos entre as normas do RGPD com a tecnologia *blockchain*, essa característica acaba por trazer uma nova faceta, muitas vezes despercebida: a partir do momento que se estabelece um registro distribuído e descentralizado, a privacidade das transações pode ser garantida caso apenas entidades autorizadas detenham as informações particulares dos utilizadores.

À luz do conceito de dado pessoal para fins de enquadramento no Regulamento do endereço como identificador único, a *blockchain* precisa ser entendida desde já como uma tecnologia desintermediada no registro, o que pressupõe a ausência de uma entidade central com dados pessoais e, *in re ipsa*, a não existência de uma controladora para fins legais, no formato dos bancos de dados mantidos por responsáveis pelo tratamento ou subcontratantes diretos.

De acordo com a explicação de CHICARINO[161], o uso de *blockchain* significa conferir anonimidade em sistemas de armazenamento de dados distribuídos, ou seja, mesmo que, ao mesmo tempo confira controle de acesso, a tecnologia em questão consegue ser um instrumento de anonimidade e confidencialidade (não do que é registrado que obedece à transparência, mas a personalidade jurídica por trás do respectivo *node*). Logicamente que a anonimidade provida pelo *blockchain* não é absoluta, por isso ela é denominada de "pseudo-anonimidade"[162], pelo que vai ser possível, em determinadas circunstâncias, desanonimizar o responsável legal pelo registro.

E por fim, foi elegida outra característica da auditabilidade para ainda definir a *blockchain*, já que cada bloco é validado e registrado com sua devida *timestamp*, na qual os utilizadores (ou quem quer que tenha o direito) podem facilmente verificar e rastrear os blocos anteriores. Assim, a questão passa por definir se quem participa da rede é sempre identificável através de seu endereço único para

---

[159] Rieger, Craig G.; David I. Gertman; Miles A. McQueen. "Resilient control systems: Next generation design research." 2009 2nd Conference on Human System Interactions. IEEE, 2009.

[160] O endereço é apenas umas das formas de identificação de pessoas singulares na *blockchain.*

[161] Chicarino, V. R., et al. Ibid. "Uso de blockchain para privacidade e segurança em internet das coisas." VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Brasília: SBC, vol. 28, 2017.

[162] Chicarino, V. R., et al. Ibid.

fins de proteção de dados. Conforme ZHENG[163], cada transação pode ser rastreada interativamente e isso contribui para fins de responsabilização e de transparência dos dados armazenados na *blockchain*.

Parte da doutrina associa a *accountability* da *blockchain* à sua própria estrutura. Para CHICARINO[164], uma vez que somente os utilizadores que possuem as chaves privadas podem realizar transações, os registros acabam por ser auditáveis. No exemplo da atuação das entidades de validação, encontra-se a evidência que existe forma de controlar e auditar as comunicações e prover controle de acesso entre os dispositivos num livro-razão distribuído, tornando os registros virtualmente inapagáveis e inalteráveis, perenemente auditáveis.

2.5. O Protocolo Do Consenso

O já mencionado protocolo é conceito relevante dessa tecnologia que buscou alguma forma descentralizada de decidir, a exemplo de diversos usos conhecidos da *blockchain* que utilizam o voto da maioria como uma forma de realizar transações e confirmá-las. Para explicar a conceção aqui apresentada, a forma de atingir o consentimento entre partes (que não se conhecem ou não confiam no outro) buscou beber da fonte de uma antiga alegoria que explica bem como as relações das partes de um sistema precisam se entender a fim do correto funcionamento do todo: o Problema dos Generais Bizantinos[165].

Neste problema, um grupo de generais organizaram um cerco ao redor de uma cidade, entretanto precisam atacar de uma só vez e em conjunto, caso contrário o ataque irá falhar. Para tanto, os generais precisam se comunicar e chegar a um acordo do momento exato de atacar, todavia não conseguem se comunicar diretamente, precisando mandar mensagens e comandos por mensageiros através da cidade. Visto que os líderes não estão em comunicação direta, o conteúdo da mensagem pode ser alterado e chegar um comando para atacar em dia e hora errado, o que resultaria na derrota. Eis que se deparam com um ambiente sem confiança para se obter consenso, problemática central que a *blockchain* visa suplantar.

Em outras palavras, a metáfora dos generais bizantinos ilustra, de forma prática, a dificuldade de obter o consenso distribuído[166]. E esta é uma problemática que acompanha os sistemas de

[163] Zheng, Zibin et al. Ibid. p. 352-375.
164 Chicarino, V. R., et al. Ibid.
[165] Lamport, L.; Shostak, R; Pease, M. "The byzantine generals problem" ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, n. 3, 1982. pp.382–401
[166] Para aprofundar, ver obra de Cardoso, Bruno Campos. "Algoritmos como 'máquinas de cultura': Notas sobre política e produção de consenso no sistema peer-to-peer Bitcoin." Anais da ReACT-Reunião de Antropologia da Ciência e Tecnologia, vol. 4, n. 4, 2019.

processamento descentralizados, seja um exército, seja uma base de dados distribuída. O escopo principal, nesta senda, seria alcançar a confiabilidade geral do sistema, sob a inexistência de processos defeituosos, afinal a recomendação é que exista concordância entre os *nodes* sobre dados ou valores na computação. Por isso, seja seguir a ordem de um líder no contexto de uma guerra, ou confirmar uma transação, aplica-se a lógica do consenso distribuído e o desafio de obtê-lo em um ambiente sem confiança entre as partes. De acordo com CARDOSO[167], este consenso distribuído corresponde a uma produção coletiva que envolve movimentações e balanços da rede baseados em algoritmos, que criam uma rede de regras transacionais definidas e, sobretudo, dispensa autoridades reguladoras centrais.

E, visto o problema, a *blockchain* insere-se em tal contexto por não existir nenhum *node* central para assegurar que os registros distribuídos são sempre iguais, com objetivo de assegurar a uniformidade do sistema. Para solucionar a questão, existe o acima denominado "protocolo de consenso", cuja utilização serve para sedimentar a confiança, mesmo onde ela não há. O fato de o dado ser interligado de forma criptografada a outros blocos, qualquer alteração fica perceptível e as novas inserções precisam passar pelos demais utilizadores da rede, o que faz recair no protocolo de inclusão de novos registros a responsabilidade para assegurar a confiança. A relação do consenso com a inserção de um novo bloco fica evidente na doutrina de GREVE[168], cujo contributo visa definir o consenso como fator crucial em algum problema que exista a necessidade de acordo, o que lhe torna propriedade seminal, afinal permite estabelecer um critério sobre a forma de agregação do próximo bloco à cadeia.

Na *blockchain*, a validação de um novo bloco vai obedecer a regras pré-estabelecidas. Os ditames do protocolo de consenso vão ser o paradigma para eleger qual segmento de eventuais bifurcações da cadeia é o verdadeiro. E é por este procedimento que as decisões sobre o que será inserido na *blockchain* não dependem de autoridade centralizadora, pois os participantes obedecem a um protocolo prévio com regras de inclusão/validação, assegurando independência e descentralização do registro.

Sobre a independência em respeito a um ente centralizador, interessante a linha de CHRISTIDIS et al, que identificam a *blockchain* como algo sem precedentes, afinal os diversos usos que antes precisavam de um intermediário de confiança, agora possuem uma arquitetura descentralizada sem autoridade central que "alcança a mesma funcionalidade e oferece a mesma

[167] Ibid
[168] Greve, Fabíola et al. Ibid.

quantidade de certeza" [169]. Apesar de os sistemas de registro distribuídos não serem conceitos recentes, os autores pretenderam ressaltar que a finalidade é alcançada, apesar de caminhos diferentes serem utilizados.

Cada utilizador, por si só, tem a capacidade de verificar cada bloco ou o conjunto; os *nodes* não precisam se conhecer para criar uma relação de confiança. Na realidade, a verificação ocorre entre o próprio utilizador perante o registro *per si;* afinal eles participam da "votação" em busca do consenso e confiam na segurança criptográfica adjacente ao registro, ou seja, a confiança surge da própria *blockchain*. Corroborando esta visão, ROMANINI já definiu que "a confiança é dada pela própria tecnologia"[170], e esta tecnologia está diretamente associada a um sistema de geração de consenso entre os utilizadores, cuja veracidade ou não de uma transação ou informação poderá ser averiguada. Segundo o autor, este sistema é justamente a "confiança sem confiança"[171].

Os protocolos de consenso visam solucionar processos defeituosos que, justamente, podem inviabilizar o sistema como um todo, e por isso existe uma lista de requisitos que normalmente são buscados para tornar o protocolo utilizável. O processo ocorrerá sem defeitos se na execução não apresentar nenhuma falta, ou então as faltas que, porventura, apareçam sejam toleráveis.

Assim, é pertinente mencionar alguns requisitos para o protocolo de consenso:

- precisa haver um término, cujo sinal é a escolha de um valor pelos seus agentes/processos;

- posterior validação é requerida, quando todos os agentes propõem o mesmo valor, é suposto que todos os processos não defeituosos devem seguir este mesmo valor;

- a terceira faceta é a integridade, cujo entendimento é que todo processo não defeituoso deve escolher um valor máximo que é interligado à quarta faceta do acordo, na qual todo processo não-defeituoso concorda com o mesmo valor.

Em resumo, a *blockchain* consegue respeitar os 4 pilares dos protocolos de consenso, afinal mesmo que a cadeia se divida (conforme será visto), acaba prevalecendo a cadeia "em *fork*" mais autêntica[172]. A *blockchain* oferece também a posterior validação pelo próprio sistema que, em dado momento, retira dados não autênticos e garante mais certeza matemática a cada bloco. A integridade é um dos pontos fortes da estrutura pensada para o próprio bloco, na qual as falhas não são toleráveis pelos pequenos detalhes e sequências numéricas dentro do próprio bloco, como acontece com o

[169] Christidis, Konstantinos et al. Ibid. p. 2295. Tradução livre

[170] Romanini, Anderson Vinicius; Márcia Pinheiro Ohlson. "De elos bem fechados: o pragmatismo e a semiótica peirceana como fundamentos para a tecnologia blockchain utilizada no combate às fake news." São Paulo: Communicare, 2018. p. 66

[171] Tradução livre de "trustless trust". Veja-se Romanini, Anderson Vinicius et al. Ibid. p. 66

[172] Baliga, Arati. "Understanding blockchain consensus models." Persistent, vol. 4, 2017. pp. 1-14.

timestamp[173], e ainda a relevante assinatura criptográfica do bloco anterior, por força do parentesco entre os blocos.

Ante o exposto, existem diversos protocolos de consenso que podem ser utilizados, e a definição da espécie de protocolo também será relevante para a averiguação do próximo capítulo acerca da conformidade da *blockchain* com o RGPD, afinal é de grande relevância ter a ciência de como os dados a serem registrados estão sendo validados e por quem estão sendo validados, a fim de determinar qual "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais"[174], ou seja, quem poderá ser definido como responsável pelo tratamento.

Primordialmente, o protocolo adotado foi o *Proof-of-work* (que será designado PoW). Nesta "prova de trabalho", o protocolo provoca uma competição matemática entre os *nodes* ligados à *blockchain*, no qual o objetivo é saber qual será o primeiro a encontrar um *hash* respectivo ao novo bloco, considerando a dificuldade imposta de tentativa por força-bruta. Calha de ser uma competição em que o trunfo é possuir poder computacional: com mais poderio computacional, maior a probabilidade de validar um novo bloco. Esta foi a lógica adotada por NAKAMOTO na conceção do Bitcoin, criando a figura do minerador, elemento que irá submeter a equação resolvida ao consenso da maioria para o fim de inserir o bloco na cadeia, e em troca receberá um percentual (que no caso da Bitcoin, tem valor financeiro). Nesta conceção, foi pensado inclusive em um algoritmo de "ajuste de dificuldade", para regular a chamada oferta de poder computacional – a *hash rate*[175] - que funciona como um termômetro de incentivo
econômico ao esforço de validação dos *nodes*.

O PoW é uma estratégia de consenso usada pela rede Bitcoin, idealizada no *paper* base por NAKAMOTO de 2008[176]. Como já foi dito, o protocolo exige um complicado processo computacional de autenticação, a partir da noção de que cada *node* da rede poderá calcular o código *hash* que consta no cabeçalho do bloco, e disso, decorre um resultado que precisa ser igual que determinado valor. Em outras palavras, os validadores vão calcular continuamente, usando o respectivo *nonce*, cuja marca será a prova para demonstrar que o cálculo foi correto e será confirmado pelos outros *nodes*, evitando assim que um novo bloco seja validado em fraude.

---

[173] Li, Yang, et al. Ibid.
[174] União Europeia. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid.
[175] Veja-se em: Cardoso, Bruno Campos. Ibid.
[176] Nakamoto, Satoshi. Ibid.

E partindo disto, o resultado do cálculo vai ser considerado um resultado autêntico, e nesta relação em que um *node* faz todo o cálculo do *hash*, o processo se chama *mining* e o *node* vencedor será designado de validador. Em resumo, cria-se propositadamente uma complexidade no processo de resolução de um desafio criptográfico, que será resolvido através de poder computacional, e à entidade que o resolver, dar-se-á o direito de inserir um novo bloco na cadeia, por este trabalho que o PoW carrega este nome.

Como o procedimento descrito é descentralizado, é possível que vários blocos possam ser gerados simultaneamente, quando vários validadores acham o *nonce* adequado praticamente ao mesmo tempo. Em resultado disto, a mesma cadeia pode abrir várias bifurcações possíveis, sendo matematicamente improvável que duas vertentes distintas gerem o próximo bloco simultaneamente, por isso que no protocolo do PoW, a cadeia que se tornar mais longa é julgada como a mais autêntica. Mesmo diante do fato dos validadores atuarem em dois "*forks*" diferentes, cada novo bloco será inserido em ambos *forks* e o sistema vai acabar seguindo o *fork* maior, por matematicamente apresentar maior probabilidade de ser a sequência mais autêntica. Segue esta lógica a doutrina de ZHEN[177], cuja defesa é que seria improvável que dois *forks* competidores pudessem gerar o mesmo bloco simultaneamente, por isso que o autor corrobora o pensamento de que "a cadeia que se tornar mais longa será julgada a autêntica"[178].

E a noção de trabalho vem exposta pelo tempo e dificuldade de validar uma transação, e é por isso que no modelo deste protocolo específico, utilizou-se um mecanismo de incentivo, a saber um prêmio de uma pequena porção do ativo financeiro que é transacionado naquele sistema, no caso, a criptomoeda. E esta relação de dificuldade proposital veio bem explicada na obra de BUTERIN[179], na qual autor explica que a presença do, já mencionado, *hash* SHA256 em cada bloco, representado por uma sequência de 256-bit, acaba oferecendo um alvo diretamente ajustável, ou seja, intencionalmente feito para ser computacionalmente difícil. O *hash* SHA256 é aleatório, sendo a forma de validar um bloco, o antigo método da tentativa e erro (levando em conta o *nonce*, mas conferindo se o novo *hash* confere)[180].

BUTERIN apresenta alguns números que demonstram a experimentação forçada no processo de validação. Quando o autor averiguou, precisava-se de 264 tentativas, mas a certa quantidade de blocos a média de dificuldade será recalibrada, levando em conta o tempo que ficará em torno de 10

[177] Zheng, Zibin et al. Ibid. p. 359
[178] Ibid. P. 359. Tradução livre.
[179] Buterin, Vitalik et al. Ibid.
[180] Mackenzie, Donald. Ibid. p. 7

minutos para cada bloco novo. Este ato de recalibragem da rede explica a definição do autor em falar da existência de um alvo ajustável. A flutuação do nível de dificuldade torna-se uma rentável indústria quando os *nodes* que validam, denominados validadores na *blockchain*, são compensados pelo já denominado esforço computacional variante, com retribuição na moeda da própria plataforma, ou ainda quando a mesma transação pode possuir diferentes denominações, fazendo que a diferença também seja direcionada ao minerador como uma taxa de transação[181].

Outra forma de pensar, seria o *Proof-of-Stake* (PoS), cuja validação de novos blocos ocorre em decorrência da participação de ativos digitais, e responde a uma proporcionalidade entre recompensa e peso dos votos, cujo valor será atribuído à quantidade de ativos de cada participante. Nos ensinamentos de KIAYIAS et al., ao invés de mineradores investindo em recursos computacionais para participar de um processo para "eleger um líder" [182], o PoS executa uma função para eleger aleatoriamente um *node* que irá validar o registro ou transação e receber uma recompensa proporcional à sua participação.

A quantidade de ativos reunidos acaba por demonstrar a lógica deste protocolo. Em outras palavras, o que foi dito é que, na tentativa de afastar o alto processamento computacional em uma corrida para incluir blocos na cadeia, o ente validante provavelmente será aquele que mais investir nos ativos do sistema. Sequer existe criação de ativos, tudo já fora criado e a prova de participação é diretamente proporcional à fração de moedas que se possui, no contexto da criptoeconomia. SALEH defende que o PoS em substituição ao PoW destina-se a criar um sistema *blockchain* sem desperdícios de energia, por isso que, para o autor é uma verdadeira alternativa adotar o protocolo baseado na participação e não no esforço/trabalho.[183]

Um dos problemas identificados do protocolo PoS é referente ao processo de eleger um líder, acima mencionado. Na simulação de eleição, para que esta seja justa e aleatória entre as partes interessadas, KIAYIAS et al[184] identificam que complexidade deve ser introduzida no processo, a gerar a dificuldade computacional já debatida, entretanto, o que acaba por ser um cenário de possível manipulação pelo adversário. Os autores exemplificam com a circunstância de que um adversário que controle um conjunto de partes interessadas, existe uma chance de tentar simular a execução do protocolo tentando diferentes sequências com escopo de encontrar uma continuação de protocolo que

[181] Neste sentido, veja-se Buterin, Vitalik et al. Ibid.
[182] Kiayias, Aggelos, et al. "Ouroboros: A provably secure proof-of-stake blockchain protocol." Annual International Cryptology Conference. Springer, Cham, 2017. p.1
[183] Neste sentido, veja-se: Saleh, Fahad. "Blockchain without waste: Proof-of-stake". SSRN 3183935, 2020.
[184] Kiayias, Aggelos, et al. Ibid.

favoreça as partes adversárias. Esta abertura conduz a uma vulnerabilidade denominada "*grinding*"[185], na qual os adversários podem usar recursos computacionais com intuito de influenciar a eleição do líder.

Outro modelo seria o DPoS - *Delegated-Proof-of-Stake* – no qual vai ocorrer uma participação delegada, mesmo que o protocolo seja similar ao PoS, os participantes não irão votar diretamente na validade do novo bloco; neste caso serão eleitos delegados para promover a validação em nome dos participantes. Na definição em WENTING et al.[186], o DPoS segue a lógica proposta pelo Bitshares[187], na qual neste protocolo, primeiramente vota-se em um grupo de "testemunhas" ou delegados que irão validar e gerar novos blocos de forma escalonada e segmentada.

Apesar de terem sido desenvolvidos os protocolos acima, que sequer esgotam os diversos outros protocolos de consenso existentes, um esquema passa a ser explicado, a fim de que oferecer soluções de privacidade no uso da *blockchain*, sobretudo no momento do registro das transações na cadeia, nomeadamente o *Zero-knowledge proof* (ZKP).

2.6. Como Provar Sem Conhecimento

Entretanto, vislumbrando a evolução desta investigação que vai culminar em expor usos em conformidade da *blockchain* com o RGPD, um protocolo sinaliza uma possível solução para a dificuldade de se validar um registro ou transação, sem ter acesso aos possíveis dados pessoais que, porventura, estejam inseridos no bloco. Ao definirem a *blockchain* como uma plataforma a todos aberta[188], inclusive para atacantes, LEI XU *et al* buscam nos seus termos, mitigar a problemática da privacidade e propor um sistema *blockchain* que apresente o *zero-knowledge scheme*[189]. Frisa-se que esta prova de conhecimento-zero, seguindo a tradução comumente adotada[190], oferece uma forma de validação sem focar no conteúdo em si, conforme será explicado.

---

[185] Kiayias, Aggelos, et al. Ibid.

[186] Li, Wenting, et al. "Securing proof-of-stake blockchain protocols." Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, Cham, 2017. pp. 297-315.

[187] Schuh, F., Larimer, D.: Bitshares 2.0: General overview. Disponível em http://docs.bitshares.org/downloads/bitshares-general.pdf, acesso em 02/05/2020.

[188] Notadamente se referem às blockchains públicas e não às permissionadas.

[189] Xu, Lei, et al. "Enabling the sharing economy: Privacy respecting contract based on public blockchain." Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. Springer, Cham, 2017. Tradução livre.

[190] Neste sentido: Ribeiro, Vinicius G.; Rafael Campello; Raul F. Weber. "Mecanismos de conhecimento zero empregados por esquemas de chave pública." 30ma Conferencia Latinoamericana de Informatica (CLEI2004), 2004. & Zago, Anselmo, Mateus P. Dias, and Guilherme Pagotto. "Whitepaper do Marketplace de Aplicativos de Economia Compartilhada", 2017.

A priori, o *zero-knowledge proof*[191] (ZKP ou prova de conhecimento zero) possibilita uma parte provar para outra que uma declaração (geralmente matemática) é verdadeira sem, contudo, revelar qualquer coisa além da veracidade da declaração. Segundo QUISQUATER[192], este é um conceito explicável por alegoria, cujo, assim como o exemplo mencionado dos generais bizantinos, o protocolo ZKP pode ser compreendido através de uma metáfora da caverna. O autor cria um cenário de dois personagens, um provador da declaração (chamado de P) e o verificador da declaração (denominado V). Primeiro as partes vão rotular os caminhos da caverna como A e B, ficando o V do lado de fora e P entra na caverna tomando aleatoriamente um dos caminhos. Se V gritar o nome de um caminho, escolhido aleatoriamente para que P retorne, se este P realmente souber o segredo, basta abrir a porta e retornar ao longo do caminho desejado (registre-se que o V não sabe o caminho em que P entrou). A questão é que, se V fizer uma única vez o teste, a chance de P acertar o caminho sem saber o segredo é de 50%, entretanto se este teste for repetido várias vezes, as chances de P sair pelo caminho correto e ser bem-sucedida, sem ter ciência do segredo, são improváveis.

Ante o exposto acima, se o provador sair do teste pelos caminhos escolhidos pelo verificador, este poderá concluir que provavelmente aquele sabe o segredo. É, de certa maneira, uma forma de provar que sabe algo sem revelar o conteúdo daquilo que se sabe. E este esquema não corresponde a sequer algo novo da ciência informática, a doutrina já desenvolve a ZKP desde a década de 1990, dentre a qual autores como GOLDREICH et al.[193] na época já o consideravam um importante modelo criptográfico. De fato, estudiosos da privacidade acabam por ficar atentos às potencialidades do ZKP, afinal uma parte pode convencer outrem da exatidão de uma declaração, sem sequer saber os detalhes da mesma. De acordo com LEI XU[194], neste protocolo, o verificador não poderá aprender nada, exceto o fato de a afirmação ser verdadeira (por isso, que se fala em conhecimento zero).

Inclusive no contexto das criptomoedas, apesar de não ser transversal a todas *blockchains*, o ZKP já vem sendo utilizado por alguns paradigmas que clamam oferecer uma solução na verificação de registros e transações de maneira anônima. De acordo com MIERS et al[195], a Zerocoin serve de

191 Que vem sendo traduzido como "Prova de conhecimento zero" para autores como Ribeiro, 2004, ibid; ou, como "Prova de conhecimento nulo" para autores como Silveira, Alexandre Marques Albano da. "Prova de conhecimento nulo baseada em isomorfismo de subgrafos". Universidade Federal do Ceará. 2015.

192 Quisquater, Jean-Jacques; Louis C. Guillou; Thomas A. Berson. "How to Explain Zero-Knowledge Protocols to Your Children". Advances in Cryptology - CRYPTO '89: Proceedings, v.435, 1990. pp. 628-631.

193 Goldreich, O.; S. Micali; A. Wigderson. "Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems". Journal of the ACM (JACM), vol. 38, n. 3, 1991. pp. 690–728.

194 Xu, Lei, et al. "Enabling the sharing economy: Privacy respecting contract based on public blockchain." Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, 2017. Tradução livre.

195 Miers, I.; Garman, C.; Green, M; Rubin, A.D. "Zerocoin: Anonymous distributed e-cash from bitcoin" Proceedings of IEEE Symposium Security and Privacy (SP), Berkeley, EUA, 2013. pp.397–411

paradigma no uso do *zero-knowledge proof* na *blockchain*. Neste caso, os entes validadores não precisam validar a transação baseados na assinatura digital, mas sim autenticar registros através de uma lista pré-definida de moedas válidas. No esquema adotado por esta empresa, não existe ligação entre o pagamento original e os registros, o que impossibilita a análise do conteúdo das transações e, por conseguinte, uma vinculação pessoal dos dados registrados. Este exemplo ilustra um uso da *blockchain* que se preocupou em adotar o esquema ZKP para fins específicos.

Apesar de uma tentativa de respeitar a privacidade, a Zerocoin acaba por revelar algumas informações no processo de validação, conforme explanado acima. Esta questão parece ser observada, segundo SASSON et al., pela Zerocash, cuja marca registrada é o protocolo zk-SNARKs, "*zero-knowledge Succinct Non-interactive Arguments of Knowledge*"[196], cujo fator diferencial é justamente ocultar o montante das transações a serem registradas, diferentemente da Zerocoin, somado ao fato de que os valores das moedas em posse dos utilizadores também permanecem sem serem revelados.

De outro lado, mas de maneira suplementar, outra ferramenta criptográfica que é debatida na busca de uma validação, sem exposição total da informação, é o *Commitment scheme* ou esquema de comprometimento. Na doutrina clássica sobre esta ferramenta criptográfica, o comprometimento poderá ser inclusive um complemento a ser utilizado no protocolo ZKP. O comprometimento é usado como prova de conhecimento no ZKP, a fim de permitir que o provador (P) participe de provas de "dividir e escolher"[197], nas quais o verificador (V) vai ser introduzido a uma escolha do que aprender, revelando apenas o que corresponde à escolha do verificador. Nos ensinamentos de GOLDREICH et al.[198], os esquemas de compromisso permitem que o provador especifique todas as informações com antecedência e apenas revele o que deve ser revelado posteriormente na prova.

Todavia, o *Commitment scheme* não apenas serve para o provador, mas também para o verificador, o qual geralmente específica suas escolhas de forma antecipada ao comprometimento. E foi a conclusão que GOLDREICH chegou em obra posterior[199]: as provas mediante o *Zero-knowledge proof* podem ser feitas em paralelo, através do comprometimento criptográfico de ambas as partes, qual seja no exemplo o provador (P) e verificador (V). Os compromissos serão firmados de maneira simultânea e, mais importante, sem revelar informações adicionais.

---

[196] Sasson, E.B.; Chiesa, A.; Garman, C. et al. "Zerocash: Decentralized anonymous payments from Bitcoin". Proceedings of 2014 IEEE Symposium on Security and Privacy (SP), San Jose, EUA, 2014. pp.459–474.

197 "*Cut and choose*"

[198] Goldreich, Oded; Silvio Micali; Avi Wigderson. "Proofs that yield nothing but their validity, or all languages in NP have zero-knowledge proof systems" Journal of the ACM, vol.38, n. 3, 1991, pp. 690–728.

[199] Goldreich, Oded; Hugo Krawczyk. "On the Composition of Zero-Knowledge Proof Systems" SIAM Journal on Computing, vol. 25, n. 1, 1996. pp. 169–192.

Relevante trazer ainda uma explicação que fragmenta o processo do esquema de comprometimento, o que o torna mais lógico. Segundo DI CRESCENZO et al.[200], haverá duas partes relacionando-se através de algoritmos probabilísticos: a primeira fase estabelece determinado valor v, executa o *commit* para firmar o compromisso e envia-o à parte contrária. A segunda parte resulta da atuação da parte comprometida em compartilhar ações extras e o receptor da mensagem executar um *reveal* para confirmar o valor v. A privacidade da informação decorre desta duplicidade, afinal (i) no primeiro momento, quem recebe o compromisso não poderá descobrir o valor de v; (ii) no segundo aspecto acerca da vinculação, quem firma o compromisso do valor v, não poderá alterar para v' após a primeira fase, conforme preceituou FISCHLIN[201].

A criptografia pode oferecer ferramentas diversas para fins múltiplos; aliás, o modelo pensado para Bitcoin não é sequer o único no âmbito das criptomoedas, muito menos no que tange à *blockchain* que é mais ampla. Recursos informáticos que sejam adotados por um sistema devem corresponder com os desígnios legais de quem comanda ou decide por aquele conceito, em outras palavras, a escolha do protocolo de validação na *blockchain* é uma decisão de quem a desenvolve, por ser um acordo pré-estabelecido. Trazer as diferenças de protocolo e as funcionalidades dos esquemas de comprometimento, ou a forma de provar algo sem saber o conteúdo, são alguns dos vários recursos que o conceito da *blockchain* oferece. Uma pluralidade de nuances que vão ser cruciais para pensar em modelos que respeitem os direitos fundamentais da privacidade e Proteção de dados uma vez que o modelo adotado por NAKAMOTO, na Bitcoin, passou pela *blockchain* pública, sem *nodes* com privilégios especiais, o que não acaba sendo a única forma de se pensar na cadeia de blocos.

E do debatido ZKP surge a corrida para desenvolver uma *blockchain* que respeite à proteção de dados, sob todos os ângulos, para poder ser implementada pela Administração Pública para fins de transparência. Sejam transações financeiras, sejam registros de imóveis, ou qualquer uso que se vislumbre para a *blockchain*, as informações pessoais são divulgadas de acordo com o caso específico. A exemplo do clássico sistema da Bitcoin que, apesar de ser aberto e sem privilégios, permite ao participante ocultar seu relacionamento com as identidades, segundo o próprio *whitepaper* de NAKAMOTO[202]. Dentre os sistemas considerados como mais sofisticados[203], os *nodes* envolvidos em um

[200] Crescenzo, G. Di; J. Katz; R. Ostrovsky; A. Smith. "Efficient and non-interactive non-malleable commitment". International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2001. pp.40-59.
[201] Fischlin, M.; R. Fischlin. "Efficient non-malleable commitment schemes". Annual International Cryptology Conference, Springer, 2000. pp. 413-421.
[202] Nakamoto, Satoshi. Ibid.
[203] Xu, Lei, et al. Ibid.

registro poderão ocultar o relacionamento entre si, o que acaba por ser o caso da Zerocash[204]. Tudo isso apenas corrobora o fato de que a privacidade das identidades envolvidas depende de escolhas por parte da entidade que desenvolve aquele sistema.

2.7. Regulação Da Blockchain

E a fim de finalizar a análise das peculiaridades da *blockchain* que servirão para analisar a conformidade de uso desta tecnologia com os ditames da Proteção de dados pessoais, precisa-se definir a questão da regulação para inserir registros da cadeia de blocos, ou seja, e em termos gerais, de que forma a blockchain pode "assumir diferentes níveis de permissão com diferentes categorias de participantes"[205].

Os exemplares mais conhecidos de utilização da *blockchain* talvez seja a Bitcoin e Ethereum, cujo ponto em comum se prende com as dinâmicas regulatórias associadas uma vez que, na realidade, operam como *"Permissionless blockchains"* (*blockchain* não-permissionadas ou públicas). De imediato, esta tradução pode conduzir a um dúbio sentido a respeito do termo público, afinal este decorre de *publicus*[206], e nos países de língua portuguesa este termo assume diversas facetas e sentido.

Apesar de associado ao Estado/Governo, o termo público a definir a *blockchain* não diz respeito a ser do povo, ou a ser estatal, ou contrário ao privado; na verdade, a *blockchain* pública diz respeito à existência ou não de regulação, no sentido de que elas são descentralizadas numa rede *peer-to-peer*, na qual qualquer *peer* poderá conectar ou desconectar-se à rede a qualquer momento, seja como um leitor, seja como um validador[207]. WÜST ainda julga interessante o fato da *membership* ser aberta: é uma rede de relacionamentos sem qualquer entidade central que administre quem a ela se filia, ou sequer existe algum instituto com poder de banir um *node* comprovadamente com atitude maliciosa ou que, por exemplo, tente realizar registros ilegítimos na *blockchain*.

A *blockchain* pública parte da confiança na tecnologia de maneira pura e genuína, afinal se houver algum participante tentando destruir o próprio registro, não há entidade capaz de julgar e afastar, mas o próprio *design* entropicamente seguro vai dificultar que qualquer entidade faça parte e valide as transações, a não ser que conte com um poderio computacional que consiga manipular o

---

[204] E. B. Sasson, et al. Ibid.

[205] Tradução livre para "different permission levels that different categories of participants" em RAMOS, Luis Felipe M.; SILVA, João Marco C. Ibid. p. 3

206 Do latim, "relativo ao povo"

[207] Wüst, Karl; Arthur Gervais. "Do you need a blockchain?." 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018.

quórum mínimo estabelecido para o consenso. WÜST alega, por outro lado, que essa abertura implica que o conteúdo escrito seja lido[208] e reconhece que a possibilidade de leitura por qualquer entidade pode suscitar questionamentos acerca da privacidade e proteção de dados, todavia para o autor não significa um problema, uma vez que com uso da criptografia primitiva, é tecnicamente possível estabelecer um design de '*permissionless blockchain*' que consiga ocultar informações e dados pessoais relevantes[209] sob o desígnio pensado pela *Zerocash*, já mencionada.

Noutra senda, há as "*Permissioned Blockchains*", traduzidas para "arquitetura permissionada"[210] ou "rede permissionada"[211]. A lógica que define uma *blockchain* permissionada é que se segue uma regulamentação, existe uma espécie de pré-seleção dos participantes, cujas aplicações são restringidas, conforme bem explicado em FORMIGONI FILHO et al[212] e YERMAK[213]. Em MOURA et al[214], inclusive, traça-se a diferença de regulação entre estes dois tipos de *blockchain*: se na *blockchain* pública, as chaves criptografadas de acesso ao sistema são amplamente conferidas, seja para qual for a operação (consultar a cadeia de blocos ou para realização das operações em uma rede aberta), por outro lado, na *blockchain* permissionada, a certificação dos utilizadores é controlada e existe uma obrigação de solicitar permissão para registrar.

Uma visão similar, mas que enxerga o ato de permissão em um momento anterior, é a que é trazida na obra de KARL WÜST et al[215]: ao invés de definir a rede permissionada como uma rede de autorização para transações, perspectiva o conceito sob o limitado número de participantes como o cerne desta questão. Segundo este autor, a existência de uma entidade central vai servir para decidir e atribuir o direito de as entidades virarem participantes, e uma vez atribuídos esses direitos, elas vão poder ler e/ou escrever na cadeia de blocos. Para citar exemplares que usaram este tipo de arquitetura permissionada, pode-se mencionar a Hyperledger Fabric e a R3 Corda, conforme mencionado por BROWN[216]. Relevante recordar que esta forma poderá adotar um formato híbrido, no qual os

---

[208] Wüst, Karl cita Sasson 2014. Ibid.
[209] Wüst, Karl apud Sasson 2014. Ibid.
[210] Melo Jr, Wilson S., et al. "Uso de Redes Blockchain em aplicações de Metrologia e Avaliação da Conformidade.". Disponível em https://www.researchgate.net/profile/Wilson_Melo_Junior/publication/336071460_Uso_de_Redes_Blockchain_em_aplicacoes_de_Metrologia_e_Avaliacao_da_Conformidade/links/5d8ced5892851c33e9405bb8/Uso-de-Redes-Blockchain-em-aplicacoes-de-Metrologia-e-Avaliacao-da-Conformidade.pdf Acesso em 02/04/2020
[211] Moura, Luzia Menegotto; Frick de, Daniela; Francisco Brauner; Raquel Janissek-Muniz. "Blockchain e a Perspectiva Tecnológica para a Administração Pública: Uma Revisão Sistemática." Revista de Administração Contemporânea, vol. 24, n. 3, 2020. pp. 259-274.
[212] Formigoni Filho, J. R., Braga, A. M., Leal, R. L. V. (2017). Tecnologia blockchain: Uma visão geral. Disponível em https://www.cpqd.com.br/wp-content/uploads/2017/03/cpqd-whitepaper-blockchain-impresso.pdf Acesso em 02/04/2020
[213] Yermack, D. "Corporate governance and blockchains". Review of Finance, vol. 21, n.1, 2017. pp. 7-31.
[214] Moura, Luzia Menegotto Frick de et al. Ibid.
[215] Wüst, Karl e Arthur Gervais. Ibid.
[216] Brown, Richard Gendal; James Carlyle; Ian Grigg; Mike Hearn. "Corda: An introduction". R3 CEV, 2016.

participantes podem registrar transações em cadeias de blocos paralelas, o que - para WÜST et al - é capaz de oferecer encapsulamento e privacidade para a rede[217].

Há ainda autores que reconhecem a existência de uma *blockchain* privada. Uma corrente da doutrina define a "permissionada privada", como uma vertente inserida no conceito de permissionada. Segundo MENG et al[218], a *blockchain* permissionada pode ser categorizada como pública ou privada: aqui, embora existam restrições para inserir dados na cadeia, a diferença reside no poder de ler ou não os dados da *blockchain*. Para esta classificação, no caso da permissionada pública, nem todos validam e registram blocos, mas todos podem acessar os registros; na permissionada privada, o acesso para ler os dados também resta circunscrito[219].

Dito isto, merece resgatar a recorrente questão de privacidade que emana da *blockchain*, porque é sua característica tradicional ser publicamente verificável, atributo este que permite que qualquer entidade verifique o estado do sistema e, como já foi demonstrado anteriormente, o estado de cada transação vai ser confirmada por entidades verificadoras[220], mediante um requisito de existência e manutenção do próprio sistema[221]. Apesar de ter sido explicado que os verificadores poderão ser restritos a depender do tipo da *blockchain*, apenas o fato de algum terceiro verificar registros e transações, suscitam-se questionamentos jurídicos quanto à privacidade.

Tudo resta mais evidente quando se compara com o oposto, um sistema centralizado, e WÜST explica que quem observa um sistema centralizado não precisa ver todos os detalhes, porque o sistema é baseado na confiança de uma entidade centralizadora, o que não acontece com a *blockchain*. O que ocorre é uma dicotomia, já que não existe uma centralizadora de confiança, quem observa o sistema precisa ver mais detalhes, precisa de um livro-razão mais transparente, em contraponto ao sistema centralizado onde a transparência pode ser menor, porque as entidades permutam o poder de ver detalhes, para conhecer menos e confiar mais na autoridade central[222].

Mais conhecimento não significa um problema *per si,* a questão coloca-se quando se verifica o tratamento de dados pessoais e não há uma base legal que o consubstancie.

Se a circunstância concreta recair no âmbito do RGPD, debatido no primeiro capítulo, cada propósito inserido no contexto da *blockchain*, seja o simples acesso aos registros na cadeia, seja a

---

[217] Wüst, Karl e Arthur Gervais. Ibid.

218 Meng, Weizhi, et al. "When intrusion detection meets blockchain technology: a review." Ieee Access 6, 2018. p. 10183

[219] Meng, Weizhi, et al. Ibid.

[220] Tradução para "*verifiers*"

[221] Peters, Gareth W.; Efstathios Panayi. "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money." Banking beyond banks and money. Springer, Cham, 2016. pp. 239-278.

[222] Wüst, Karl e Arthur Gervais. Ibid.

atuação da entidade validadora, precisarão atingir os padrões legais e principiológicos estabelecidos no Regulamento e no quadro jurídico primário da União Europeia.

Por isso, no capítulo seguinte são confrontados os aspectos da tecnologia *blockchain* que podem levantar problemas perante o direito fundamental à Proteção de dados pessoais, visando explorar se, e de que maneira, a *blockchain* pode ser adequada ao RGPD, para posteriormente ser pensada para uma Administração Pública mais transparente.

CAPÍTULO III

3.1 Adequação Da *Blockchain* Em Relação Ao RGPD

A partir deste capítulo, busca-se trazer a tecnologia *blockchain* desenvolvida no capítulo passado para o contexto da Proteção de dados pessoais, sobretudo para fins de conformidade em relação ao RGPD. A pertinência temática desta discussão deve-se ao fato de que ainda não existe consenso entre os Estados-Membros, ou sequer entre as Autoridades de controlo (designadas DPA), que realizam o controle e execução do Regulamento. No exato momento, existem alguns materiais oficiais de consulta, os quais serão analisados neste capítulo, para fins de consistência.

Na primeira parte, cumpre analisar o âmbito desta problemática, sabendo as particularidades de cada um dos institutos, ou seja, a natureza dos dados que são inseridos na *blockchain*, a partir de uma percepção mais detalhada da arquitetura desta tecnologia. Não obstante, resta relevante trazer as entidades que estão envolvidas e interessadas na cadeia de blocos, afinal, descrever os *stakeholders* será delimitar um universo em que o responsável pelo tratamento e o sub-contratante poderão ser identificados.

Em seguida, regras previstas no RGPD são explanadas como uma forma de enquadrar os tratamentos possivelmente provenientes da *blockchain* perante as obrigações legais, cabendo levar a cabo uma análise de tais tratamentos perante os princípios inerentes ao regime jurídico da proteção de dados, quanto à sua licitude, atendendo aos fundamentos legais para a sua consecução, aos potenciais incidentes de segurança e perspectivando a implementação da análise de risco. Não suficiente, os direitos dos titulares dos dados, sobretudo aqueles que possam criar algum conflito com as mais diversas propriedades da *blockchain,* precisam ser equacionados individualmente para fins de conformidade.

E, por fim, neste capítulo, ao chegar às respostas para a questionada escolha por um modelo de *blockchain* que ofereça providências para atender aos direitos dos titulares, pertinente é adentrar em um princípio que deve ser um norte e permear as escolhas da entidade que desenvolve a *blockchain* desde o início do seu desenvolvido, a saber proteção de dados desde a conceção e por defeito.

3.2 A Arquitetura Da Blockchain, Sob O Ponto De Vista Da Proteção De Dados

Primeiramente, conforme já foi referido, o pressuposto da *blockchain* é garantir integridade de dados através de um registro distribuído[223], em que cada cópia recai sobre cada um dos participantes da rede. A consistência e a integridade destes livros-razão dependem de duas características basilares: uma corresponde aos blocos estarem criptograficamente interligados, pelo fato de o posterior estar ligado ao anterior através do *one-way hash*; o outro fator relevante é que a confiabilidade recai no próprio sistema (tecnicamente confiável) – uma espécie de confiança no protocolo em detrimento de subordinar os participantes a uma entidade centralizadora de confiança[224]. O protocolo e as propriedades técnicas em conjunto transformam-se numa espécie de entidade fictícia, sobre a qual recai a fidúcia dos participantes, uma regra pré-estabelecida que vai permitir às partes transacionarem e registrarem entradas no sistema, sem se preocupar "quem" supostamente é responsável para validar um bloco e inseri-lo na cadeia, pois o procedimento segue regras pré-definidas[225].

Apesar de o protocolo de consenso e ligação criptográfica entre blocos constituir uma essência a ser seguida por quem desenvolve uma plataforma baseada na *blockchain*, existem outras características que acabam sendo uma escolha de componentes na constituição do sistema. A adoção do termo componentes dá-se porque o componente é uma parte da arquitetura, ou em outras palavras, a arquitetura vai resultar de uma escolha baseada na nos componentes adotados. E, por isso, devem ser considerados outros aspectos, entre os quais se pode mencionar a estrutura dos dados nos campos de dado retido no bloco; qual o tipo de protocolo que será utilizado para formar e verificar blocos[226]; que algoritmos criptográficos vão ser utilizados para garantir a autenticação e a verificação; que *design* de governança[227] constituirá regras para tecnologia e, por fim, se/como irá acontecer a troca de informações entre os participantes.

E diante desta escolha pela arquitetura que se entender ideal, cria-se um ambiente pronto para receber os mais diversos tipos de utilizadores, quais sejam partes interessadas[228], os designados "participantes" para fins de padronização de nomenclatura. Os participantes vão ser conectados através de várias motivações e podendo ser munidos de vários privilégios dentro da rede. Sobretudo na

---

[223] Neste sentido, Houben, R.; Snyers, A.Ibid.

[224] Neste sentido: Kuner, Christopher. Et al. "Blockchain versus data protection". International Data Privacy Law, vol. 8, n. 2. 2018. pp.103-104

[225] Conforme afirma Kuner, Christopher. Ibid, pp. 103-104: "*Widespread distribution of copies of the ledger, together with a consensus process that does not require any centralized, trusted, intermediary to manage the ledger*".

[226] Kuner, C. et al, Ibid, pp.103-104, definem o algoritmo de consenso como um processo acordado para armazenar uma ou mais cópias do livro-razão e para adicionar mais entradas.

[227] Termo traduzido da obra de Finck "very technical specificities and governance design of blockchain use cases". Ver mais em Fink, Michèle. "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law?" Study. European Parliament, 2019.

[228] Tradução para stakeholders.

blockchain permissionada, conforme previamente mencionado, os participantes vão assumir diferentes tipos de acesso e influência, a saber: i) leitores (que possuem o direito de acesso ao conteúdo e podem visualizar todo conteúdo registrado na *blockchain* através de uma cópia instantânea do livro-razão); ii) os participantes escritores que vão ser participantes com acesso ao livro-razão, mas além de ler seu conteúdo, podem submeter informação a ser armazenada; e, por último, iii) os participantes validadores. Desde logo, registra-se que a ressalva sobre os validadores feita por WIRTH et al, na qual os validadores existem (em certos modelos de *blockchain)* através de um interesse econômico em usar recursos computacionais para validar uma transação, mas não precisam - ou sequer estão preocupados - em ter ciência do conteúdo pessoal no livro-razão distribuído[229], não corresponde a algo transversal a todos os protocolos de *blockchain*, mas ilumina um ponto importante que é a desnecessidade de ciência do conteúdo no processo de validação.

Passa-se a analisar, em conjunto, a arquitetura dando atenção aos diversos tipos de participantes que podem existir. Tendo em conta as categorias apresentadas anteriormente, de maneira breve, cumpre relembrar que a primeira categoria corresponderia à *blockchain* pública sem permissão que, a exemplo da Bitcoin, qualquer entidade participante poderá ser leitor, utilizador e validador simultaneamente. Nesta espécie não existe uma entidade com mais privilégios que outra, a rede é descentralizada por participantes com poderes de acesso e edição iguais. E esse modelo, segundo KUNER, por oferecer demasiada abertura, ausência de permissão e um potencial anonimato dos participantes[230], os sistemas públicos de *blockchain*, conforme o autor, são problemáticos sob a perspectiva legal e regulatória, a depender das circunstâncias. A problemática identificada pelo autor seria para fins de proteção de dados, mas também em outras searas, em relação àquela diz respeito que se os dados não forem anonimizados, o RGPD é materialmente aplicável e, consequentemente, os direitos e princípios dos titulares são juridicamente exigíveis.

Por outro lado, a conceção inicial é alterada quando ocorre um novo arranjo nos componentes da *blockchain* que conduzem a um design diferenciado. Na *blockchain* permissionada, alguma autoridade desenvolvedora (que pode corresponder a um ou alguns participantes) poderá definir regras de permissão diversas para cada participante, sobre as quais vai ser definido que participante poderá ser leitor, escrever blocos ou ainda validar e inseri-los em cadeia. Segundo estudo da UE, se alguma entidade precisar ser autorizada para executar ou validar um registro na *blockchain*, será uma

[229] Wirth, Christian; Michael Kolain. "Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data". 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET), 2018.
[230] Neste sentido, Kuner, C. et al (2018). Ibid.

blockchain permissionada[231]. E ainda em tempo, por outro lado, há quem defenda a existência das *blockchains* privadas que seriam diversas das permissionadas, o que, para doutrina majoritária, estaria mais ligada à conceção de uma base de dados privada distribuída.

Os modelos de regulação descentralizados através da tecnologia *blockchain* correspondem a um ecossistema com multiplicidade de atores, que assumem os mais diversos papéis. Entre os papéis que tais atores poderão desempenhar surge também o inerente ao tratamento de dados pessoais. Mesmo quando a situação não pode ser definida como única, surge uma necessidade particular de promover uma análise cuidadosa dos papéis e responsabilidades de cada categoria de participante que surja.

Assim, vislumbrando a definição de responsável pelo tratamento dada pelo artigo 4º do RGPD, o primeiro passo seria definir que entidade é "que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais". À luz da definição legal, WIRTH suscitou este desafio de aplicar o artigo 4º do RGPD no contexto da *blockchain*. Consoante o autor, o Regulamento focou-se em determinar que entidade tem a habilidade de controlar ativamente o fluxo de dados através dos sistemas de TI, mas a *blockchain* rompe com este entendimento porque, em certos modelos permissionados, as entidades que administram a infraestrutura das chaves potencialmente podem determinar as finalidades e meios o que as torna responsáveis pelo tratamento[232].

E, nesta senda, há o impulso de identificar o responsável pelo tratamento, sob os termos da RGPD, que recai no contexto de que a *blockchain* é concebida para não existir nenhuma autoridade centralizadora com poder de decisão total. Determinar as finalidades, sob o conceito legal, é, em outros termos, decidir. Decidir fins e meios, pelo princípio da *accountability,* é um poder que vai precisar recair sobre alguma entidade, mesmo que a conceção do sistema seja distribuída; afinal, o processamento da *blockchain* vai gerar efeitos jurídicos na esfera subjetiva de cada participante.

A obra de NASCIMENTO et al já havia elencado que uma das características da cadeia de blocos é uma *"participation in democratic decision-making by enabling accountability*"[233]. Por conta disto, muitas entidades desenvolvedoras de sistemas baseados na *blockchain* são desafiadas a encontrar um determinado arranjo para estabelecer uma rede em que seus participantes tomem decisões e sejam responsáveis por elas. Se a entidade que desenvolve a rede *blockchain* define que não haverá uma autoridade centralizadora com poder de decisão, esta definição vai determinar as

[231] Nascimento, S.; Pólvora A. (coord.) *et al.* "Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies". EUR 29813 EN, Publicações oficiais da União Europeia, Luxemburgo, 2019.
[232] Wirth, Christian. Ibid. 2018.
[233] Nascimento S., et al. Ibid. 2019. p. 45

finalidades e os meios de tratamento, antes mesmo do mesmo acontecer. E a seguir esta linha de pensamento, a Autoridade de Controlo Francesa (a CNIL[234]), em importante diretriz sobre a *blockchain* no contexto do RGPD, estabeleceu o entendimento que se o participante da rede *blockchain* tiver o poder de tomar decisões para o grupo[235], ele poderá reputar-se como um responsável pelo tratamento à luz do Regulamento.

Surge, nesta perspetiva, o papel do participante que valida as transações e registros no livro-razão distribuído, comumente denominado validador. A validação de transação envolve a simples verificação que o registro atingiu critérios e padrões adequados (seja o pré-definido formato ou tamanho do bloco), por isso é que a CNIL entendeu que o fato de validar uma transação já realizada não significa determinar finalidades e os meios de tratamento por si só[236]. A recomendação é não considerar os validadores como responsáveis pelo tratamento, afinal o ato de validar não define qualquer propósito, este que já foi definido em momento anterior, seja na opção pela arquitetura, seja no momento de registrar algum dado.

Entretanto, a doutrina majoritária aponta no sentido de que a entidade validadora pode ser enquadrada no conceito legal de subcontratante, tendo em conta que a simples consulta a dados já configura tratamento, consoante o artigo 4.2 do RGPD. Ante o exposto, neste caso do participante validador, o tratamento de dados pessoais pelo validador pode não definir finalidades, mas pode ocorrer por conta de um responsável que assim o decidiu pelo registro, recaindo assim o validador na definição de subcontratante.

Seguindo esta lógica, MARTINI et al[237] isentam o participante validador de qualquer controle sobre as informações por ele validadas, visão esta reiterada por FINK[238], cujo contributo visou esclarecer que mesmo algumas decisões recaindo na discricionariedade do validador (a saber, por exemplo, atualizar o software para usar a plataforma), tal poderá, ainda assim, não ser suficiente para considerar a figura do validador como responsável pelo tratamento.

Caso se valide a transação feita, quem decide fazê-la é o próprio participante com poderes para escrever. Doravante denominado participante escritor, esta entidade da *blockchain* vai decidir

---

[234] *Commission Nationale de l'Informatique et des Libertés*

[235] "To identify one participant who makes decisions for the group and to designate the said participant as a data controller". Ver mais em Commission Nationale de l'Informatique et des Libertés (CNIL). Solutions for a responsible use of the blockchain in the context of personal data. Disponível em https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data Acesso 29 de junho de 2020.

[236] Commission Nationale de l'Informatique et des Libertés. Ibid.

[237] Martini, Mario; Quirin Weinzierl. "Die Blockchain-Technologie und das Recht auf Vergessenwerden". Neue Zeitschrift für Verwaltungsrecht, NVwZ, 2017.

[238] Fink, Michèle. Ibid.

submeter os dados para serem validados posteriormente o que, para a CNIL, significa que *"os participantes, que detêm o direito de escrever na cadeia e os que possuem o direito de enviar dados para verificação podem ser considerados controladores dos dados*"[239]. Sob este ponto de vista oficial, pode-se suscitar que o participante escritor pode ser legalmente considerado responsável pelo tratamento de dados por determinar os modos (ao optar por registrar dados na *blockchain*) e os propósitos (relacionados com a coleta e o tratamento de dados por si).

E, sob esta definição, a Autoridade francesa elencou 2 situações em que o participante seria, por definição, o responsável pelo tratamento: na circunstância em que o participante seja uma pessoa singular e os dados pessoais tratados na operação de registro na *blockchain* estão relacionados com atividade profissional ou comercial (entende-se que a norma busca excepcionar o princípio do *"household exemption*", previsto no artigo 2º, n.º .2, c) RGPD, de quando há exercício de atividades exclusivamente pessoais ou domésticas por pessoa singular).

De outro lado, a simples (e qualquer) situação em que um participante seja associado a uma pessoa coletiva (o que indica a impossibilidade em recair na exceção do uso doméstico, instituto este reservado apenas para pessoas singulares). Em outras palavras, a CNIL adotou uma determinação que se baseia no âmbito material do RGPD (debatido no capítulo I deste trabalho) para encontrar um fundamento jurídico para enquadrar os participantes da *blockchain* (tema do capítulo II) de forma a identificar putativos responsáveis pelo tratamento de dados pessoais ao escrever registros e transações no livro-razão distribuído.

Um parêntese precisa ser aberto, pois talvez o critério de apenas considerar a exceção de uso doméstico reste insuficiente para encontrar o devido responsável pelo tratamento na *blockchain*. A exceção de âmbito material do Regulamento não significa que uma pessoa singular não possa se encontrar em uma situação particular e ao mesmo tempo ser enquadrada como responsável pelo tratamento, uma vez que, mesmo sem fins econômicos, o manejo de dados pessoais pode recair no escopo legal do RGPD.

E é contrariamente a este entendimento limitador que FINK relembra a exceção do uso doméstico para ser interpretada de forma estrita[240]. A CNIL ao limitar-se a pessoa singular com finalidades econômicas para ser um controlador de dados pessoais, por exclusão deixa de fora a pessoa singular que, sem finalidades econômicas, pode não estar investida de um propósito estritamente particular ou doméstico.

---

[239] Commission Nationale de l'Informatique et des Libertés. Ibid. p. 1. (tradução livre)
[240] Fink, Michèle. Ibid.

Não obstante, a partir do momento em que se fala em um livro-razão distribuído, uma base de dados descentralizada, ou qualquer outra definição que a *blockchain* assuma, o fato do indivíduo por si só decidir (pessoa singular), investido no papel de participante, escrever um dado pessoal na cadeia, mesmo que com finalidade de foro íntimo, pela natureza da arquitetura adotada pela *blockchain*, não se vislumbra qualquer chance de o dado permanecer no âmbito doméstico do participante. E por isso prevalece o conceito do caso Bodil Lindqvist[241] uma vez que o próprio TJUE assim o fez quando interpretou que a *household exemption* ficou afastada para divulgação de dados pessoais na internet para um número indefinido de indivíduos (semelhante ao que ocorre no modelo público da *blockchain*). E assim a jurisprudência na União Europeia evoluiu para impor limites à restrição de âmbito material à Proteção de dados.

Em 2014, no caso Ryneš, o TJEU, ao falar do princípio da *household exemption*, clamou pela necessidade deste ser "objeto de interpretação estrita"[242]. E nesta senda, o TJEU fez importante distinção entre os termos meramente para exclusivamente para a correta interpretação desta exceção, conforme os termos do Considerando 30: "Esta interpretação estrita também encontra fundamento na própria letra desta disposição, que exclui da aplicação da Diretiva 95/46 o tratamento de dados efetuado no exercício de atividades não meramente pessoais ou domésticas, mas sim «exclusivamente» pessoais ou domésticas"[243]. Apesar de mencionar a Diretiva 95, o termo exclusivamente segue utilizado no Artigo 2.2(c) RGPD.

Seguindo o mesmo entendimento, o TJEU, em Satamedia[244], expressamente determinou que a exceção é apenas para atividades no curso da vida familiar e privada dos indivíduos e manifestamente não se aplica a atividades que os dados pessoais vão ser acessados por um número indefinido de pessoas. Ou seja, conforme a jurisprudência apresentada, restará em descumprimento do artigo 2, n.º 1, c) do RGPD quem utiliza a *blockchain* e pretende conformidade com o RGPD através da exceção exercício de atividades exclusivamente pessoais ou domésticas.

Ainda sobre o critério optado pela CNIL, na sua recomendação, de a natureza ou não de participante estar em função do desígnio ser econômico ou não econômico acaba por não coincidir,

---

[241] Acórdão TJEU, Lindqvist, de 6 de Novembro de 2003, processo C-101/01, considerando 47. Nos exatos termos: "Esta excepção deve, portanto, ser interpretada como tendo unicamente por objecto as actividades que se inserem no âmbito da vida privada ou familiar dos particulares, o que não é manifestamente o caso do tratamento de dados de carácter pessoal que consiste na sua publicação na Internet de maneira que esses dados são disponibilizados a um número indefinido de pessoas.".

[242] Conforme Acórdão TJUE, Rynes, de 11 de dezembro de 2014, processo n.º C-212/13, considerando 29.

[243] Acórdão TJUE, Rynes, de 11 de dezembro de 2014, processo n.º C-212/13, considerando 30.

[244] Acórdão TJEU, Satamedia, de 16 de dezembro de 2008, processo n.º C-73/07, considerando 44.

totalmente, com a teleologia do RGPD, na medida em que o RGPD pode ser aplicável em relações sem fins econômicos, como aliás ficou patente no mencionado acórdão Lindqvist.

Assim, seria mais acertado se a recomendação não utilizasse critério díspar daquele que resulta do espírito e da finalidade do Regulamento. Ao invés de olhar para o viés econômico (que não existe na letra do RGPD quando cria as exceções de âmbito material no artigo 2, n.º 2, se o órgão tivesse vislumbrado a natureza da *blockchain*, poderia interpretar que a questão debatida do *design* distribuído e descentralizado impossibilitaria entender algum uso desta tecnologia que seja estritamente doméstico ou particular.

Em outras palavras, não cabe levantar critérios de exceção de âmbito material para descaracterizar qual seja o participante que, por não possuir um interesse econômico, estaria isento de responsabilidade pelo tratamento por ele definido. Esta conclusão resta arriscada, inclusive, por aproximar a *blockchain* das criptomoedas, que estas sim possuem um caráter econômico inerente, mas que, ao contrário do que o senso comum costuma definir, acabam por ser espécies daquela que, por sua vez, é gênero e traz uma acepção mais ampla.

Para corroborar a crítica tecida acima, o exemplo da recomendação francesa demonstra bem a adoção de um critério extralegal. Segundo a CNIL, a pessoa singular que compra e vende Bitcoin, por conta própria, não poderá ser responsável pelo tratamento, ao contrário de um outro indivíduo que o faz como parte de uma atividade profissional ou comercial. Note-se que é improvável arrazoar determinada situação em que algum indivíduo se disponha a investir em criptomoedas por mero deleite e sem uma finalidade comercial de lucrar com aquele sistema. E por saber que a *blockchain* pode ir muito além do setor de criptomoedas[245], definir responsabilidade de tratamento em virtude de atividade comercial ou não acaba por ser um lapso de técnica interpretativa e extrapola as hipóteses do artigo 2.2 do RGPD.

3.3 Natureza Dos Dados Na Blockchain

Cumpre ser analisada a natureza dos dados pessoais que, porventura, estejam inseridos ou relacionados com a *blockchain*. Primordialmente, distinguem-se os identificadores dos participantes: cada participante, seja leitor, escritor ou validador, vai ser identificado por uma série de caracteres

[245] Conforme distingue Basu: "Blockchain is not Cryptocurrency or Bitcoin". Para aprofundar este propósito, ver em Basu, Dr Paritosh. "Emerging Dimensions of Blockchain Technology." AIMA Journal of Management Research, n. 3, 2018.

alfanuméricos dispostos de forma aleatória que, em termos informáticos, é denominada "endereço", gerado a partir de uma chave pública relacionado com a conta conexa a tal participante.

O conceito da infraestrutura de chave pública (PKI) surge descrito na obra de DOUKAS et al[246], que o detalha a PKI como sendo efetiva modalidade de dados criptografados para garantir um elevado nível de confiança para intercâmbio de informação em um ecossistema de insegurança crescente. A infraestrutura conta com um par de chaves matematicamente relacionadas. Se uma chave (a pública) é usada para cifrar a informação, a única chave (privada) relacionada pode decifrar a informação. Em caso que a chave pública possa ser comprometida, ainda assim, não é computacionalmente possível fazê-lo com a chave privada[247].

Em elementares termos, na criptografia assimétrica adotada por diversos sistemas baseados na *blockchain*, a chave pública relaciona-se com uma chave privada, segredo unicamente conhecido pelo participante do sistema. Tecnicamente é possível associar uma chave pública a uma privada, e a chave privada pode ser relacionada a um certificado digital que formalize relação de uma pessoa singular como participante. Por isso há a discussão sobre se o endereço na *blockchain* é, ou pode vir a ser, um identificador único, à luz do artigo 4.º, n.º 1 do RGPD, já que pode ser ligado à identidade do participante pessoa singular.

A presente questão é saber se há a possibilidade da identificação de uma pessoa singular através de seu endereço na rede da cadeia de blocos distribuída. E pelo desenho detalhado da *blockchain*, caso o número de identificação seja mostrado, segundo a CNIL, ele vai ser considerado como identificador único. E é conforme esta visão que a informação relativa à pessoa identificável dificilmente pode ser minimizada, nos termos do artigo 4.1 RGPD, considerando que a publicidade deste número de identificação único é inerente à "arquitetura da *blockchain*"[248].

Além do endereço para cada participante, seguindo este panorama de mapear possíveis identificações, os dados adicionais[249] também podem possivelmente ser considerados dados pessoais, pela eventualidade de virem a relacionar-se com indivíduos além dos participantes. Salientou-se, oportunamente, que, relativamente à "proteção de dados desde a conceção e por defeito"[250], resta a

---

[246] Doukas, Charalampos, et al. "Enabling data protection through PKI encryption in IoT m-Health devices." 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE). IEEE, 2012. P 26

[247] Doukas, Charalampos, et al. Ibid. p. 26: "In case the public key gets compromised, still it is not computationally feasible to retrieve the private key". Tradução livre

[248] Nos termos exatos da Autoridade Francesa (CNIL): "The very architecture of blockchains means that these identifiers are always visible, as they are essential for its proper functioning. The CNIL therefore considers that this data cannot be further minimised and that their retention periods are, by essence, in line with the blockchain's duration of existence" in: CNIL. Ibid. p.6

[249] Ou nos termos técnicos: "payload"

[250] Ibid.

incumbência do responsável pelo tratamento em garantir, seja no momento de definição dos meios de tratamento como no próprio tratamento, as medidas técnicas e organizativas adequadas, de acordo com o artigo 25 RGPD, de forma a promover a proteção de tais dados. Por este princípio e de forma de respeitar outros como a ideal pseudonimização e a necessidade de *accountability*[251], a escolha de como os dados vão ser registrados no livro-razão distribuído deve ser pensada pelo responsável pelo tratamento, que não surge como simples tarefa, sobretudo porque, perante esta tecnologia, nem sequer é consensual a definição do responsável.

Mesmo assim, a recomendação da Autoridade Francesa foi preferencialmente no sentido de registrar dados na *blockchain* através da técnica de *"commitment",* ou conforme já explicado, o esquema de comprometimento, cuja característica é a de ser uma ferramenta criptográfica usada como prova sem conhecimento (ZKP)[252], a fim de permitir que o provador (P) participe de provas, nas quais o verificador (V) realiza uma escolha do quer aprender, revelando apenas o que corresponde à escolha ao verificador, e assim garantindo privacidade.

A segunda alternativa, caso o recomendado esquema de comprometimento não seja possível, seria registrar os dados em geral no formato de *hash digest*, utilizando a função *hash* como técnica criptográfica para cifrar os dados. Em outros termos, a CNIL recomenda expressamente o uso de criptografia para assegurar o adequado nível de confidencialidade. Sabendo que confidencialidade pode ser definida como "a garantia de que a informação não será obtida por pessoas não autorizadas"[253], a recomendação da CNIL indica uma preocupação em que tão-somente os participantes com os direitos e privilégios necessários possam ser capazes de acessar a informação, esteja ela armazenada, em processamento ou em trânsito. Todavia, participantes com diferentes direitos e privilégios são uma característica da rede permissionada, indicando que a prioridade da UE, caso siga a linha da CNIL, vai ser priorizar uma *blockchain* permissionada em detrimento de uma rede pública utilizada pela maioria das criptomoedas baseadas na *blockchain*.

Segundo CHICARINO et al.[254], em uma rede pública como a Bitcoin, a confidencialidade é buscada por mecanismos como a pseudonimização dos números identificadores dos participantes, fazendo alusão ao instituto estipulado no artigo 4.5 RGPD: "o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações

[251] Responsabilidade, conforme artigo 5.2 "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n. 1 e tem de poder comprová-lo" Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid.
[252] Conforme definido em Jean-Jacques Quisquater, Ibid.
[253] Chicarino et al. Ibid. p. 11
[254] Chicarino et al. Ibid.

suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas" pelo responsável pelo tratamento. Consoante o ensinamento de que os endereços *blockchain* são resumos criptográficos das chaves públicas, e sendo essas chaves públicas possíveis identificadores únicos de uma pessoa singular, acaba por ser dado pessoal por força do Regulamento. Neste sentido, FINK estabelece que "dois conjuntos de dados armazenados na *blockchain* podem ser potencialmente definidos como dados pessoais para fins do Regulamento; assim como os metadados transacionais armazenados nos blocos, bem como as chaves públicas"[255], corroborando a visão de que a chave pública relacionada aos participantes pode se enquadrar no conceito jurídico de dado pessoal.

Se tais dados pessoais forem pseudonimizados, acaba por advir a ressalva do Considerando 26 RGPD. A pseudonimização por si só não afasta o regime jurídico da proteção de dados, já que os dados "possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares"[256]. Todavia, o Considerando 29 não condena a técnica da pseudonimização, inclusive a recomenda. Somado a esta recomendação, há o artigo 6º, n.º .4, e) RGPD que estabelece que uma das formas de salvaguarda adequada é a pseudonimização. Não suficiente, merece destacar a previsão da proteção de dados desde a conceção do artigo 25º exaltando a pseudonimização como uma medida técnica e organizativa adequada.

Em outras palavras, o RGPD é aplicável aos dados pseudonimizados. Inclusive, de acordo com BORGESIUS, sob o ponto de vista jurídico, "dados pseudonimizados são sempre dados"[257]. Apesar desta afirmação generalizar o termo, representa grande esforço prático provar se os métodos de pseudonimização são capazes de produzir dados anônimos, algo que haveria uma possibilidade de acontecer, segundo a Autoridade de Controlo do Reino Unido, nomeadamente "Information Commissioner's Office" (ICO)[258].

Então, diante do exposto, pode-se afirmar que a pseudonimização é uma técnica acolhida pelo RGPD como forma de salvaguardar os direitos, e também uma medida técnica e organizativa. Por não extravasar o âmbito conceitual, o endereço do participante em uma *blockchain* continua a ser um dado pessoal, com todas as prerrogativas a ele inerentes. Neste sentido, mostra-se que o uso de uma

---

[255] Fink, Michèle. Ibid. p. 10 (tradução livre)

[256] Considerando 29, Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid.

[257] Zuiderveen Borgesius, F. "Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation" Computer Law & Security Review, vol. 32, 2016. p. 256 (Tradução livre)

[258] Information Commissioner's Office (November 2012), 'Anonymisation: managing data protection risk code of practice' Disponivel em https://ico.org.uk/media/1061/anonymisation-code.pdf Acesso em 29 de junho de 2020. Nos termos: "This does not mean, though, that effective anonymization through pseudonymization becomes impossible"

blockchain com dados, se possível, pseudonimizados pode ser aconselhável, pois além da segurança gerada pela técnica de salvaguarda, ainda pode haver mais confidencialidade, uma vez que nem todo participante terá acesso a essa informação relacionável que representa um dado pessoal.

Como a *ultima ratio*, o direcionamento da CNIL foi adotar o *offchain*[259], a fim de armazenar dados em texto claro fora da blockchain (até mesmo a informação sobre o responsável pelo tratamento) e registrar no livro-razão apenas uma prova de existência de dados armazenados externamente. *Data venia* a posição da DPA Francesa, preocupar-se em esconder dados de entidades participantes que assumem o papel de responsáveis pelo tratamento é dissipar energia em algo que não seria relevante para fins de adequação. A tecnologia por si só, conforme bem explicado pela CNIL[260], não pode ser objeto de regulamentação pelo RGPD, mas sim seus usos em específico. E neste sentido, se o uso da *blockchain* oferecer a visualização de dados que identifiquem uma possível pessoa através de um participante, pelo fato de tal participante ser um responsável pelo tratamento, não se pode falar que está inserido no âmbito do Regulamento que busca tutelar os direitos do titular dos dados perante o responsável pelo tratamento, e não proteger os direitos desta entidade que define as finalidades e meios de tratamento.

Superada a problemática de guarda em texto claro o endereço do participante responsável pelo tratamento, parte-se para a análise dos dados inseridos dentro do bloco, desde logo focando-nos na questão de armazenar os dados pessoais em texto claro e suas possíveis implicações. Primeiramente, o senso comum já vem debatendo esta questão de que os dados inseridos na *blockchain* não podem ser deletados e vão perenemente permanecer na *blockchain* sem direito ao apagamento ou retificação.

Acertadamente do ponto de vista matemático, NASCIMENTO *et al* reconhecem que é tecnicamente possível modificar o livro-razão distribuído[261]: a obra demonstra um cuidado semântico ao definir a característica da *blockchain* de ser extremamente difícil ou quase impossível de haver alteração ou apagamento. Ou seja, é improvável que exista uma alteração em todas as *ledgers* espalhadas. Este cenário não afeta apenas a integridade, mas também pode afetar a disponibilidade dos dados registrados.

Para a questão de o dado pessoal estar publicamente disponível no bloco registrado, a CNIL dirigiu esforços em pensar soluções que garantissem a privacidade e a confidencialidade em determinadas circunstâncias, e acabou por concluir que se a informação estiver cifrada através de um

[259] Commission Nationale de l'Informatique et des Libertés. Ibid.
[260] "Blockchain is a technology on which personal data processing can rely but it is not a data processing operation with its own purpose". Commission Nationale de l'Informatique et des Libertés. Ibid.
[261] Nascimento S. et al. Ibid.

algoritmo e chave, o *cleartext* irá ser disponibilizado tão somente a quem detiver a chave privada utilizada na cifragem. Esta solução visa solucionar outras problemáticas decorrentes, desde a necessidade de conformidade com os direitos dos titulares ao respeito pelos princípios inerentes ao RGPD, como o da minimização dos dados. Como bem elencou a Autoridade francesa, a função *hash* é capaz de, ao invés de disponibilizar estes dados pessoais em *cleartext,* será feito em *ciphertext* e a informação em si será suscetível de ser obtida[262]

Por consecução lógica, o apagamento da chave privada utilizada para cifrar os dados inseridos no bloco significa tornar os dados ininteligíveis. Desde o Considerando 83, ou no estipulado no artigo 6.º, n.º 4, e)[263], a técnica da cifragem é reconhecidamente um mecanismo de salvaguarda adequada, pois torna o processo de decifragem juridicamente seguro. Pela natureza da irreversibilidade, a doutrina bem considera que a verdadeira anonimização dos dados pessoais, fruto da cifragem, é uma forma de recair o tratamento fora do âmbito de aplicação do RGPD, sob a condição de que os titulares não sejam mais identificáveis[264]. Corrobora esta visão, por força do Considerando 26, o próprio "regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação"[265], o que deixa evidente que uma vez cifrado de forma irreversível, há um afastamento da aplicação do RGPD.

E ainda, cumpre diferenciar a cifragem da pseudonimização, pelo fato desta apresentar sempre um residual risco de re-identificação[266], que pela inteligência do Considerando 28, resta evidente que não retira do âmbito material de aplicação do Regulamento, em contraponto à anonimização. Quanto à análise do risco de re-identificação, há de se testar a fim de avaliar a probabilidade daquela (ao aplicar esse teste e documentar as decisões, o procedimento terá evidências de que o risco de divulgação foi considerado adequadamente e que qualquer decisão será auditável). Esta avaliação acaba por ser um exame útil, porque considera se um "invasor" seria capaz de alcançar a re-identificação se motivado a tentar isso. Conforme *guideline* da ICO, o intruso motivado é considerado uma pessoa que começa sem nenhum conhecimento prévio, mas que deseja identificar o indivíduo de quem os dados pessoais são derivados[267].

---

[262] Commission Nationale de l'Informatique et des Libertés. Ibid. Nos termos: "through state of the art algorithms and keys, the data controller can make the data practically inaccessible".

[263] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid.

[264] University College London. Anonymisation and Pseudonymisation. Disponível em https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/anonymisation-and Acesso em 17/04/2020.

[265] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid

[266] University College London. Ibid

[267] Information Commissioner's Office. Anonymisation: managing data protection risk code of practice. Disponível em https://ico.org.uk/media/1061/anonymisation-code.pdf Acesso em 17 de abril de 2020.

A conclusão que a ICO (Autoridade de Controlo do Reino Unido) chegou no seu código foi que as normas de Proteção de dados não se aplicam a dados anonimizados, uma vez que os titulares dos dados não são mais identificáveis. Entretanto, faz-se uma ressalva de que algumas poucas restrições legais se aplicam aos dados mesmo que anonimizados. A solução proposta pelo Comité Europeu para a Proteção de Dados (CEPD) da cifragem para anonimizar de forma irreversível encontra consonância com a doutrina e posicionamento de outras Autoridades que na supervisão do RGPD já aceitam a circunstância de o dado cifrado ser uma forma de tratamento que não incide nas atenções da proteção de dados. E por isso, se o dado além de não estar em *cleartext*, estiver cifrado dentro do bloco, o Regulamento é inaplicável[268].

Mesmo sendo uma forma de exclusão de incidência normativa, a CNIL em seu documento foi adiante e apresentou outra solução além da cifragem para anonimização irreversível: armazenar no livro-razão distribuído apenas um *hash* correspondente a dados que, por sua vez, serão armazenados fora da *ledger*. É o já anteriormente denominado *off-chain storage*. A CNIL retoma esta alternativa para ser arrazoada no contexto da observância de direitos dos titulares, a exemplo do direito ao apagamento dos dados, previsto no artigo 17º do RGPD. Uma vez que um *hash* devidamente desenvolvido, através de uma criptografia de alta entropia, garante que dificilmente se chegará no dado pessoal de origem por força-bruta. A doutrina também usa o termo *off-chain* e alguns autores, a exemplo de EBERHARDT e STEFAN, enxergam privacidade no estabelecido esquema de conhecimento zero que consegue verificar computacionalmente registros, mantendo as informações privadas já que não precisam tornar-se públicas para fins de verificação[269].

Ante todo o exposto, há uma certa contradição em falar de direitos dos titulares do RGPD sobre dados anônimos, uma vez que o RGPD não se aplica, exceto se o fato de existir dados armazenados em outro sítio significar que este processo da *off-chain* seja considerado uma pseudonimização (o que faria sentido, porque a pessoa singular continua identificável mediante a utilização de informações suplementares, a ser enquadrado no conceito do artigo 4.1 RGPD). Em outras palavras, se a arquitetura do sistema for baseada em um modelo permissionado em que os dados restam realmente anonimizados, o âmbito material não enquadra aquele propósito específico na *blockchain*, e por conseguinte, o RGPD é inaplicável.

---

[268] Information Commissioner's Office. Ibid.

[269] Eberhardt, Jacob; Stefan Tai. "Zokrates-scalable privacy-preserving off-chain computations." 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018.

Por outro lado, caso ofereça dados presumidamente pseudonimizados, a alternativa de armazenamento *off-chain* parece não ser o cenário ideal que consegue retirar do âmbito de aplicação do Regulamento, mas o que não descaracteriza como uma alternativa, desde que os princípios e direitos dos titulares sejam respeitados. Uma ressalva consiste em reconhecer que essa solução requer o uso de um outro sistema a fim de armazenar os dados de fato e, apesar de se tratar de uma escolha do responsável pelo tratamento, se o sistema *off-chain* for centralizado, a essência de segurança e integridade de um registro distribuído perde-se e a *blockchain* vira apenas uma representação de uma base de dados tradicional, com todos os inerentes incidentes de segurança, cujo resultado significa uma violação dos dados pessoais suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, na esteira do artigo 34.1 do RGPD. Ou seja, mesmo que os dados distribuídos possam oferecer um elevado grau de confidencialidade, ao estarem centralizados, precisam manter as devidas medidas técnicas e organizativas para evitar, por exemplo, um ataque centralizado que ponha em risco a disponibilidade do sistema e sua integridade, a exemplo do relatório de impacto destacado pela CNIL para assegurar que nesta *off-chain* os riscos sejam mínimos para os titulares dos dados[270], sem prejuízo das demais particularidades da avaliação de impacto prevista no artigo 35 do RGPD[271] .

A solução proposta pela CNIL, como possível forma de respeitar os direitos sobre dados pessoais, dando observância ao RGPD, baseou-se no anteriormente debatido esquema de comprometimento. De forma breve, o comprometimento criptográfico consiste em uma técnica em que se pode verificar um dado pessoal, mantendo-o oculto, e ainda sendo possível demonstrar em estágio posterior que o valor cometido é criptograficamente interligado aos dados pessoais. O comprometimento*,* por si só, não apresenta riscos em termos de confidencialidade, de acordo com a obra de MARTIN-BARITEAU[272].

De toda forma, as várias Autoridades demonstram que há uma preocupação com a recorrente dicotomia entre *blockchain* e direito ao apagamento do artigo 17 RGPD, para os casos em que o dado pessoal em causa tenha de ser deletado. No entanto, a suposta incompatibilidade resta minorada através da técnica do comprometimento, esta que permite o registro de dado pessoal sem divulgá-lo (nem mesmo permite uma associação posterior), criando-se uma prova segura e não relacionável. Segundo a interpretação da CNIL, é tecnicamente impossível atender ao titular de dados que faz requerimento pelo apagamento dos dados registrados na *blockchain*. Entretanto, a diretriz da CNIL faz

[270] Commission Nationale de l'Informatique et des Libertés. Ibid.
[271] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid
[272] Martin-Bariteau, Florian. "Blockchain and the European Union General Data Protection Regulation: The CNIL's Perspective." Blckchn. ca Working Paper, vol. 1, 2018.

o contraponto de ressaltar que o esquema de comprometimento pode ser considerado uma forma adequada de salvar compromissos na *blockchain,* permitindo tornar o dado "praticamente inacessível e, com isso, aproximar-se aos efeitos de um apagamento"[273].

3.4 Pressupostos Jurídicos Necessários

Foi demonstrado que existem diversas formas de arquitetura *blockchain* e que algumas delas já oferecem uma solução que torna o RGPD inaplicável materialmente, nomeadamente i) quando a *blockchain* permissionada for programada para que o participante leitor não consiga aceder aos dados pessoais em *cleartext*; ii) quando o participante validador consiga validar e registrar o bloco através de um esquema de comprometimento; iii) quando o participante com poderes de escrever registros na *ledger* não for enquadrado como responsável pelo tratamento se a arquitetura da *blockchain* tratar dados anonimizados através de técnicas de cifragem.

Em contrapartida, se a arquitetura permite apenas a pseudonimização dos dados pessoais, ou ainda, que algum participante (que não seja o responsável pelo tratamento) visualize o dado registrado de forma explícita, passa-se a elencar diversos ditames legais para a adequação de certo propósito específico que utiliza a *blockchain*.

O artigo 5.º, n.º 1, a) do RGPD elenca três princípios básicos que sustentam o tratamento de dados pessoais, quais sejam licitude, lealdade e transparência. Para fins de lealdade do tratamento, pondera-se que a *blockchain* deve ser usada com neutralidade, ou seja, que a obrigação de processar dados desta maneira seja previsível para os titulares dos dados. Mesmo quando existe uma mudança de modalidade, em que a relação bilateral entre responsável-titular passe a ser descentralizada e distribuída, é expectável que o titular seja alertado dessa alteração de forma a que o tratamento não se torne ilegal à luz dos termos do RGPD. Esta também é uma das razões que determina que, à luz deste princípio, tanto a CNIL como a doutrina majoritária, conforme preceitua FINK[274], não vislumbra qualquer problema na sua adoção.

Ainda no que tange ao artigo 5.º, n.º 1, a) do RGPD, a observância de demandas de transparência também não parece ser problemática. A CNIL resolveu analisar a *blockchain* sob uma perspectiva *lato sensu*, o que se veio a revelar fundamental de forma a não focar a análise apenas no tratamento de dados em si mesmo, mas vocacionando-se a entender o registro no livro-razão

[273] Tradução livre de Commission Nationale de l'Informatique et des Libertés. Ibid. p. 8.
[274] Fink, Michèle. Ibid.

distribuído como um processo que envolve várias etapas. Antes da operação de tratamento real, identifica-se que informações serão trocadas em momentos anteriores, a exemplo da criação de um perfil e com o ingresso do participante, ou ainda quando um software cliente é instalado nos terminais dos utilizadores, permitindo o envio de dados ao livro-razão distribuído.

Ora, o direito à informação, que assiste os titulares dos dados, foi perspectivado como uma das faces da transparência, já que, por conta do labor jurisprudencial do TJEU, no caso Bara (2015)[275], ficou assente a necessidade de serem disponibilizadas informações aos titulares dos dados previamente à realização do tratamento[276], devendo-se, portanto, aproveitar tais circunstâncias preliminares para efetivamente dar cumprimento àquele direito, em termos claros e objetivos.

Em uma lógica da *blockchain* permissionada, na qual as operações de tratamento que serão realizadas vão depender de uma entidade ou algumas entidades especiais, esse dever de informação resta mais provável. E é por isso que, no modelo de regulação público, o próprio participante ao aderir à rede poderá ser reputado o responsável pelo tratamento. Por esta diferença, a questão prende-se com a necessidade de identificar, em cada momento, qual a entidade que está definindo as finalidades e os meios, e para cada circunstância desta especificamente, haverá um ou vários entes a ser responsabilizados.

E é por este motivo que BÖHME et al[277] definiram que as regras de uma rede *blockchain* não são um acordo entre *nodes,* mas meras somas de comportamentos independentes. Noção esta que WIRTH et al[278] reiteram para afirmar que cada participante tem igual influência e liberdade para escolher (ou até iniciar) uma rede *blockchain* com regras próprias, mudar as regras existentes e decidir qualquer outro propósito/meio desde que acompanhados da maioria, sendo, para o autor, exemplo da definição de "Responsáveis conjuntos pelo tratamento", conforme artigo 26 GDPR[279].

Passando ao princípio do artigo 5.º, n.º .1, b) - a limitação das finalidades – a obrigação legal é que os dados devem ser tratados para uma finalidade específica, explícita e legítima, e não devem ser tratados de maneira incompatível com essa finalidade. A impressão geral é que a *blockchain* oferece neutralidade em relação a esse princípio, uma vez que apresenta uma arquitetura não rígida e pelas características criptográficas é muito difícil um *node* alterar os fins de um livro-razão distribuído. E é por

[275] Acórdão do TJUE, Bara, de 1 de outubro de 2015, processo C-201/14.
[276] Ibid.
[277] Böhme, Reiner and Paulina Pesch. "Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie". Datenschutz und Datensicherheit (DuD). 2017 in Wirth, Christian et al. Ibid.
[278] Wirth et al. Ibid.
[279] Ressalva-se que esta abordagem diz respeito a uma espécie de protocolo *blockchain*, dentre outros possíveis.

isso que a cadeia de blocos é utilizada como tecnologia por trás dos *smart contracts*[280], confiando-se a executoriedade contratual à *blockchain*, uma vez que regras e propósitos pré-definidos nela, são virtualmente inalteráveis, conferindo segurança jurídica de que a finalidade de utilização será limitada ao que for determinado previamente.

Prova desta autoexecutoriedade é a definição de WIRTH a qual definiu que "*smart contracts podem ser executados de forma completamente automática a representar identidades digitais, o que nos permite providenciar dados pessoais a uma terceira parte quando o acesso for devidamente necessário*"[281]. Por ser facilmente executado, o *smart contract* também deve oferecer aos responsáveis pelo tratamento na *blockchain* para que eles selecionem um objetivo e que apresentem uma finalidade demonstrável, caso seja necessário. Há sempre um risco semântico de ambiguidade ou interpretação aberta de um objetivo, as quais devem ser evitadas para evitar futuros questionamentos.

Além disso, ainda sobre a finalidade limitada, caso o objetivo tenha sido alcançado, a limitação pode ser reforçada pelo uso de ferramentas de exclusão automatizadas. Os já suscitados mecanismos criptográficos, com gerenciamento de chaves apropriado, podem tornar os dados ininteligíveis e bloqueados para outras potenciais operações de tratamento.

Ademais, há certas hipóteses legais em que não se exige rigor na finalidade limitada, a exemplo da *blockchain* legitimada por um interesse público[282]. Ou seja, uma finalidade científica ou histórica, de pesquisa ou estatística, de acordo com o artigo 89.1 do RGPD, ou, por óbvio, quando a finalidade não seja considerada incompatível com a finalidade original, consoante o artigo 6.º, n.º .4 do RGPD. O debate do interesse público é crucial para analisar a *blockchain* como solução para a Administração Pública que é feita neste trabalho.

Ante o exposto acerca do princípio da limitação das finalidades, inexiste incompatibilidade aparente entre este princípio e a *blockchain*. De fato, a situação da regulação pública em que ocorre um acesso irrestrito de dados a um amplo público, acaba por ser um desenho adotado por diversas aplicações na web e não apenas da *blockchain*, mas que apresenta um desafio reconhecido.

Depreende-se do RGPD que a limitação das finalidades é essencialmente um aspecto comportamental e de regulação, cujo desafio é compatibilizar a direção adequada com a confiabilidade dos pares envolvidos. Do ponto de vista técnico, soluções satisfatórias podem ser postas para resolver

[280] Segundo definição de Christidis e Devetsikiotis: "self-executing scripts that reside on the blockchain– integrate these concepts and allow for proper, distributed, heavily automated workflows". Veja-se mais em Christidis, Konstantinos; Devetsikiotis, Michael. Ibid. pp. 2292-2303.

[281] Wirth, Christian. Et al. Ibid. p. 2 (Tradução livre)

[282] Camilo defende que o RGPD abrange qualquer troca de informações por autoridades em meio a uma atividade de interesse público. A este propósito, veja-se Camilo, Juan. "Blockchain-based consent manager for GDPR compliance". Open Identity Summit 2019, 2019.

esta problemática de dados pessoais, a saber criptografia de última geração apropriada e uma cadeia eficaz de custódia das chaves criptográficas. Ou seja, pode-se afirmar que recursos informáticos poderão auxiliar para evitar um acesso irrestrito que ameaçaria este princípio do artigo 5.º, n.º .1, b) RGPD.

O artigo 5.º, n.º 1, c) traz um princípio de relevância, sobretudo na análise de risco proposta pelo Regulamento, a saber a minimização dos dados. A natureza da *blockchain* com sua disposição de registro único e em sequência da cadeia, somado com a persistência do sistema e do possível acesso indiscriminado por cada participante gerou preocupações com a minimização. A CNIL reconhece que existe uma tensão[283], porém é crucial realizar a interpretação deste princípio à luz da finalidade, sendo que o tratamento de dados apenas ocorre em relação aos dados estritamente necessários a essa finalidade específica. Não obstante, a obra de RAMOS e SILVA[284] pontuou que, à luz deste princípio do RGPD, deve-se escolher cuidadosamente o formato sob o qual os dados serão registrados, identificando problemas na observância a este princípio quando a arquitetura pública é adotada.

Usualmente, erguer-se o argumento de que os dados pessoais devem ser processados apenas se o objetivo do tratamento não puder ser razoavelmente cumprido por outros meios[285]. Sob esta ótica, o teste de minimização comprometeria alguns usos da *blockchain,* passando a exigir que meros participantes assumam papel de controle a demonstrar de maneira responsável que a *blockchain* é a melhor forma para o pretendido tratamento. Do ponto de vista subjetivo, esta exigência pode gerar um debate vazio de buscar explicar o porquê de se optar por participar de um livro-razão distribuído em detrimento de outras formas de registro.

Por consecução lógica, pode-se questionar a instituição que desenvolve a rede, quando a mesma assume o papel de responsável pelo tratamento, na definição de algum recurso técnico a ser adotado por tal *ledger*, mas por outro lado, o participante escritor resta em dificultosa tarefa se precisar explicar o motivo de ter usado tal tecnologia. Acaba por ser improvável que todo participante tido como responsável pelo tratamento esteja apto a responder a lista de FINK[286], que inclui desde a quantidade de dados processados, até a extensão do tratamento e o período de retenção.

Pela extrema dificuldade, o RGPD passaria a regular a tecnologia por si só, o que a CNIL entendeu não ser adequado, afinal apenas em cada caso concreto é que se pode questionar recursos técnicos que vão além de uma mera opção. Por este ponto de vista oficial, a *blockchain* não tende a

[283] Commission Nationale de l'Informatique et des Libertés. Ibid.
[284] RAMOS, Luis Felipe M.; SILVA, João Marco C. Ibid.
[285] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid.Considerando 39.
[286] Fink, Michèle. Ibid.

ameaçar a minimização dos dados, sobretudo se utilizar medidas técnicas de pseudonimização e cifragem, que funcionam para conferir uma presunção de que os dados a serem utilizados, e sobretudo divulgados, não passam do razoavelmente necessário. Ainda sobre o fato de a lei não regular a tecnologia *per si,* cumpre trazer a visão de MOEREL e STORM, cujo contributo foi expressamente declarar que *"GDPR applies to the use of a technology, not the technology itself"*[287].

Por estes motivos, no que tange especificamente o princípio da minimização de dados, o uso da *blockchain* não pode ser considerado incompatível com o RGPD[288]. Neste modo de funcionamento único em que a cadeia de blocos apresenta, o questionamento é o fim desejado de quem a adere. Se o acúmulo de dados ocorrer e desde que coletados para atingir um propósito, e inexistir outra alternativa mais viável e que use menos dados pessoais, a minimização de dados não será violada. Na análise de risco, é uma possibilidade de beneficiar-se significativamente da coleta qualitativa de dados, determinada pela própria arquitetura da rede. A CNIL[289] ainda aventou que o armazenamento fora da própria cadeia, quando a minimização resta difícil de ser justificada, passaria a ser uma justificativa plausível, entretanto, pelos motivos acima expostos, esta solução iria trazer outras questões a serem solucionadas.

No artigo 5.º, n.º .1, d) encontra-se o princípio da exatidão, que cria a exigência tanto por dados precisos, e quando necessário, atualizados. Tendo em vista a inicialização de uma *blockchain*, a utilização de dados precisos é uma questão de governança, não relacionada à tecnologia específica. Acaba por ser uma questão de cuidado e atenção de quem registra dados pessoais na mesma: se o dado inserido for correto, a entidade se beneficia do recurso anti-adulteração da *blockchain*, entretanto quando o dado inserido está inexato, o registro é inalterável. Por estas características, a *blockchain* é uma ferramenta para promover o princípio da exatidão, pela sua própria arquitetura.

Dando prosseguimento à lista de princípios, na alínea e) há talvez o maior desafio de qualquer uso de uma *blockchain*, qual seja o princípio da limitação da conservação. Pela força normativa, os dados pessoais devem apenas ser conservados de uma forma que permita a identificação dos titulares durante o período necessário para as finalidades para as quais são tratados. Apenas pela literalidade da norma, percebe-se a criação da regra que põe o responsável pelo tratamento no denominado "*risk-*

[287] Moerel, Lokke e Marijn Storm. "Why blockchain is not inherently at odds with GDPR" Disponível em https://mofotech.mofo.com/topics/why-blockchain-is-not-inherently-at-odds.html Acesso em 30/06/2020.
[288] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid.
[289] Commission Nationale de l'Informatique et des Libertés. Ibid.

based approach"[290] em que a retenção dos dados é uma decisão de quem o controla, mas a incumbência de demonstrar as finalidades também recai como obrigação legal do responsável. Nota-se, entretanto, a abertura de algumas exceções, nas quais o período de retenção fica estendido, quais sejam, investigação científica ou histórica, ou ainda, para fins estatísticos. E diante deste cenário para respeitar a limitação do armazenamento, teoricamente não deve existir nenhum obstáculo real para a exclusão de todos os registros do livro-razão, onde o apagamento total da *ledger* é uma opção tecnicamente viável.

Uma outra solução, proposta diante desta problemática da ausência de um período de retenção para fins de limitar a conservação, seria armazenar o livro-razão inteiro apenas em uma ou poucas instâncias. Segundo MOEREL propõe em sua obra[291], o problema da limitação seria solucionado se a cada bloco inserido gerasse a instrução aos demais *nodes* para excluir informações no bloco novo que já fora verificado. Segundo a autora, esta ação iria permitir a verificação para inserção do bloco e sem perder as informações do livro-razão completas que podem ser alvo de uma verificação total posterior. Isto seria, segundo a mesma, uma mudança de *design* para aumentar a confidencialidade e economizar capacidade de armazenamento e até reduzir consumo de energia no processo de validação[292].

Voltando aos princípios listados no RGPD, no artigo 5.º, n.º.1, f) desenvolve o princípio da integridade e confidencialidade, que conforme dito anteriormente, a integridade não apresenta empecilho algum e, pelo contrário, o uso da *blockchain* oferece uma excelente opção para garantir a integridade da informação nela registrada. No que tange à confidencialidade, o RGPD elenca expressamente que a garantia de segurança deve evitar tratamento não autorizado ou ilícito, o que significa que na *blockchain* permissionada, cada participante tenha acesso apenas ao suposto. De fato, a essência de um livro-razão distribuído é a desintermediação, que é alcançada transmitindo todas as transações internas e permitindo verificações cruzadas. Portanto, a confidencialidade individual não é o objetivo do mecanismo e não é assim que o princípio deve ser interpretado.

Por outro lado, o foco está em restringir o processamento de informações de transmissão apenas aos supostos participantes, evitando que sejam processadas indevidamente por quaisquer outras partes não relacionadas à *blockchain*, sobretudo se for adotado o modelo de *blockchain*

[290] Quelle fala que esta análise de risco faz as regras e princípios "funcionarem melhor" (tradução livre). Veja-se Quelle, Claudia. "Enhancing compliance under the general data protection regulation: The risky upshot of the accountability-and risk-based approach." European Journal of Risk Regulation vol. 9, n. 3, 2018.

[291] Moerel, Lokke. "Why blockchain is not inherently at odds with GDPR. Blockchain & Data Protection and Why They Are Not on a Collision Course". European Review of Private Law 6-2019, Kluwer Law International BV, Países Baixos, 2019.

[292] Moerel, Lokke. Ibid.

permissionada. Seguindo esta linha, RIBITZK et al, sob a perspectiva de dados sensíveis de saúde, emitiram opinião contrária à *blockchain* pública para fins de confidencialidade, expressamente defendendo que as *blockchain* permissionadas são as mais apropriadas[293].

O perigo alertado em atenção à confidencialidade acaba por ser uma questão de governança, principalmente, no que concerne a existência de participantes "confiáveis" em certas circunstâncias de interesse público. Além disso, para fins de interesse público, onde o uso de uma *blockchain* pode ocorrer por decorrência legal, os legisladores devem incluir disposições que desencorajam qualquer quebra de confidencialidade e, sempre que apropriado, considerar a quebra uma ofensa jurídica. Não obstante, na estruturação da regulação permissionada, no que tange o princípio da segurança da informação, a adoção das devidas medidas adicionais para reforçar a segurança são necessárias.

Uma medida para evitar conluios da maioria dos participantes para evitar falhas no protocolo que sustenta o registro de informações, bem como, limitar o impacto de uma potencial falha de protocolo na segurança das transações seria a opção adequada pelo método de validação a ser utilizado. A doutrina aponta que os *nodes* podem ser subvertidos e tentar deitar a rede abaixo, mandando diferentes resultados para os demais *nodes*.

Se na pior dos cenários de conluio, a rede não resistir aos *nodes* maliciosos, segundo NGUYEN e KIM[294], a rede vai bloquear tais *nodes* e eles não podem mais enviar transações, pois segundo os autores, a utilização de dois algoritmos torna esta rede imune não a tentativas de ataques, mas aos efeitos destes ataques. Nos próprios termos acerca dos protocolos de validação: "*Byzantine fault tolerance based consensus: a kind of consensus that could prevent the cases of crashing nodes and subverted nodes*" e o "*Crash fault tolerance based consensus: a kind of consensus that could only prevent the cases of crashing nodes*"[295].

Diante desta esteira, além de munir-se de adequados protocolos para um possível ataque coordenado, estabelecer procedimentos técnicos e organizacionais[296] para divulgar vulnerabilidades de *softwares* a todos os participantes, incluindo um plano de emergência a ser implementado em caso de vazamento de dados, seria relevante, para os casos a exemplo desta alteração de protocolos quando uma vulnerabilidade é identificada, e para notificar incidentes de segurança e violações de dados

---

[293] Ribitzky, Ron, et al. Pragmatic, Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology: Paving the Future for Healthcare. Disponível em https://blockchainhealthcaretoday.com/index.php/journal/article/view/24/21 Acesso em 30/06/2020.

[294] Nguyen, Giang-Truong; Kyungbaek Kim. "A Survey about Consensus Algorithms Used in Blockchain". Journal of Information processing systems vol. 14, n. 1, 2018. p. 101-128.

[295] Nguyen, Giang-Truong, and Kyungbaek Kim. Ibid. p. 116.

[296] À luz do artigo 32 do RGPD que determina a adoção de "medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco". Veja-se em: Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid

pessoais às respectivas Autoridades de Controlo, sem olvidar de comunicar o incidente aos titulares de dados envolvidos, na forma do artigo 33 do RGPD[297].

Por fim, uma atenção maior à definição das alterações no *software* utilizado para criar transações e para validar as mesmas, o que supostamente deve seguir devida documentação. Inegável perceber que procedimentos técnicos e organizacionais devem ser estabelecidos para garantir um alinhamento entre as permissões planejadas e a aplicação prática naquela finalidade específica, na qual a *blockchain* foi adotada.

3.5 Os Direitos Dos Titulares Dos Dados E A Blockchain

O direito de informação, previsto no RGPD, não aparenta ser problemático em relação a um uso permissionado da *blockchain*, porque a previsão legal estipula que o responsável pelo tratamento tem o dever de prestar informações, de forma concisa e sob um formato acessível e de termos claros[298]. Até o formato de envio para os participantes validadores importa antes de submeter os dados pessoais. E interpretou-se que pelo formato auditável e pelos registros estarem íntegros pela criptografia de alta entropia, o uso *blockchain* não oferece qualquer perigo no que tange o artigo 13 e artigo 14 do RGPD. As informações listadas no artigo 14, n.º 2, RGPD podem ser disponibilizadas pelos termos de uso a serem aceitos antes de baixar um *software* baseado na *blockchain*.

De outro lado, há o direito de acesso, previsto no artigo 15 do RGPD, cuja estipulação determina que o titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito estão sendo tratados e mais algumas informações, dentre as quais, as exatas finalidades. Este direito do artigo 15 RGPD pode ser analisado em conjunto com o direito de portabilidade do artigo 20 RGPD, cuja obrigação é de fornecer dados num formato estruturado, de uso corrente e de leitura automática para permitir a transmissão a outro responsável pelo tratamento, sem qualquer impedimento.

Tais direitos, de diferentes conceituações, são vistos em conjuntos por oferecer a mesma conclusão: não se vislumbra qualquer obstáculo pelo uso da *blockchain*[299], tendo em vista que o próprio *design* conjecturado à cadeia de blocos já facilita o acesso rápido e eficiente pelo participante com

[297] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid.
[298] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid.
[299] "Right of access and the right to portability: the CNIL considers that the exercise of these rights is compatible with blockchains' technical properties". Ver mais em: Commission Nationale de l'Informatique et des Libertés. Ibid

direito para tal que possui a *ledger* em tempo real à sua disposição e poderá realizar a portabilidade do que fora registrado na mesma.

Posicionamento de FINK que apesar de não suscitar obstáculos, ressalvou que deve ser pressuposto a existência de mecanismos adequados de governança, sobretudo no modelo permissionado tal ressalva se faz mais necessária. Nos seus termos, "a princípio, não há obstáculos para o Artigo 15 não ser implementado no que se refere à blockchain. Isto, todavia, pressupõe a existência de adequados mecanismos de governança que permitem uma efetiva comunicação e gestão dos dados"[300].

Superado os direitos acima discutidos, passa-se a analisar outros dois em conjunto: o direito de oposição e o direito ao apagamento, estes que levantam maior polêmica em debates acadêmicos e não acadêmicos. O que conecta os dois direitos é que um indivíduo que exerce devidamente o direito de oposição, previsto no artigo 21 do RGPD, cuja permissão é de se opor a qualquer momento ao tratamento. A solução para se opor a registros feitos na *blockchain* em que os dados estão conectados é, justamente, deletar a cadeia inteira. A conceção de segurança e integridade da *blockchain* reside nesta interconexão das suas partículas, os blocos, e é tecnicamente ineficiente modificar blocos e manter a integridade do sistema como um todo, o que conduz a um caminho de que a solução para usar a *blockchain* em conformidade com o direito de oposição, e consequentemente o direito de apagamento, será adotar uma arquitetura que pense na privacidade desde a "conceção e por defeito", em atenção ao artigo 25.

Por isso, se a disposição interligada cria uma dificuldade de apagar uma parte sem comprometer o resto, precisa-se pensar em uma utilização que consiga uma solução para o todo. FINK ressaltou que *"*a dificuldade de implementar o Artigo 17 do RGPD é devido a fatores técnicos, mas também por conta do design de governança"[301], ou seja, os desafios de compatibilização do direito ao apagamento com algum uso da *blockchain* recai, primordialmente, no modelo de regulação que foi optado desde a conceção.

Pensando no problema da integralidade, a CNIL considerou que é tecnicamente impraticável responder ao requerimento de apagamento feito por um titular dos dados quando os dados estão registrados na cadeia, sem deletá-la por completo, tendo em vista sua propriedade característica de forte integridade garantida através de ligações criptográficas entre os blocos e os respectivos códigos *hash*. E em busca de uma solução, a CNIL reiterou que se os dados forem armazenados através de um

[300] Fink, Michèle. Ibid. p. 76 (Tradução livre)
[301] Fink, Michèle. Ibid. p. 79 (Tradução livre)

esquema de comprometimento e de forma cifrada através de um código *hash*, tornando o dado ilegível em *cleartext*, o responsável pelo tratamento praticamente torna a informação inacessível, chegando perto de obedecer ao apagamento. Do ponto de vista técnico-jurídico, pode-se criticar este posicionamento a dizer que chegar perto de um direito, não significa observá-lo. Por isso que seria mais producente por parte das Autoridades encararem o uso da cifragem como uma forma de retirar aquele tratamento do âmbito material do RGPD, ao invés de recomendar aos responsáveis pelo tratamento uma solução que ofereça uma quase observância de um direito.

Ao reconhecer o problema sobretudo de apagar um bloco que esteja com dados em texto claro, a CNIL destacadamente recomendou não registrar os dados de forma legível na *blockchain*, além da utilização de alguma das soluções criptográficas anteriormente mencionadas. E deste empecilho, surge outro direito que resta comprometido em uma utilização da *blockchain* no modelo de governança pública, onde os dados são legíveis e não existe níveis de diferenciação entre os participantes, a saber o direito à retificação previsto no artigo 16 do RGPD.

Salienta-se que o Regulamento prevê que o titular tem o direito de "obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito"[302]. Se a *blockchain* for devidamente analisada, vai-se entender que a mesma é um processo, um bloco não existe por si só e um titular dos dados tem todo direito de exigir que o registro entregue uma informação correta sobre ele, por isso que um bloco que registre algo posteriormente, corrigindo bloco anterior, cumpre a lógica de que naquele registro específico que é feito na *blockchain*, a informação final está correta, mesmo que bloco anterior contenha dado pessoal desatualizado.

A CNIL, entretanto, apesar de reconhecer que uma transação subsequente pode cancelar uma transação anterior, ainda que aquela anterior permaneça na cadeia, defende a impossibilidade de modificar um bloco da cadeia sem gerar um novo bloco, seguindo a essência do conceito definido no caso *Nowak*[303]. Em casos extremos, precisar-se-ia realizar um *hard-fork* em busca de retificar o fluxo dos registros. Aproximou-se o pedido de exclusão de dados, ao pedido de retificação, o que coloca este último numa situação mais difícil do que deveria, afinal o apagamento mostra mais obstáculos para ser solucionado senão for pensado desde a conceção do registro que utilize a *blockchain*, ao contrário da retificação, que dependendo do caso concreto, pode ser solucionada com um simples registro posterior.

---

[302] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid. Artigo 16.

[303] "Nowak case, Advocate General Kokott argued that the right to rectification ought to be 'judged by reference to the purpose for which the data was collected and processed". Veja-se Opinião de AG Kokott em Acórdao TJUE, Peter Nowak, de 20 de dezembro de 2017, processo C-434/16, Considerando 35.

Por fim, houve a atenção para o direito do artigo 22 do RGPD, designadamente o de não ficar sujeito a decisões individuais automatizadas[304], incluindo definição de perfis. Um dos usos recorrentes, inclusive, da *blockchain* passou a ser os *smart contracts* que são considerados inteligentes por apenas automatizar a execução de uma regra/acordo. E diante deste cenário, medidas adequadas para salvaguardar os direitos e liberdades e interesses legítimos do titular dos dados precisam ser observadas neste aspecto. Quando o *smart contract* produz uma decisão de efeitos legais[305], o titular dos dados deve poder obter intervenção humana, expressar seu ponto de vista e contestar a decisão após a execução do contrato inteligente. O responsável pelo tratamento (ou os diversos responsáveis) deverá, por força do artigo 22, fornecer a possibilidade de intervenção humana, permitindo que o titular dos dados conteste a decisão, mesmo que o contrato já tenha sido executado e independentemente do que está registrado na *blockchain*.

Contudo, uma questão desta problemática surge, qual seja a circunstância específica de quando o contrato é celebrado pelo próprio titular dos dados, funcionando a plataforma *blockchain* como uma modalidade de executar um comando já celebrado contratualmente. De fato, os contratos oferecem várias fases, prévias e posteriores inclusive, mas se toda a manifestação de vontade já foi declarada e o *smart contract* é apenas uma forma mecanizada de executar uma decisão tomada pelo próprio titular dos dados, não há de que se falar em "decisão automatizada", conceito elementar para separar um algoritmo simples de um sistema de inteligência artificial dotado de poder de decisão, que se aplica para separar uma ação prevista em *smart contract* da decisão com efeitos jurídicos frutos de um sistema autônomo.

3.6 Proteção De Dados Desde A Conceção E Por Defeito

A opção legislativa assentou a Proteção de dados no centro destes conceitos, o que significa que os responsáveis pelo tratamento devem ser capazes de demonstrar que implementaram medidas *ad hoc* em observância aos princípios regulamentados[306]. Não obstante, cada salvaguarda específica deve ser pensada para garantir os direitos e liberdades dos indivíduos, inclusive em circunstâncias que

[304] Já tinha sido definido no Grupo de trabalho do artigo 29.° para a proteção de dados: "the ability to make decisions by technological means without human involvement". Ver mais em Europeia, União. Grupo de trabalho do artigo 29.° para a proteção de dados. "Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679". Vol. 1, p. 8.

[305] Conforme Fink expressamente definiu "smart contract produces a 'decision' having legal or otherwise significant effects, this form of purely automated decision-making". Para mais desenvolvimento, veja-se: Fink, Michèle. Ibid.

[306] Não apenas adotar medidas, mas instruir os parceiros comerciais para que o responsável pelo tratamento atinja suas obrigações legais. Neste sentido, veja-se Moerel, Lokke. Ibid.

comumente as técnicas de implementação não teriam sido devidamente aplicadas para um tratamento eficaz e necessário dos dados pessoais. A Autoridade francesa preferiu adotar uma visão cuidadosa, deixando evidente que busca um princípio de efeitos não apenas genéricos, mas sim, que determina um cumprimento formal e demonstrável do RGPD, desde fases preparatórias.

E nesta ótica, o princípio acaba tendo efeito direto na *blockchain*, uma vez que a tecnologia é desafiada pela sua própria natureza de implementar regras que precisam ser observadas, sem afastar a *blockchain* da sua essência de um livro-razão distribuído e descentralizado. A implementação de alguns princípios, a exemplo da minimização e limitação de propósito, precisa ser pensada desde o desenvolvimento de qualquer tecnologia que possa servir de plataforma para tratamento de dados pessoais.

E dentre os obstáculos que a natureza da *blockchain* pode ter evidenciado perante o RGPD, ao terem sido propostos *designs* de regulação em que o direito de exclusão poderia ser atendido, assim a *blockchain* pode ser compatível com o artigo 17 do RGPD, caso este regramento seja aplicável materialmente. Fala-se comumente em um conflito aparente entre o direito de exclusão e a *blockchain*, todavia, é imperioso destacar o efeito do princípio do artigo 25 RGPD como elemento definidor neste contexto.

No caso de uma transação mediada ou em uma transação direta, a exclusão de dados individuais é possível e basicamente igual a eliminação de dados (até a destruição do dispositivo onde os dados são armazenados). Todavia, em um ambiente desintermediado, caso o modo de envio dos dados pessoais seja somente para um livro-razão distribuído, essa exclusão individual não é possível. A exclusão global na *blockchain* é, sim, possível de ser programada, ocorrendo de uma forma interligada. Em outras palavras, a exclusão acaba por ser mais viável se feita em totalidade, o que significa que na exclusão de um único bloco, a exclusão de toda a cadeia deve ser tecnicamente necessária.

Se nada impede a exclusão total da cadeia, a atenção deve estar voltada ao efeito desta supressão. E é por isso que o envio de dados que podem ser utilizados apenas no contexto específico da *blockchain* (dado de uso único), em formato não interoperável em contextos diversos, apresenta possível solução satisfatória para atender a exclusão de dados individuais. Relevante destacar que não se pode estender o direito ao apagamento de dados para os dados de outros sujeitos, sendo que na lógica de interligação existente na *blockchain*, a exclusão de dados referentes a um bloco resta impossibilitada após uma transação posterior de dados ter sido realizada.

De toda forma, enviar dados não interoperáveis de utilização única acaba por ser considerado similar ao de apagamento dos dados pessoais, sem significar a exclusão total do livro-razão distribuído,

entretanto surge a problemática da quase observância de um direito, acima mencionada. Esta dificuldade já fora prevista em RAMOS e SILVA[307] que enxergaram, especificamente nas circunstâncias da *blockchain* pública, um obstáculo aos titulares dos dados que desejem exercitar o seu direito ao apagamento.

A seguir outra rota, um dos caminhos anteriormente proposto, acerca da ZKP, já pode ser categorizado como técnica que vai além. Provar com conhecimento zero significa conseguir a síntese de como ocorre o fluxo de dados pessoais, para fins de criar comprometimentos vinculativos sobre valores de dados válidos apenas para as partes envolvidas em uma transação, ao mesmo tempo em que não produzem significado para nenhuma outra parte. A forma de provar criptograficamente um valor, sem revelar o conteúdo do mesmo, vai ser uma maneira que respeita o RGPD e afasta o tratamento de dados ao âmbito material do Regulamento, e é por isso que os responsáveis pelo tratamento devem, segundo as Autoridades de Controlo, buscar aplicar as técnicas mencionadas no contexto da *blockchain*.

O uso da *blockchain*, sem desconsiderar o potencial dessa tecnologia, deve respeito aos direitos dos titulares de dados. Mas para cada *blockchain* que resolva seguir a forma de regulação recomendada de ser permissionada e com fins de utilizar o mecanismo de prova de conhecimento zero, deve-se enaltecer que esta decisão não pode ser superveniente, não cabe improvisos. E é por isso que este debate é indissociável do tópico do assunto previsto no artigo 25 RGPD. A adoção de um *design* que valida transações e realiza registros através do protocolo ZKP precisa ser concebido desde o momento em que o responsável pelo tratamento define os meios e propósitos do tratamento, ou seja, o princípio da "proteção de dados desde a conceção", previsto no artigo 25 do RGPD.

Além do mais, a criação de esquemas de certificação para os diversos contextos em que uma *blockchain* pode ser implementada são recomendados para ser alcançado um uso em conformidade com o RGPD. Qualquer adoção da *blockchain*, além de observar a proteção de dados por defeito, ainda irá abrandar a complexidade dos mecanismos adotados e vai permitir os responsáveis pelo tratamento a dialogar construtivamente com as partes interessadas.

Por tudo que já foi exposto, pode-se, a esta altura, afirmar que certos usos da *blockchain* podem utilizar técnicas que apresentam maior responsabilização e soluções operacionais ao problema da aparente incompatibilidade daquela tecnologia com o regime europeu da proteção de dados. A conformidade no uso da *blockchain* será uma análise de risco de quem a desenvolve que, pelas regras

[307] "This may present serious obstacles for the data subjects who wish to exercise their right to be forgotten". Ramos, Luis Felipe M.; SILVA, João Marco C. Ibid. p. 4.

do artigo 25 do RGPD, deve pensar em medidas técnicas e organizativas para promover a denominada proteção de dados desde a conceção e por defeito. Ante os desafios levantados, uma estrutura que consiga responder a alguns recorrentes questionamentos sobre a *blockchain*, qual seja o direito consagrado no artigo 17 do Regulamento (apagamento dos dados), seria importante para fins de adequação. Adicionalmente, a entender que ao enviar dados não interoperáveis de utilização única, ou utilizar técnicas de cifragem com exclusão da chave respectiva, seria adotar um procedimento diverso, mas com os mesmos efeitos jurídicos que o apagamento dos dados pessoais.

Passado por este e outros pontos sensíveis, chega-se a modelos de *blockchain* que oferecem uma maior segurança jurídica, por simplesmente oferecerem medidas técnicas e organizativas que vislumbram a aplicação com eficácia dos princípios da proteção de dados, sem olvidar de oferecer as garantias necessárias ao tratamento, de uma forma que este procedimento cumpra os requisitos do RGPD e proteja os direitos dos titulares dos dados. E esta observância legal é essencial para a adoção pela Administração Pública.

Caso o tratamento seja de dados anonimizados, a problemática resta mais facilitada ainda, uma vez que não irá incidir o Regulamento e consequentemente os princípios e direitos dos titulares são inexequíveis, pela inexistência de uma pessoa singular identificada ou identificável, e por conseguinte, ausência de dado pessoal *per si*. E é tendo todas as nuances teóricas em vista que se passa a tratar da *blockchain* como uma solução de mais transparência à Administração Pública, sob a ótica do combate à corrupção, que mesmo sendo do paradigma do Direito Público, os usos da *blockchain* devem atender os princípios e direitos dos titulares, caso o RGPD seja aplicável ao tratamento.

CAPÍTULO IV

4.1 Incorporação de novas tecnologias pelo setor público

Visto que dentre os modelos de *blockchain* mais recomendáveis, encontram-se os que oferecerem medidas técnicas e organizativas mais eficazes na proteção dos princípios e direitos dos titulares, é preciso arrazoar utilizações da *blockchain*, num ponto de vista prático e mais específico, para servir ao Estado no escopo de gerar mais transparência na Administração Pública e, possivelmente, gerar mais confiança institucional e dificultar a prática da improbidade administrativa.

Sob uma perspectiva histórica, pode-se vislumbrar que a *blockchain* surge no contexto da iniciativa privada (a criptomoeda Bitcoin foi o primeiro uso conhecido da *blockchain*, que com ela não se confunde[308]), entretanto passa a ser suscitada em outro panorama: no setor público. A célebre dicotomia público-privado, que ocorreu no "período do Estado Liberal, não funciona propriamente nos dias atuais"[309] criando um "complexo público-privado"[310]. Segundo LIMBERGER, depois da criação do Estado constitucional, todo o século XIX foi uma construção jurídica com a finalidade de normatizar os poderes estatais[311].

Entretanto, segundo o autor, ao final do século XX ficou evidenciado um "desmantelamento destes controles e a ausência de construção de mecanismos eficientes"[312]. Seria um sintoma governamental da modernidade líquida de BAUMAN[313], em que as instituições que conjugam relações entre agentes públicos, mas também Administrado-Administrador, estariam mais frágeis por não seguir o mesmo ritmo, passando pela possível demora do Estado em incorporar novas tecnologias.

Acelerar a inovação no Governo e incorporar novas tecnologias no setor público é uma luta dos últimos anos[314], afinal o setor privado acaba por se desenvolver tecnologicamente de forma mais rápida, com a introdução de novos produtos e serviços, além de inovar seus modelos de negócios. No setor público, a inovação também deve existir para tentar acompanhar as demandas sociais cada vez mais céleres, entretanto o processo de inovação passa pela edição de leis e regulamentos por parte do

[308] Houben, R.; Snyers, A. "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion". Parlamento Europeu, 2018. p. 24

[309] Limberger, Têmis. "Transparência administrativa e novas tecnologias: o dever de publicidade, o direito a ser informado e o princípio democrático." Revista de Direito Administrativo, n. 244, 2007, p. 255

[310] García-Pelayo, Manuel. "Las transformaciones del Estado contemporâneo". Madrid: Alianza, vol. 3, 1982. p. 25

[311] Limberger, Têmis. Ibid. p. 255

[312] Limberger, Têmis. Ibid. p. 255

[313] Bauman, Zygmunt. "Modernidade líquida". Rio de Janeiro: Jorge Zahar, 2001.

[314] Segundo West, a burocracia é um dos fatores que impede a adoção de novas tecnologias no setor público em West, Darrell M. "Digital government: Technology and public sector performance". Nova Jersey: Princeton University Press, 2005.

Legislativo e implementação de políticas públicas que orientem os processos administrativos com base na introdução de novas tecnologias, por parte do Executivo, como bem observam MOMO et al[315].

O fato de existir uma Administração Pública que consegue introduzir novos processos tecnológicos para tornar a própria prestação do múnus público algo mais escalável e célere, e desta forma, corresponder às novas demandas sociais, para VIEIRA et al[316], existe relação direta com um incremento da democracia. Isto ganha sentido a partir do momento em que se discerne um dos fundamentos do Direito Administrativo que regula a relação entre Estado e particular: a "supremacia do interesse público"[317]. A democracia resta fortalecida quando os representados vivem em uma sociedade, na qual os seus representantes entendem e acompanham suas demandas, e por isso que pelo fato de se viver atualmente em uma sociedade da informação (termo este cunhado por Daniel Bell ainda na década de 1970[318]), é importante que o Estado busque se atualizar.

Diante do exposto, é natural existir a pauta tecnológica que cresce e pressiona o Estado a mudanças institucionais centradas na tecnologia. De acordo com SCHWAB[319], uma Revolução Industrial teve início na virada do século, sendo a de número 4 na história, cuja estampa foi justamente ser baseada em uma Revolução Digital. Por mais que a Administração Pública, pelos motivos estruturais já expostos, apresente uma dificuldade maior em incorporar novos processos tecnológicos[320], a inovação é uma forte corrente entre os administrativistas que, diante de tantas soluções, elegem a *blockchain* como uma ferramenta capaz de conferir confiabilidade e segurança aos dados[321]. O desafio comumente suscitado é justamente lidar com a dicotomia que se apresenta quando questionada a *blockchain* conforme o regime da proteção de dados mas, ao mesmo tempo, questiona-se quanto a certos problemas da Administração Pública, inclusive em relação aos dados dos cidadãos, e de que forma poderiam ser assegurados por esta mesma tecnologia.

De imediato, ao detalhar que a *blockchain*, conforme já explicado, gera uma chave criptografada única a partir de uma rede de verificação de aceitabilidade do código, tornando a transação segura e irreversível[322], é possível vislumbrar várias dificuldades da Administração Pública

---

[315] Momo, F. S.; Schiavi, G. S.; Behr, A.; Lucena, P. "Business models and blockchain: What can change?" Revista de Administração Contemporânea, vol. 23, n. 2, 2019, pp. 228-248.

[316] Vieira, F. M.; Santos, V. V. B. "Governo eletrônico: A busca por um governo mais transparente e democrático". Congresso Consad de Gestão Pública, Brasília, DF, Brasil, p. 3.

[317] Ávila, Humberto. "Repensando o princípio da supremacia do interesse público sobre o particular." Revista trimestral de direito público, vol. 24, 1999. p. 159.

[318] Bell, Daniel. "O advento da sociedade pós-industrial: uma tentativa de previsão social". São Paulo: Cultrix, 1977.

[319] Schwab, K. "A quarta revolução industrial". São Paulo: Edipro, vol. 1, 2016

[320] Segundo os ensinamentos de West, Darell, ibid.

[321] Moura, Luzia Menegotto Frick de, et al. Ibid. pp. 259-274.

[322] Neste sentido, veja-se: Swan, M. "Blockchain: blueprint for a new economy" Sebastopol: O'reilly, vol. 1, 2015.

que a *blockchain* poderá solucionar. Assim como o princípio da legalidade que assume relevância em diversas searas, a transparência é um princípio polivalente que dialoga e, de certa maneira, complementa a estrita observância à lei, uma vez que indivíduos e instituições, além de deverem respeito às normas positivadas, devem buscar, dentre suas particularidades, meios hábeis a demonstrar de forma transparente o cumprimento de regras e princípios.

Na perspectiva do Direito Público, esta relação legalidade-transparência fica ainda mais exacerbada, uma vez que as pessoas jurídicas de natureza pública precisam prestar contas e divulgar, por força de lei, não apenas estatísticas, mas índices de eficiência. Para citar como exemplo, a Lei de Responsabilidade Fiscal brasileira[323] visou disciplinar os gastos do administrador público, mas sedimentou a importante ideia de transparência na gestão fiscal.

Nesta abordagem, acaba-se por conferir efetividade ao princípio da publicidade, norteador da Administração Pública[324], mas também se conjugam noções de participação popular em setores estratégicos da gestão do Erário público, o que permite gerar uma noção desejada de maior controle social. O próprio cidadão, por ter acesso a fiscalizar, e até por poder escolher formas de gerir o patrimônio público[325], acaba por funcionar como uma concretização do princípio republicano, tendo em conta que se o interesse público para a verdadeiramente administrar a *"res publica*", a República resta fortalecida.

Uma ligação plausível é a que a falta de transparência na Administração Pública acaba por conduzir a um aumento na corrupção[326]. E eis que o supramencionado controle social encontra na noção concebida pelo direito anglo-saxão, que diz respeito à *accountability*[827], um real caminho para concretização. Segundo LIMBERGER[328], existe uma comprovada relação nos países com informação mais transparente sendo os que apresentam menores índices de corrupção. Para ilustrar, o autor cita um estudo realizado pela organização não governamental Transparency Internacional, cujo objeto de análise envolveu a graduação de 159 países em uma escala de zero a dez para o nível de transparência do serviço público e a conclusão foi que quanto menor a nota recebida (leia-se quanto menor a transparência pública), maior era o índice de corrupção[329].

---

[323] Brasil. Lei Complementar, n. 101, 4 maio 2000. LRF – Lei de Responsabilidade Fiscal, Brasília.

[324] Di Pietro, Maria Sylvia Zanella. "Direito administrativo". São Paulo: Atlas, vol. 11, 1999. pp. 115-116.

[325] Neste sentido, da Silva Figueiredo, Vanuza; Waldir Jorge Ladeira dos Santos. "Transparência e controle social na administração pública." Temas de Administração Pública, vol. 8, n. 1, 2013.

[326] Lalountas, "Corruption, globalization and development: How are these three phenomena related?." Journal of Policy Modeling 33.4 (2011): 636-648.

[327] Pederiva, João Henrique. Accountability, Constituição e contabilidade. Revista de Informação Legislativa, Brasília, v. 140, p. 18, 1998

[328] Limberger, Têmis. "Transparência administrativa e novas tecnologias: o dever de publicidade, o direito a ser informado e o princípio democrático." Revista de Direito Administrativo 244 (2007): 259

[329] Transparency International 2020. Disponível em https://www.transparency.org/en/ Acesso em 24 de maio de 2020

Em termos diversos, a transparência insuficiente do Estado é um fator de afastamento do cidadão em relação à gestão pública, o que escancara uma relação contraditória por si só: a coisa pública "pertence" ao representante eleito e não ao representado eleitor, os patrimônios se confundem e o interesse particular passa a guiar as políticas públicas. A corrupção é uma inversão de valores. Uma inversão de valores que pode atingir vários níveis, sendo um dos mais críticos quando passa a ser institucionalmente aceite, e deste ponto, a sociedade passa a conviver com um sistema endêmico de corrupção.

Muitos cidadãos em meio a este contexto sentem-se revoltados, outros entram em um processo de desinteresse e acabam por se afastar, o que de uma forma ou de outra, acaba por ser consequência de falta de transparência e *accountability* na gestão pública. E é neste sentido que KAUFMANN já argumentou que: *"*se não existe transparência, a corrupção vai ser gerada e fortalecida, especialmente se existir relevante uma estrutura institucional que não promova as necessárias medidas para salvaguardar a Administração contra a corrupção"[330].

E neste contexto, o desenvolvimento tecnológico dos últimos anos causou, segundo PÉREZ LUÑO[331], uma ressignificação das relações de cidadania e da relação dos entes públicos com os administrados, sendo que, na visão deste autor, o próprio conceito de cidadania reclama uma redefinição. Se a cidadania merecer ser redefinida, a Administração Pública precisa acompanhar este processo, pois uma pressupõe a outra.

E para supor uma democracia que atenda às demandas do mundo digital, precisa-se, basicamente, desenvolver o uso da tecnologia por dois pontos de vista: (i) sobre a utilização de novas tecnologias por parte da própria Administração Pública, as quais ofereçam transparência e responsabilização dos gestores nos mais diversos usos (a fim de órgãos de controle e o próprio cidadão possa averiguar os propósitos lícitos e adequados); (ii) por outro lado, a utilização de novas tecnologias por parte do próprio cidadão, a fim de aproximá-lo da prestação personalizada de serviços públicos em linha e da efetivação do supramencionado controle social da gestão pública[332].

E neste contexto individual do paradigma do cidadão, existem diversos obstáculos, uma vez que o acesso à internet não é universal, e quando ocorre, muitas vezes, é sem literacia por parte dos utilizadores. E, por isso, o exercício de uma cidadania eletrônica ou cibercidadania, nos termos de

[330] Kaufmann, D.; Siegelbaum, P. "Privatization and corruption in transition economies". Journal of International Affairs, Vol. 50, n. 2, 1997. pp. 419-458. (Tradução livre)
[331] Pérez Luno, Antonio-Enrique. "¡Ciberciudadanía@ o Ciudadanía@.com?" Barcelona: Editorial Gedisa, 2004. p. 11.
[332] Figueiredo, Vanuza da Silva et al. Ibid.

LUÑO[333], resta comprometida se a utilização das novas tecnologias reste impossibilitada pela ausência de preparo dos cidadãos. Desta problemática, surge o desafio de "construção de uma sociedade mais solidária, justa e democrática"[334]. Se algum uso tecnológico puder exercer um papel na democratização da informação, de forma transparente e segura, sobretudo baseado na lei como fundamentação legal, acaba por ser uma ferramenta crucial no desenvolvimento de uma sociedade mais justa, em consequência de uma Administração Pública mais democrática e eficiente.

Diante do exposto, traz-se a *blockchain* como uma das possíveis ferramentas na busca por aperfeiçoar a Administração Pública, nos diversos pontos críticos acima mencionados, afinal é necessário, a esta altura, pensar como a *blockchain* poderá promover maior transparência da gestão pública, se é possível aplicar a responsabilização em algum uso estatal da *blockchain*, assim como democratizar a informação por meio desta noção da cadeia de blocos descentralizada e distribuída, e também, como diminuir níveis de corrupção pelo uso indevido do patrimônio público através de soluções centradas na *blockchain*.

Não obstante, precisa-se mencionar plataformas de fiscalização e registros que ofereçam segurança jurídica contra alteração indevida e sejam fáceis de serem acompanhadas pelos maiores interessados na adequada gestão do patrimônio público: os próprios indivíduos enquanto aqueles que confiam que seus representantes obedecem ao princípio da supremacia do interesse público que rege o Direito Administrativo[335].

4.2 Blockchain e sua aplicação na Administração Pública

Não se pode partir de uma premissa que a *blockchain* pode oferecer uma solução para todos os problemas, afinal toda tecnologia demanda uma utilização concreta para poder ser considerada como uma solução positiva. Conforme já explanado anteriormente, a *blockchain* é uma forma diferente de registro, que dentro deste conceito, poderá assumir diversos modelos, desde um completamente aberto e sem qualquer entidade regulatória, até um modelo permissionado com utilizadores sob diversas categorias, que, conforme os ensinamentos de WIRTH & KOLAIN, apresentam uma entidade

[333] Pérez Luno, Antonio-Enrique. Ibid. p. 101
[334] Limberger, Têmis. Ibid. p. 260
[335] Neste sentido, veja-seos de Di Pietro, Maria Sylvia Zanella; Ribeiro, Carlos Vinícius Alves. "Supremacia do interesse público e outros temas relevantes do direito administrativo". São Paulo: Atlas, 2010.

para manejar a infraestrutura de concessão de chaves, potencialmente determinando os propósitos e meios do tratamento de dados na *blockchain* permissionada[336].

A *blockchain* oferece uma tecnologia com potencial de proporcionar segurança no armazenamento e gerenciamento de dados públicos auditáveis, uma vez que os registros são criptograficamente desenhados para não serem alterados, podendo oferecer, através da natureza descentralizada, uma segurança aos arquivos da Administração Pública. Desta forma, o escopo é evitar que um ataque ilícito direcionado adultere alguma base de dados estatal específica, uma vez que a cópia do registro está descentralizada e atualizada simultaneamente dentre os *nodes* da rede. Adicionalmente, a forma criptográfica de promover o registro facilita a auditoria, uma vez que fica registrado o endereço de quem inseriu o bloco na cadeia, sendo possível realizar a ação regressiva para averiguar que órgão público, ou até mesmo que servidor (caso seja necessário e adequado juridicamente), é que realizou tal entrada.

PRZEYBILOVICZ et al[337], em sua obra, relatam os desafios de usar as tecnologias da informação para o desenvolvimento de uma Administração Pública em linha, chamada pelos autores de "Governo Eletrônico"[338]. O trabalho de implementação da *blockchain* deve observar o caminho traçado pelos autores, no qual o contexto legal e socioeconômico deve ser levado em consideração, assim como os atores envolvidos e a capacidade institucional dos órgãos participantes. Este pensamento se complementa com um movimento que SILVEIRA e ABREU chamam de rejuvenescimento da União Europeia, a tentar se tornar uma Europa digital, onde a tecnologia é popularmente adotada[339].

Por isso, desde logo se afirma que a *blockchain* jamais pode ser acreditada como uma fórmula pronta a ser aplicada por todo o órgão público. Levando em consideração todas as circunstâncias, a *blockchain* poderá ser escolhida como uma forma de registrar dados do poder público, e assim o sendo, será uma análise de risco feita pelo administrador público, preferencialmente no formato do artigo 35 RGPD, considerando titulares de dados envolvidos e se a instituição pública em questão apresenta capacidade para esta implementação.

E, portanto, não cabe averiguar se a *blockchain* de forma geral e abstrata pode ser implantada pela Administração pública também *lato sensu*, considerando que a *blockchain* depende de uma

---

[336] Para Wirth, Christian; Michael Kolain. Ibid: a entidade de controle por definir "purposes and means"

[337] Przeybilovicz, E., Cunha; M. A., Meirelles; et al. "The use of information and communication technology to characterize municipalities: Who they are and what they need to develop e-government and smart city initiatives". Revista de Administração Pública, vol. 52, n. 4, 2018. pp. 630-649.

[338] Przeybilovicz, E., Cunha; M. A., Meirelles; et al. Ibid. pp. 630-649

[339] Abreu, Joana Covelo; Silveira, Alessandra. "Interoperability solutions under Digital Single Market: European e-Justice rethought under e-Governance paradigm". European Journal of Law and Technology, v. 9, n. 1, 2018. Tradução livre

utilização concreta, a fim de delimitar as particularidades das diversas variáveis que ela poderá assumir, a saber desde a arquitetura pensada até as regras de regulação, qual protocolo de registro será adotado ou até se é necessário utilizar mecanismos de anonimização para fins de assegurar a proteção dos dados pessoais dos titulares envolvidos. Não apenas a *blockchain* se considera conceito abstrato que precisa de concretização, consoante ocasiões do caso em concreto, mas também a Administração Pública demanda delimitações fidedignas com a realidade, uma vez que possui uma infinidade de tipos de atos administrativos, autoridades, órgãos e demais institutos da doutrina administrativista[340].

Primeira característica, anteriormente mencionada, diz respeito à segurança no armazenamento e gerenciamento de dados públicos a fim de que eles sejam auditáveis. Nesta senda, precisa-se vislumbrar como a atual Administração Pública estrategicamente define os meios para armazenar os dados públicos. A base do registro público ocorre através da responsabilidade das próprias estruturas das pessoas coletivas, ou de outras entidades que, por força de lei, acabam por exercer essa funcionalidade pública.

Neste sentido, o próprio esqueleto desta gestão pública pode vir a ser um conceito diverso ao da *blockchain*, definição esta que decorre da ideia de esta tecnologia pressupor uma ruptura. A Administração Pública funciona consoante o método do livro-razão das partidas dobradas[341], uma vez que cada registro vai ser centralizado em uma dessas instituições ou órgãos públicos. Na relação do Erário público com os administrados irá haver a figura de um terceiro de confiança investido de poder estatal, a fim de validar transações e certificar situações de fato e de direito através de seus instrumentos próprios.

De maneira a exemplificar, uma entidade que exerce o papel de confiança vai, através da fé pública legalmente conferida[342], armazenar os bens, emitir declarações ou outros instrumentos cabíveis, a fim de criar, modificar ou extinguir direitos. A deficiência deste processo é histórica por ter sido construída à luz da própria noção de Estado: entidades oneram o Erário público sob a cátedra de exercer a função de intermediário de confiança no registro de dados e transações.

Existe uma parte significativa do arcabouço estatal que funciona apenas para essa função de registrar livros de forma centralizada e certificar de acordo com a partida dobrada, tudo que fizer

[340] Conforme listado na obra de: Di Pietro, Maria Sylvia Zanella. Ibid.

[341] Carqueja, Hernâni O. Ibid. pp. 465-496

[342] Segundo Lopes: "A fé pública decorre, pois, das disposições da lei civil que a conferem aos actos e declarações de certos funcionários (...) A fé pública implica uma presunção dupla, ou seja, a de que o registo é integral, isto é, de que nada existe para além dele, e a de que o registo é exacto, e portanto conforme à realidade extraregistral". Veja-se Lopes, J. de Seabra. "Direito dos Registos e do Notariado". Coimbra: Almedina, vol. 2, 2003.

referência ao que for registrado, precisa corresponder ao registro governamental[343]. A gestão de dados de interesse público, nesta conceção, vai necessitar necessariamente de um armazenamento principal: a exemplo do casamento civil que vai ser armazenado pela conservatória de registro civil, ou seja, por uma intermediária de confiança. Estruturar uma pessoa coletiva exclusivamente para centralizar registros, a princípio, é um ônus ordinário, mas significativo, ao Erário público.

E pelo viés qualitativo da descentralização, o registro centralizado de informações de interesse público não apenas onera o patrimônio público com a necessidade de constituição de diversos órgãos e instituições com o dever de atestar e certificar transações armazenadas de forma não distribuída. O registro descentralizado, quer seja através da *blockchain* ou não*,* tem o potencial de "reduzir o papel de um dos mais importantes atores econômicos e regulatórios na nossa sociedade - o intermediário"[344]. Quando a base de dados está centralizada, oferece-se ao processo de adulteração apenas um alvo, em detrimento da forma pensada para a *blockchain*, afinal um simples acesso ilegítimo a uma base de dados centralizada de um órgão público que se obtém total controle aos dados e transações nela armazenados.

A *blockchain*, pelas características anteriormente já desenvolvidas, oferece uma cadeia de registros em que cada bloco de transação permanece criptograficamente interligado ao subsequente e uma possível adulteração será perceptível pelo próprio sistema à luz da incompatibilidade no código *hash*. E, por este motivo, além da acima mencionada virtual redução de despesa com a estrutura administrativa, a *blockchain* poderá oferecer à Administração Pública um instrumento que consegue evitar adulteração de informações, estatísticas, atos administrativos ou qualquer outro dado que o Estado armazena, lesando o patrimônio público, promovendo o favorecimento pessoal ou visando qualquer outro fim ilícito.

E sob o ponto de vista publicista, a problemática do armazenamento tradicional vai ser abordada de forma diferenciada pelo uso da *blockchain*. Mesmo que não seja adotado o *design* de regulação totalmente público, por essência, a *blockchain* vai constituir um registro descentralizado entre vários *nodes*. E é por essa característica da descentralização que uma adulteração na base de dados governamental vai ser prontamente notada e restar sem efeito, uma vez que os outros *nodes* detêm em tempo real uma cópia fidedigna da cadeia de blocos.

---

343 Conforme detalhado em Vigna, Paul; Casey, Michael J. Ibid.

344 Wright, Aaron; De Filippi, Primavera, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 2015 in Taufick, Roberto Domingos. "Mercado de Loterias no Brasil: concorrência, governança e responsabilidade social na era de blockchain". Brasília: Escola Nacional de Administração Pública, Diss., 2019. p. 18.

Aumentar segurança e transparência na gestão pública acaba por ser uma forma de efetivar o princípio da eficiência da Administração Pública. Então, a propositura de uma adoção da *blockchain* representa uma modificação funcional administrativa, remetendo à ideia de que "o princípio da eficiência possui o condão de gerar mudanças no comportamento funcional da Administração"[345]. Por outro lado, caso seja possível, se o cidadão for tornado um *node* deste processo, com uma cópia simultânea de toda a cadeia de registros, princípios democrático e de participação popular efetiva vão estar mais próximos de serem observados.

De acordo com ALLESSIE et al[346], se for realizado um levantamento de projetos para averiguar em que setores públicos a aplicação da *blockchain* já vem sendo possível, sobretudo por referência à Administração Pública europeia, nota-se uma lista diversificada: protótipos da *blockchain* em serviços notariais, bases distribuídas e *smart-contracts* para registro e transferência de propriedades de terras, certidões acadêmicas, pagamentos governamentais e até mesmo sistemas por completo de identidades baseadas na referida tecnologia em questão. Contudo, a investigação dos autores concluiu que, apesar de muitos projetos, a maioria encontra-se em fase de testes e ainda não se pode aferir com exatidão e de forma conclusiva quais os impactos na gestão pública. A dificuldade reside na percepção objetiva do real ganho de um projeto que envolva a tecnologia *blockchain* e proponha uma mudança, até estrutural, na Administração Pública.

Não obstante, das impressões extraídas das declarações dos autores deste estudo, pontuou-se que "projetos que envolvem uma menor multiplicidade de *stakeholders* e uma governança mais centralizada possuem menor complexidade, tais como os projetos de aplicações notariais"[347]. Outro obstáculo a ser considerado, em senda diversa, seriam os projetos com soluções mais complexas envolvendo bases distribuídas e *smart contracts*, por exemplo. Tais soluções encontram desafios na implementação, geralmente pela incompatibilidade com os processos administrativos em operação e pela não conformidade com as regras procedimentais vigentes.

Por isso é que se percebe a existência de diversos obstáculos a uma adoção maciça da *blockchain* nas diversas esferas públicas, por questões de interoperabilidade, incompatibilidade de processos ou apenas receio do administrador em adotar uma tecnologia que, apesar de não ser uma construção nova, ainda é associada a algo incipiente e que demanda diversos debates. No paradigma

---

[345] Morais, Janaina Jacolina. "Princípio da eficiência na Administração Pública". Ethos Jus: revista acadêmica de ciências jurídicas. Avaré: Faculdade Eduvale de Avaré, v. 3, n. 1, 2009. p. 99-105.

[346] Allessie, D.; Sobolewski, M.; Vaccari, L.; Pignatelli, F. "Blockchain for digital government". Luxemburgo: Publicação oficial da União Europeia, 2019.

[347] Moura, Luzia Menegotto. Ibid. p. 6.

da Administração Pública, à luz do princípio da Legalidade que rege e vincula o poder executivo[348], não se suscita ilicitude caso os dados pessoais a serem tratados assim o forem em conformidade com o artigo 6.º, n.º .1, c) do RGPD[349], o qual fundamenta o tratamento de dados para fins de cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito. E, por este motivo, a obrigação legal será o fundamento legal requerido pelo artigo 6 do RGPD[350] e assim restará afastada a ilicitude do tratamento de dados pessoais baseado e distribuído na *blockchain* já que a existência de uma lei defina que algum dado pessoal específico é de interesse público e assim deverá ser registrado em algum sistema baseado na *blockchain* criará a base jurídica para o tratamento em causa.

Ante o exposto, acaba por ficar facilitado o enquadramento da *blockchain* para fins de conformidade com a Proteção de dados consagrada no RGPD, se aplicada na égide administrativa. Se a legalidade administrativa promove uma exigência estrita ao mandamento normativo, a base legal do artigo 6.º, n.º.1, c) do RGPD é uma consecução lógica do tratamento de dados pessoais pelo Poder Público, uma vez que, via de regra, o Estado está vinculado à lei através de seus representantes. Neste sentido, vale a definição clássica que norteia a doutrina do Direito Administrativo que, na obra de MEIRELLES, a legalidade, como princípio de administração, significa que o administrador público está, em toda sua atividade funcional, sujeito à lei e às exigências do bem comum, e deles não se pode afastar ou desviar, sob pena de praticar ato inválido e expor-se à responsabilidade disciplinar, civil e criminal, conforme o caso[351] - atuando assim o princípio da legalidade administrativa como o pressuposto, o fundamento e o limite da atividade administrativa.

É importante salientar que a base legal supramencionada é a mais adequada quando presente a atuação da Administração Pública, uma vez que a própria Autoridade de Controlo do Reino Unido deixou bem claro que, quando se trata de autoridade pública, no uso de suas atribuições legais e para consecução de suas tarefas oficiais, o tratamento vai ser lícito[352]. Esta visão oficial parte do pressuposto que os poderes administrativos atuam baseados na lei e o tratamento de dados, seja pelo uso da *blockchain* ou não, vai encontrar licitude *juris tantum.*

Por fim, se a *blockchain* for utilizada no paradigma da Administração Pública e os dados pessoais tratados estiverem anonimizados, através da utilização de técnicas trazidas no capítulo

---

[348] Ressalvada a diferença da legalidade estrita e discricionariedade administrativa conforme: Di Pietro, Maria Sylvia Zanella. "Da constitucionalização do direito administrativo: reflexos sobre o princípio da legalidade e a discricionariedade administrativa. Supremacia do interesse público e outros temas relevantes de Direito Administrativo". São Paulo: Editora Atlas, 2010. p. 169

[349] Europeia, União. Parlamento e Conselho. Regulamento (UE) 2016/679, de 27 de abril de 2016. Ibid

[350] Ibid.

[351] Para aprofundar, veja-se em: Meirelles, Hely Lopes. "Direito Administrativo Brasileiro". Ed. São Paulo: Malheiros, vol. 30, 2005.

[352] Information Commissioner's Office. Lawful basis for processing. Disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ Acesso em 22 de agosto de 2020

anterior (dentre as quais o esquema de comprometimento e prova de conhecimento zero), o tratamento situa-se fora do âmbito material do RGPD. Sob o ponto de vista da proteção de dados, o não enquadramento legal faz com que o suposto uso da *blockchain* se perspective viável na medida em que os dados deixam de demandar particular cuidado no seu tratamento em virtude de deixarem de se configurar como pessoais (opera-se, portanto, uma operação *ex ante* de despersonalização dos dados).

De outra forma, há os casos em que, por força de algum instrumento normativo, surge a obrigação legal de realizar um registro, divulgar publicamente uma transação ou qualquer outro ato administrativo que emana da força legal e envolve o patrimônio público e ao mesmo tempo dados pessoais. Nestes casos, se a forma, legalmente definida, de registrar for através da *blockchain*, cujas entradas ficarão descentralizadas e distribuídas, o tratamento reside no âmbito material do RGPD, porém encontrará licitude através da base legal do artigo 6.º, n.º 1, c), uma vez que o órgão público estará a obedecer a um ditame legal.

Dito isto, precisa-se endereçar uma problemática suscitada ao longo deste capítulo que sai um pouco do plano suposto e ideal, onde agentes investidos do *múnus* público apenas obedecem ao interesse público e são perfeitamente aplicadores do princípio da legalidade. De fato, a teoria do órgão público define-o como sendo uma unidade que congrega atribuições exercidas pelos agentes públicos que integram o organismo com o objetivo de expressar a vontade do Estado[353]. Ou seja, retira do agente público o aspecto de vontade quando se trata de uma decisão movida pelo interesse público. Entretanto, precisa-se ir além, ainda à luz de soluções de uma *blockchain* em conformidade com o RGPD, e para tanto passa-se a pensar em soluções baseadas na *blockchain* que visem combater a corrupção, um verdadeiro desvio da "vontade do Estado".

4.3 Corrupção como justificação prática da aplicação da blockchain

Conforme já debatido, o conceito de Administração Pública é amplo e absorve diversas vertentes, dentre as quais existem os princípios administrativos norteadores, bem como a teoria do ato administrativo, as diversas classificações de agentes públicos, etc. Logicamente, por ter sido discutida a maleabilidade da tecnologia *blockchain*, poder-se-iam levantar diversas hipóteses onde a cadeia de

[353] Neste sentido, Di Pietro. Maria Sylvia Zanella. Ibid.

blocos pode ser, ou já tem sido adotada, pelo setor público. Todavia, preferiu-se pensar em um uso da *blockchain*, sabendo da mudança funcional que esta é capaz de realizar em relação à Administração Pública, quando a posição de prevalência de algum servidor público (ou agente equiparado) é utilizada para obtenção de vantagens ilícitas, o que, de forma geral, é definido como corrupção.

A doutrina clássica não consegue ser uníssona na definição deste conceito, diante da sua complexidade, porém normalmente se advém de uma dicotomia legalidade e finalidade. Se para FRIEDRICH[354], corrupção é padrão de comportamento que se afasta das normas predominantes em um dado contexto, se associando a uma particular motivação (normalmente, e não obrigatoriamente, o ganho privado a expensas do público); para ROGOW et al.[355], basta violar o interesse comum (pelo contexto da obra, comum diz respeito a público) para vantagens especiais. E ainda neste sentido, HOETJES[356] que conceitua o fenômeno da corrupção administrativa, de um modo geral, como uma classe geral de abusos ou violações do interesse público.

Em visão diversa, JOHNSTON[357] traz que a corrupção poderia ser percebida ao que o povo pensa que é, conceituação demasiadamente subjetiva, até porque as pessoas comuns aplicam o termo corrupção a uma diversidade de atividades, associada desde irritação ao descaso, passando pelo cinismo e a resignação[358]. Deixar a conceituação, ora buscada, à mercê de julgamentos populares que são levados a decidir com base em preconceitos, pode levar a um conceito complexo e contraditório de corrupção, recaindo provavelmente numa invocação de valores e tradições profundamente enraizadas.

E, por tudo isso, à luz do princípio da supremacia do interesse público, o uso da máquina estatal para fins diversos dos que juridicamente são esperados, seria um desvio de finalidade *juris tantum*[359]. E esta duplicidade entre finalidade e lei irá traçar o enquadramento jurídico para fins de averiguar se certa atitude corresponde a um ato de corrupção. Por isso é que, em outras palavras, a corrupção ocorre quando um funcionário público, agindo conscientemente em sua capacidade oficial, é envolvido em uma transação que beneficia interesses impróprios, especialmente privados[360].

---

[354] Friedrich, C. J. "Political corruption". Political Quarterly, vol. 37, n. 1, 1966. pp. 74-85.

[355] Rogow, A. A.; Lasswell, H. D. "The definition on corruption" (cap.). In: Heidenheimer, A. J. "Political corruption - readings in comparative analysis". Nova York: Holt, Rinehart and Winston, 1970.

[356] Hoetjes, B. "Administrative corruption in the Netherlands: recent cases and recent developments. Corruption and Reform". Países Baixos, vol. 1, n. 2, 1986. pp. 133

[357] Johnston, Michal. Apud

[358] Brei, Zani Andrade. Apud

[359] Acerca do desvio de finalidade, veja-se Lazzarini, Álvaro. "Abuso de poder x poder de polícia". Revista de Direito Administrativo, v. 203, 1996. pp. 25-39.

[360] Brei, Zani Andrade. "Corrupção: dificuldades para definição e para um consenso". Revista de Administração Pública, v. 30, n. 1, 1996. pp. 64-77.

Diante dos conceitos trazidos, que envolvem vários termos, mas, na sua essência, buscam constatar se tal ato obedeceu à dúplice expectativa de respeito à lei, mas também ao interesse público que norteia o Direito Administrativo, pode-se dizer que a dificuldade não aparenta definir corrupção, mas sim o que seria interesse público, uma vez que se soma à "abstração e esvaziamento semântico", a decorrência da "amplitude do seu campo de ação"[361].

Por amor ao debate, há quem considere o interesse público como um padrão caleidoscópico de interesses privados conflitantes e substituíveis[362]. Em outras palavras, uma política pública significativa envolver não dois ou três, mas dezenas de interesses privados. Entretanto, limitar-se a pensar assim significa ignorar outros conceitos como democracia, separação de poderes, até o próprio conceito de Estado democrático composto por representantes eleitos por eleitores representados. E, por isso, o interesse público vai ser algo separado do interesse privado, e para fins de definir o que é corrupção, o interesse privado em detrimento da lei, no contexto de uma circunstância na qual era suposto ser regida pelo interesse público, para fins deste estudo, será o entendimento do que é corrupção.

Superado este momento conceitual do que significa corrupção, uma vez que a essência deste fenômeno recai no comportamento desviante da finalidade visada, ou seja, de alterar processos e expectativas, logicamente existem desvios que não buscam um benefício financeiro direto, a exemplo do nepotismo cruzado[363] que emprega politicamente privilegiados, mas os atos de corrupção por defeito, ou seja, aqueles que buscam alterar / desviar-se das finalidades para gerar vantagens ilícitas. Ressalta-se que majoritariamente o fenômeno do nepotismo é uma das faces da cultura administrativa, chegando a ser definido como o "flagelo nacional da corrupção", se pensar na ordem jurídico-administrativa brasileira[364]. Entender o problema pela essência facilita para supor soluções ao mesmo. E, com isto em vista, o escopo de qualquer solução que busque combater a corrupção no setor público precisa oferecer uma maior eficiência na conservação e uma menor probabilidade de adulteração dos livros e registro de caráter público.

---

[361] Oliveira, Vânia Aparecida Rezende de; José Roberto Pereira. "Interesse público: significados e conexões". Cadernos Gestão Social, vol. 4, n. 1, 2013. pp. 13-23.

[362] Neste sentido, Johnston, Michael. "Political corruption and public policy in America". Monterey: Brooks/Cole Publishing Company, 1982.

[363] Fenômeno explicado em Modesto, Paulo. "Nepotismo em cargos político-administrativos". Revista Brasileira de Direito Público, vol. 11, 2012.

[364] Rodrigues, João Gaspar. "Nepotismo no serviço público brasileiro e a SV 13". Revista de Direito Administrativo, n. 260, 2012. pp. 203-229.

É neste interim que se vislumbra a *blockchain*, uma vez que a tecnologia tem como uma de suas marcas a difícil alteração dos registros, porque os blocos oferecem uma segurança jurídica[365]. Se livros e registros que baseiam algum ato administrativo estiverem registrados em um sistema descentralizado e distribuído baseado na *blockchain*, atos de corrupção que precisem disfarçar desfalques financeiros ficarão eternamente auditáveis para fins de identificações, seja pelas cortes de contas, seja pelas demais com poderes investigatórios, como o Ministério Público e as repartições policiais. E, neste contexto, é de ser suposto que a violação da integridade de livros e registros públicos pode ser considerada o embrião da corrupção[366].

Diante deste sério cenário, parte-se para uma análise de casos específicos em que, por motivos diversos, em algum dado momento, a *blockchain* virou pauta para ser implementada em um projeto nacional que, dentre as possíveis finalidades, uma seja gerar mais transparência para auxiliar no combate à corrupção. Diferentes contextos, mas com um norte em comum, reduzir a opacidade e trazer confiança nas relações da Administração Pública e seus respectivos cidadãos, nomeadamente pela promoção de uma atividade administrativa mais transparente.

4.4 Caso da LAC-Chain no Peru

Dentre vários paradigmas, cumpre trazer algum exemplo concreto de país com problemas de corrupção estatal que resolveu apostar na tecnologia *blockchain* como uma das formas de combater tal problemática. E dentre os Estados possíveis, o Peru acaba por ser um país que apresenta uma série de sintomas que assolam os países da América do Sul, no que concerne o desvio da finalidade dos recursos públicos para fins que extrapolam o interesse público estrito.

Nos últimos anos, a conjuntura peruana não vem se mostrando muito pacífica, por envolver a alta cúpula em diversos casos internacionais de desvio de dinheiro público. No ano de 2019, o ex-presidente peruano Alan Garcia cometeu suicídio quando a polícia do país preparava sua prisão por

[365] Normalmente se utiliza a expressão "virtualmente inalterável e inapagável", neste sentido: Marks, Jesse. "Distributed Ledger Technologies and Corruption the Killer App." Colum. Sci. & Tech. L., vol. 20, n. 42, 2018; Alan Morrison. "Blockchain and Smart Contract Automation: Blockchains Defined", PWC, 2016.

[366] Neste sentido, Duranti et al fazem uma alusao que a confianca de um registro passa pela (im)possibilidade de alterá-lo: *"Authenticity is defined as the trustworthiness of a record as a record, meaning that the record is what it purports to be, free from tampering or corruption*." Veja-se em Duranti, Luciana; Rogers, Corinne. "Trust in digital records: An increasingly cloudy legal area". Computer Law & Security Review, v. 28, n. 5, 2012, p. 522-531.

envolvimento num esquema internacional de corrupção que diz respeito ao "Odebrecht *scandal*"[367], escândalo que envolveu diversos governos latino-americanos e a construtora que deu nome ao caso.

Não obstante o fato de o antigo presidente peruano ter evitado a prisão tirando a própria vida, dois outros nomes de relevância também foram condenados à prisão: o ex-presidente Pedro Pablo Kuczynski e a líder da oposição, Keiko Fujimori[368]. Sem esquecer que outros ex-presidentes tiveram a imagem maculada também por envolvimento com a construtora Odebrecht[369], a saber Ollanta Humala e Alejandro Toledo. Uma Administração Pública abalada por casos envolvendo tantas personalidades de cúpula que obedeceram a seguinte regra: uma empresa do setor privado (qual seja, a Odebrecht) a oferecer suborno em troca de favorecimento em negócios lucrativos, no caso ilícito, a fim de sair vitoriosa em contratos de obras e infraestruturas.

Via de regra, quem anseia desviar dinheiro público, até pela própria natureza da Administração - que demanda uma prestação de contas e conta com órgãos fiscalizadores, como os Tribunais de Contas – busca fazê-lo através de meios lícitos, sobretudo quando se trata da irregularidade provocada pelo gestor público que tem o poder de desviar do Erário público, mas precisa oferecer um balancete de receitas e despesas à luz da responsabilidade fiscal assumida. Para tanto, um dos mecanismos de desvio comum é o do faturamento desproporcional de gastos públicos através de licitações superfaturadas[370]. E seguindo esta cartilha da corrupção, assim o fizeram, por diversos mandatos, os chefes do Executivo peruano, por isso o extenso número de investigados e envolvidos.

Aos olhos de quem desvia, cria-se uma sensação de impunidade e convicção de que muitas transações se perdem no meio de uma infinidade de registros e documentos inerentes à burocracia estatal. E para ajudar as entidades da polícia e de fiscalização, é suposto haver um sistema de compras públicas que ofereça rastreabilidade desde a conceção, para que os gastos públicos estejam acessíveis de forma fácil e sem possibilidade de adulteração, para, ao menos, haver uma inspeção facilitada. E sob esta necessidade e vislumbrando melhorar esta problemática, enquadra-se na almejada relação desenvolvida até o momento de como a *blockchain* poderá registrar dados públicos

---

[367] Gallas, Daniel. "Brazil's Odebrecht corruption scandal explained". Disponível em https://www.bbc.com/news/business-39194395 Acesso em 26/06/2020.

[368] Globo. "Ex-presidente peruano Alan García morre após dar tiro na cabeça". Disponível em https://g1.globo.com/mundo/noticia/2019/04/17/ex-presidente-alan-garcia-morre-diz-imprensa-local.ghtml Acesso em 27/06/2020.

[369] Globo. "Corrupção no Peru: entenda denúncias envolvendo a Odebrecht e 4 ex-presidentes peruanos". Disponível em https://g1.globo.com/mundo/noticia/2019/04/17/corrupcao-no-peru-entenda-denuncias-envolvendo-odebrecht-e-4-ex-presidentes-peruanos.ghtml Acesso em 28/06/2020.

[370] Ligação intrínseca das licitações superfaturas e os desvios públicos conforme, Para aprofundar, veja-se: Dos Santos Gonçalves, Luiz Carlos. "El Ministerio Público Brasileño y el combate a la corrupción." Revista de la Facultad de Derecho de México, vol. 68, n. 272-1, 2018. pp 307-324.

de forma a evitar corrupção. E, nesta senda, merece destaque um projeto em desenvolvimento no Peru, que se visa dotar de uma plataforma para resolver esta dificuldade.

O Peru, perante tantos casos de corrupção que envolviam basicamente superfaturamento de compras públicas, decidiu criar um ambiente eletrônico único no qual sejam reunidos digitalmente todos os pedidos da agência governamental "Peru Compras"[371], esta que possui como incumbência regular todas as compras eletrônicas do país. Esta nova plataforma foi denominada *LAC-Chain* e será uma *blockchain* que realizará o registro de forma descentralizada, e com as caraterísticas temporais e criptográficas inerentes à cadeia de blocos. O protótipo foi uma iniciativa de interesse do Banco Interamericano de Desenvolvimento (BID), que já declarou que almeja promover um ecossistema *blockchain* na América Latina e no Caribe. Resta evidente, neste projeto, que há uma crescente preocupação em digitalizar os processos de contratação e trazê-los para uma base de dados imutável, o que, além de permitir uma auditoria de procedência e veracidade, elimina riscos de alterações ou fraudes. Um motivo declarado foi diretamente reduzir os índices de corrupção, após tantos escândalos envolvendo a construtora Odebrecht e diversos ex-presidentes peruanos.

Parece ambicioso, porém a conceção de nacionalizar uma plataforma de compras estatais baseadas na *blockchain* passa por dois anseios: i) implementar um processo altamente transparente e ii) promover a rastreabilidade de aquisições e contratos públicos. Se estes anseios forem alcançados, violações e atos de corrupção ao menos ganharão alguns obstáculos. Verdade que tal sistema peruano está em fase de testes, mas já demonstra boa receptividade, com média diária mantendo um total que varia entre 500 e 1000 pedidos, de acordo com o co-fundador da Stamping.io, José Zárate Sousa[372]. Acredita-se que, além da boa receptividade, a iniciativa do sistema Peru Compras gera um efeito em cadeia de estímulo pela adoção da *blockchain* por outras empresas e entidades, além de realizar seu potencial de trazer eficiência aos procedimentos administrativos. Uma adoção apenas que consegue acatar diversos princípios do Direito Administrativo, a exemplo da Eficiência, Legalidade, transparência, e ao fim, garantir a preeminência do Interesse Público.

Merece destaque o caráter extraterritorial da solução. A *LAC-Chain* foi designada pelo BID com o intuito de não apenas solucionar os problemas peruanos, mas ser potencialmente um ecossistema multinacional e o protótipo peruano funcionaria como um primeiro passo em um longo processo de implementação. Segundo LANZ[373], a ideia por trás do projeto é a criação de um sistema de verificação

[371] Lanz, Jose Antonio. "Peru sets its eyes on blockchain to fight government corruption". Decrypt.co. Disponível em https://decrypt.co/6893/peru-blockchain-government-corruption Acesso em 29 de junho de 2020.
[372] Lanz, Jose Antonio. Ibid.
[373] Lanz, Jose Antonio. Ibid.

de contratos governamentais que sejam imunes à manipulação de dados, receitas e despesas não autorizadas ou qualquer outro artifício fraudulento que possa conferir um contrato administrativo a uma empresa que assim não deveria fazer, por observância da lei.

E o caráter internacional decorre do potencial disruptivo desta iniciativa que é elementarmente uma solução de registro público baseado na *blockchain*, cujo desígnio é combater a corrupção e poder ser aplicado não apenas no Peru, mas em diversos outros países, em especial naqueles em que a corrupção atua de forma endêmica, conjunturas que tornam difícil perceber o sistema corruptivo como um todo.

Corrobora o que foi exposto, até o momento, a célebre frase de Steve Ghiassi, presidente da Australian Legal Technology Association, que declarou: "A chave para reduzir corrupção é criar transparência e rastreabilidade. Isto poderia reduzir o nível de fraude interna e adulteração, já que auditorias internas poderiam ser conduzidas com maior precisão em um caminho completo e visível"[374].

Caso o "Peru Compras" estivesse em funcionamento, a transparência e rastreabilidade conferida pela *blockchain* torna relevante a indagação - poderia ter sido evitado o esquema multimilionário organizado na América do Sul? - afinal foram forjadas diversas faturas fraudulentas baseadas em relações de compras estatais falsas.

Uma vez que demonstrados o cenário real e um caso concreto de uso da *blockchain* voltados à Administração Pública, cumpre trazer uma questão debatida nos capítulos anteriores, qual seja a regulação por trás desta *blockchain* da *LAC-Chain*. Segundo os relatos, a *LAC-Chain* é da modalidade permissionada, pelo fato dos *nodes* estarem sendo administrados pelo BID, através do IBD Lab Program, e apenas os *nodes* que receberem tal permissão é que poderão aceder ao website da Stamping.co (a startup provedora desta rede *blockchain* permissionada). Prova disto é o evento supramencionado em que a própria Stamping.co, através de seu diretor, declara a boa receptividade do sistema por conta de uma média diária de 500 a 1000 pedidos, leia-se pedidos de participação na *blockchain*, o que indica a existência de uma *blockchain* permissionada, com uma camada de governança acima dos demais *nodes*.

Cumpre relembrar que as redes permissionadas[375] seguem uma regulamentação, existe uma espécie de pré-seleção dos participantes, cujas aplicações são restringidas, conforme deram conta

[374] Em tradução livre de "A key part to reducing corruption is to create more transparency and traceability. It could reduce some level of internal fraud and tampering, as internal audits could be conducted more accurately with a full, visible trail". Conforme Lanz, Jose Antonio. Ibid. p. 2.

[375] Conforme explicação anteriormente trazida por: Moura, Luzia Menegotto Frick de.et al. Ibid.

FORMIGONI FILHO et al[376] e YERMAK[377]. Pode-se dizer que, na *blockchain* permissionada, as chaves de acesso são controladas e existe uma obrigação de solicitar permissão para as transações[378], assim como acontece com a *LAC-Chain* em análise. Diferente de uma *blockchain* pública em que as chaves criptografadas de acesso são amplamente acedidas, seja qual for a operação (consultar a cadeia de blocos ou para realização das operações em uma rede aberta), neste modelo da *LAC-Chain* apresenta-se um modelo de governança diferenciada: as chaves de acesso são controladas e existe uma obrigação de solicitar permissão para as transações[379].

Ainda no que concerne à regulação permissionada, é imperioso resgatar as precedentes considerações em relação à Proteção de Dados, porque a *blockchain* permissionada foi o modelo entendido, no capítulo anterior desta investigação, como mais aconselhável para fins de *compliance* com o RGPD, caso haja tratamento de dados pessoais[380]. Ressalte-se que, na *blockchain* pública, todos os participantes podem assumir o papel de leitor, escritor e validador, ao passo que, na permissionada, como é o caso da *LAC-Chain*, existirá uma entidade regulatória por trás da cadeia concedendo diferentes níveis de acesso.

Não se pode afirmar internamente quais dados serão visíveis em *cleartext* nesta *LAC-Chain*, entretanto há uma lógica de não utilizar a forma anonimizada dos dados que sejam nesta cadeia armazenados, sob a finalidade específica de justificar o tratamento de dados públicos que almejam trazer o próprio cidadão/cidadã para o processo de fiscalização das contas públicas, através de um sistema de fácil acesso e leitura. A verdade é que as contas públicas obedecem primordialmente ao princípio da publicidade[381], e o dever de publicação decorre de uma obrigação legal em fazê-lo.

Por isso é que, no caso ora debatido, mesmo que os dados a serem registrados de forma inalterável e inapagável na *blockchain* não sejam anonimizados, os dados de contratos públicos ou transações governamentais *per si* não indicam trazer o conceito de dado pessoal sob os termos do artigo 4 RGPD, acerca de "informação relativa a uma pessoa singular identificada ou identificável"[382]. Na presente circunstância de publicar contas e contratos públicos, além de ser um ato administrativo

376 Formigoni Filho, J. R. Ibid.
377 Yermack, D. et al. Ibid.
378 Moura, Luzia Menegotto Frick de et al. Ibid.
379 Moura, Luzia Menegotto Frick de et al. Ibid.
380 Neste sentido específico: "*When using a permissioned Blockchain it is possible to implement appropriate safeguards to secure cross-border flow of personal information*". Veja-se Ramos, Luis Felipe M.; SILVA, João Marco C. Ibid.
381 Neto, Orion Augusto Platt, et al. "Publicidade e transparência das contas públicas: obrigatoriedade e abrangência desses princípios na administração pública brasileira." Contabilidade Vista & Revista, vol. 18, n. 1, 2007. pp. 75-94.
382 Europeia, União. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Ibid.

com dever de publicidade[383], não se considera identificável alguma pessoa singular, uma vez que o registro diz respeito ao instituto da coletividade.

Caso um modelo similar ao apresentado for adotado por um Estado-Membro no contexto da UE, mesmo que haja o tratamento de dados através da *blockchain* inserido no âmbito material do RGPD, o tratamento encontrará sua licitude no fato de uma *blockchain* que registra dados governamentais realizar tal tratamento em cumprimento de uma obrigação jurídica, a qual o responsável pelo tratamento está sujeito, qual seja o dever constitucional e legal de promover a publicidade das contas e procedimentos administrativos.

De qualquer forma, em nome da segurança que decorre da duplicidade do processo de validação, neste caso em específico recomendou-se a utilização do esquema de comprometimento, uma vez que, no momento primordial, o *node* que recebe o compromisso não poderá descobrir o valor que está a ser validado; para em um momento posterior haver uma vinculação, conforme preceituou FISCHLIN[384]. Esta técnica de validação, em tese, respeita diversos dos princípios do RGPD, em especial a minimização dos dados prevista no artigo 5.1(c).

À luz do caso da *LAC-Chain,* resta materializado como a Proteção de dados é baseada no "*risk-based approach*"[385], na qual recai a responsabilidade sobre o Governo em exigir da subcontratante que desenvolveu a *blockchain* governamental a adoção de medidas técnicas e organizativas que garantam designadamente que o risco de erros seja minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir potenciais violações desses direitos[386].

E, diante deste cenário, evidencia-se na decisão do responsável pelo tratamento da *LAC-Chain* que o protocolo de validação e registro dos blocos vai depender dos propósitos almejados por tal *blockchain* específica, qual seja através de lei, criar um sistema de registro no combate à corrupção. Não obstante a forma de validação optada, mesmo que o esquema de comprometimento não seja acatado neste caso específico, traços de licitude são oferecidos, uma vez que o sistema está baseado em uma lei específica por parte do Governo Peruano. Caso algum Estado-Membro da União Europeia adote uma plataforma nos mesmos moldes da desenvolvida no Peru, a exigência do artigo 6°, n.° 1, c),

383 Publicidade é interpretada como um dever legal da Administração Pública. Neste sentido, veja-se: Limberger, Têmis. Ibid. pp. 248-263.

384 M. Fischlin; R. Fischlin. Ibid.

385 Veja mais em Gellert, Raphael. "Understanding the notion of risk in the General Data Protection Regulation." Computer Law & Security Review, vol. 34, n. 2, 2018. pp. 279-288.

386 Conforme Considerando 71 do RGPD. Ibid.

resta observada e um suposto tratamento de dados pessoais na *blockchain* permissionada de compras governamentais seria lícito para fins de conformidade com o RGPD.

4.5 Caso no México: BlockchainHACKMX

Em meados de 2017, o Fórum Econômico Mundial (WEF[387]) apresentou um estudo de caso sobre a corrupção no México, no qual foi emitida uma recomendação expressa de desenvolvimento de aplicações baseadas na tecnologia *blockchain* para aumentar a transparência, assegurar a autenticidade da informação pública, e por fim, melhorar a confiança dos cidadãos em seus governantes[388]. Ressalte-se que a relação da *blockchain* com o combate à corrupção trazida neste presente trabalho é uma tendência internacional demonstrada no estímulo e incentivo, ao longo dos anos, pelo incremento de soluções voltadas a proteger dados estatais a registrar na cadeia de blocos, a fim de dificultar o desvio dos recursos que tais dados representam e patenteiam.

De acordo com o "*Partnering Against Corruption Initiative*"[389], a solicitação mencionada para que o México desenvolvesse uma estrutura baseada na *blockchain* seria para priorizar o combate à corrupção através de uma transparência governamental. A transparência dos atos administrativos seria garantida pela publicação criptografada de *hashes* durante cada etapa do procedimento administrativo. Segundo ainda estipula a WEF, o uso da *blockchain* promove uma prova irrefutável de existência[390] daquela informação que nela foi registrada e estabelece padrões de confiança mais elevados dentre os inúmeros *stakeholders* envolvidos na atuação da Administração Pública. O estudo ainda detalha que a diferença entre os portais de transparência no mundo dificulta uma desejada auditoria internacional das contas públicas e, nesta aproximação à *blockchain,* poderia representar uma simplificação para fins de interoperabilidade[391].

Nesta seara, merece destacar que o projeto *anti-corruption blockchain backbone* (ACBB) vem impulsionando uma aceleração da adoção da *blockchain* para o paradigma de combate à corrupção na Administração Pública a nível global. Sem esquecer que o Sustainable Development Goals das Nações

---

[387] "World Economic Forum"

[388] Gobierno de Mexico. Iniciativa BlockchainHACKMX. White Paper disponível em https://www.gob.mx/cms/uploads/attachment/file/328774/BlockchainHACKMX__Reporte_de_avances__1_.pdf Acesso em 19/06/2020

[389] World Economic Forum. Partnering Against Corruption Initiative - Infraestructura and Urban Development. Building Foundations for Trust and Integrity. World Economic Forum. 2017. Disponível em http://www3.weforum.org/docs/WEF_PACI_IU_Interim_Report_2017.pdf Acesso em 19/06/2020

[390] World Economic Forum. Ibid.

[391] World Economic Forum. Ibid.

Unidas[392] trabalha há anos com a pauta de conceder a cada pessoa do planeta uma identidade pelo menos até 2030, e uma das formas para isso seria uma identidade digital baseada na *blockchain.* O ACBB vem desenvolvendo uma plataforma segura lastreada na *blockchain* para promover a já mencionada transparência da Administração Pública e aumentar o nível de consciência e confiança entre os administrados. O livro-razão distribuído *ACBB-trusted* pode garantir, segundo o Fórum Económico Mundial (WEF), sistemas livres de erro e disponíveis para uma universal fiscalização, o que pode auxiliar na investigação em face de atos corruptos.

Diante deste cenário, o México viu-se numa situação em que havia uma recomendação internacional para iniciar o desenvolvimento de soluções tecnológicas baseadas na *blockchain* para deliberar a corrupção que foi constatada no país. Lançado o desafio no *Campus Party* em Guadalaraja, dentre diversas ideias, a que se sagrou vencedora foi o projeto "*Contrataciones Inteligentes*"[393], cuja conceção central seria a de criar um sistema de contratações públicas baseado no padrão de contratações abertas, visando novas figuras no processo de compras estatais, assente na existência de "avaliadores independentes"[394] que supostamente terão voz e voto em todo o procedimento licitatório que ocorrerá numa rede *blockchain*.

Primordialmente, a rede BlockchainHACKMX promoveu uma investigação e análise de cada solução baseada na *blockchain* já existente, com intuito de identificar uma solução tecnológica que contava com 5 requisitos que o Governo Mexicano entendeu como primordial para lastrear a sua plataforma de contratações inteligentes: o código da solução deveria ser aberto, governança adequada aos fins esperados pela Administração Pública, capacidade de utilização de *smart contracts* avançados; implementação de uma *blockchain* privada e, por fim, a confiabilidade das transações.

No desenvolvimento do projeto, a entidade organizadora concluiu que a rede BlockchainHACKMX seria desenvolvida sobre um dos sistemas *blockchain* já existentes, qual seja a *Hyperledger Fabryc,* Bitcoin*,* Ethereum*, Chain*, ou a NEM. Acerca do primeiro requisito de oferecer um código aberto, identificou-se que as 5 ofereciam esta característica; bem como no que dizia a respeito às particularidades de regulação almejadas pela Administração Pública (que significa uma atenção à

[392] Trata-se de um conjunto de 17 metas globais estabelecidas pela Assembleia Geral das Nações Unidas, sendo parte da Resolução 70/1 da Assembleia Geral das Nações Unidas: "Transformando o nosso mundo: a Agenda 2030 para o Desenvolvimento Sustentável". Veja-se mais em Nacoes Unidas Disponível em http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E Acesso em 12/11/2020

[393] Gobierno de Mexico. Ibid.

[394] Tradução livre para "Contrataciones Inteligentes, la cual propone la creación de un sistema de contrataciones públicas basado en el Estándar de Contrataciones Abiertas, añadiendo la figura de los evaluadores independientes con voz y voto en el proceso de contratación, esto sobre una red de blockchain". In: Gobierno de Mexico. Ibid. p. 2

Proteção de dados pessoais). Sobre a possibilidade de desenvolver *smart contracts* avançados, a Bitcoin foi compreendida como incapaz de oferecer tal solução, o que afastou a sua utilização.

Então, o Conselho Consultivo desta iniciativa, dentre as mencionadas e outras circunstâncias, deliberou que a solução mais adequada para tal projeto era a plataforma código aberto oferecida pela Ethereum, sobretudo porque se permite a criação de uma rede *blockchain* privada desvinculada às demais cadeias. Ou seja, os *nodes* que integrarem a BlockchainHACKMX não estarão conectadas à rede principal da Ethereum, mas sim estarão conectados a uma rede reservada e separada exclusiva da BlockchainHACKMX.

Todavia, o Governo Mexicano fez questão de explicar expressamente que o fato de ser uma rede reservada separada da Ethereum não significa que o acesso será restringido, tendo em vista respeitar o princípio já mencionado da publicidade que norteia a atuação administrativa pública[395]. Em outras palavras, criou-se uma rede de acesso irrestrito, para consultar o teor das transações estatais que nela serão registradas, não havendo sigilo na plataforma BlockchainHACKMX; o que se verifica é apenas a criação de uma rede em separado com regramento próprio e para fins específicos. Entende-se a opção da Ethereum, explicada pelo Conselho do projeto, uma vez que o próprio conceito de *smart contracts* acabou por ser difundido após a fácil aplicação nesta espécie de *blockchain* que apresenta mecanismos idôneos de autenticação.

Alinhado com o panorama trazido pela BlockchainHACKMX que enxergou no *smart contract* uma solução que envolve *blockchain* para combater a corrupção, a *Transparency International* (entidade financiada pela UE) apresentou um estudo em que "*auditorias e medidas de segurança podem ser codificadas em um smart contract*"[396], o que representa a eles – pelo menos na teoria – uma limitação no âmbito de comprometimento de fraude ou corrupção. *Smart contracts*, nos termos da entidade, são comandos na própria *blockchain* que demonstram ações automatizadas que ficam salvas de forma inalterável e que, para a Transparency International, se o *smart contract* possuir um código escrito de maneira apropriada, poderá gerar mais transparência. Segundo a entidade, apenas estas características já os tornam potencialmente aplicáveis em diversas áreas da Administração Pública, em especial nas contratações estatais no que concerne o trabalho de limitar manipulações durante as licitações e certames de contratação pública[397].

---

[395] Gobierno de Mexico. Ibid.
[396] Kossow, Niklas; Victoria Dykes. "Blockchain, bitcoin and corruption, A review of the linkages". Berlin: Transparency International Anti-Corruption. 2018. p. 12. (tradução livre)
[397] Kossow, Niklas et al. Ibid.

Sob esta confiança de que se o *smart contract* tiver um código escrito de maneira apropriada, a transparência administrativa é aperfeiçoada, o protótipo mexicano deliberadamente apostou que se a população, de forma pública, acompanhasse em tempo real as transações que envolvem recursos públicos, a transparência do sistema licitatório restaria assegurada. Confiança e segurança da informação pública é um objetivo declarado deste uso da *blockchain* por parte do Governo Mexicano que, no seu entendimento, decorre da própria característica da tecnologia *blockchain*[398].

Por fim, cumpre trazer a regra de regulação da rede BlockchainHACKMX. Lembra-se que KARL WÜST et al. enxergaram que a rede permissionada é marcada pelo ato de permissão em um momento anterior[399], ou seja, ao invés de definir a rede permissionada como uma rede de autorização para transações, enxerga o conceito sob o pedido de permissão para ingresso de participantes. E, seguindo esta lógica, a rede mexicana pretende instituir sua *blockchain* para garantir a estrutura e uso adequado através do "*Modelo de Gobernanza*".

Em estudo base divulgado pela "*Oficina de la Presidencia de la República*" [400], o governo mexicano desenvolveu um trabalho específico para definir qual seria o modelo de governança adequado em uma *blockchain* nacional para fins de registro da Administração Pública. A consolidação passa pela adoção de políticas necessárias para uma apropriada coordenação de todas as instituições e setores que vão compor a rede *blockchain*, e pelo impulsionamento de um ecossistema de inovação em decorrência da própria adoção da tecnologia do livro-razão distribuído. E a governança é a chave para este processo, pois é uma definição antecedente que norteia a continuidade de todo o processo. Para tanto, a definição de governança adotada pelo Governo mexicano foi a do autor GONZÁLEZ BARROSO, qual seja: "governança é um processo mediante o qual os participantes da rede geram, em conjunto, uma ordem e definem os sentidos e direções da iniciativa. A governança gera uma ordem e trata de maneira definitiva de um processo de direção social"[401].

Ademais, BARROSO vai além e enxerga que as interações e contribuições dos diversos "atores", ou participantes na definição da *blockchain*, são fundamentais para que a rede funcione da maneira esperada. Esta definição adotada para guiar o projeto BlockchainHACKMX merece destaque

---

[398] Govierno de Mexico. BlockchainHACKMX gana premio en el World Virtual GovHack. Disponível em https://www.gob.mx/cidge/es/articulos/blockchainhackmx-gana-premio-en-el-world-virtual-govhack-147504?idiom=es Acesso em 19/06/2020

[399] Wüst, Karl e Arthur Gervais. Ibid.

[400] Govierno de Mexico. Modelo de Gobernanza para implementar la Red Blockchain México. Comentários a consulta pública. Disponível em https://www.gob.mx/cms/uploads/attachment/file/415646/Consolidacio_n_de_Comentarios_Consulta_Pu_blica_-_Modelo_de_Gobernanza__1_.pdf Acesso em 21/06/2020

[401] González Barroso, Fernando. "Gobernabilidad y Gobernanza. Las relaciones intergubernamentales: concepto y marco teórico. El contexto y el concepto." Espanha: Administración de la Junta de Comunidades de Castilla-La Mancha, 2009. p. 4. Tradução livre.

porque expressamente o autor declara que "o governo não é o centro do sistema, haja vista este sistema é formado por uma rede de atores. O papel da entidade de governança é, portanto, de facilitador, coordenador e capacitador das ações do Estado em interação com esta rede de atores"[402].

Um detalhe demonstra a inovação trazida pelo projeto de implementar a *blockchain* na Administração Pública que é o fato dela não ser "estadocêntrica". O Estado é, ao longo dos séculos, o centro de qualquer solução administrativa, centralizando processos e ato administrativos; entretanto, o modelo que se propõe é de uma mudança do tradicional papel do Estado, para que a rede de participantes em si seja o cerne e o Estado atue apenas como um estabelecedor de regras pré-definidas, que serão, no caso da BlockchainHACKMX, as regras de regulação que se passam a expor.

Segundo o relatório oficial, os participantes estarão organizados em um Conselho Consultivo, um Conselho Executivo e Coletivos, respectivamente representando cada um dos 3 setores, o setor público, privado, acadêmico/organização da sociedade civil (OSC)[403]. Os setores poderão participar dos conselhos para deliberarem melhorias e aproveitamento da tecnologia. O modelo proposto ainda sugeriu uma assunção de papéis especiais de coordenação, entretanto sem manter qualquer relação de hierarquia, corroborando a descentralização do poder estatal.

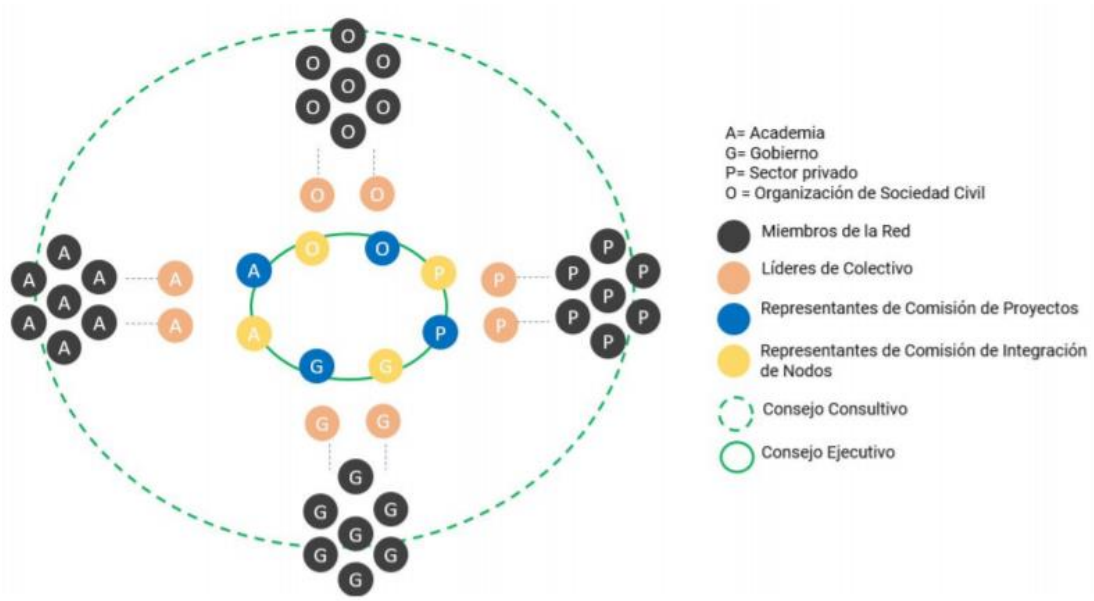


Figura 2: Estrutura regulatória da BlockchainHACKMX[404]

[402] González Barroso, Fernando. Ibid. 2009.
[403] Govierno de Mexico. Modelo de Gobernanza para implementar la Red Blockchain México. Ibid.
[404] Govierno de Mexico. Modelo de Gobernanza para implementar la Red Blockchain México. Ibid.

Para ilustrar a estrutura de regulação do sistema, destaca-se na Figura 2 uma horizontalidade dos *nodes* da rede *blockchain* em que cada ciclo de representatividade e governança tem membros de todos os setores. Se o nível executivo tem representantes eleitos, interessante notar a confiança no sistema que permite os membros do "*Gobierno (G)*" restarem no mesmo ciclo consultivo do "*Sector Privado (P)".* Fato este que demonstra a descentralização proposta pela *blockchain* e resgata uma afirmação feita anteriormente nesta investigação, sob esta aplicação concreta desta tecnologia, na qual defendeu-se que há uma "revolução que acaba de começar"[405].

Um modelo regulatório para algo que irá estruturar transações e registros da Administração Pública que acredita que a descentralização do sistema permite um desígnio sem qualquer hierarquia ou entidades centralizadoras de confiança, vai acabar por permitir uma solução que torna áreas obscuras por onde estão ocorrendo desvio de verbas públicas um ambiente mais transparente, sem hierarquia *by design* e que dificulta a atuação de corruptos. Prova da abertura foi que o modelo de governança proposto pela BlockchainHACKMX ainda se mostrou aberto à adoção de um relevante conceito, a democracia líquida[406]. No modelo da *blockchain* nacional mexicana, os *nodes* da rede podem votar na seleção de representantes e nos membros dos Conselhos Executivos e Consultivos.

Uma vez que o modelo de governança resta elucidado, e sua estrutura demonstra uma dificuldade para atos de corrupção, cumpre regressivamente mencionar se a iniciativa BlockchainHACKMX depreende atenção ao princípio da Proteção de dados pessoais. Esta problemática veio expressamente listada como um dos tópicos do "Protocolo de seguridade"[407]. A rede mexicana conta com protocolos para garantir integridade do sistema e proteger os utilizadores, dentre os quais o Governo Mexicano listou a Identidade dos participantes que serão coletadas, a privacidade e Proteção de dados vão ser fundamento para medidas que visam justamente resguardar as informações pessoais destes participantes, e ainda protocolos de cibersegurança que visam medidas de prevenir e enfrentar ataques cibernéticos. Todas elas, segundo o relatório da governança, serão definidas e implementadas pelo acima mencionado Conselho Executivo, com assistência do Conselho Consultivo.

Em outras palavras, assuntos de suma importância como a privacidade e a cibersegurança vão ser fruto de um debate que envolverá todos os *stakeholders,* afinal a partir do momento que se menciona que o Conselho Consultivo da BlockchainHACKMX irá participar da definição de estratégias

[405] Crosby, Michael et al. Ibid. p. 7.

[406] Segundo Sala, a democracia contemporânea busca modelos representativos e participativos. Em ambos, a soberania não tem encontrado total satisfação. Veja-se em Sala, Jorge Francisco Aguirre. "Los límites de la representatividad política y las alternativas de la democracia líquida." Revista Internacional de Pensamiento Político, vol. 10, 2015.

[407] Govierno de Mexico. "Modelo de Gobernanza para implementar la Red Blockchain México". Ibid.

nestes assuntos, significa que entidades de toda a sociedade são chamadas a construírem juntas um sistema em conformidade com as leis nacionais de Proteção de dados e segurança da informação. Esta abordagem pode servir de paradigma para qualquer outro país que deseja implementar a *blockchain* a nível nacional, sobretudo se for um dos Estados-Membros da União Europeia que almeje implementar um sistema em conformidade com o RGPD e ao mesmo tempo oferecer as medidas necessárias para evitar ou enfrentar ciberataques.

E tendo em vista o panorama da UE, a BlockchainHACKMX expressamente listou experiências de estudos de casos de outros países que serviram de inspiração para o projeto, tendo em vista uma global tendência de utilização da *blockchain*, mormente para inovar na prestação de serviços públicos e no combate à corrupção. Entre os países que já experienciam o uso nacional da *blockchain*, o primeiro exemplo que inspirou a iniciativa mexicana foi a Estônia, cuja solução, por estar inserida no contexto da União Europeia, merece ser trazida separadamente.

4.6 Estudo de caso – KSI blockchain

Segundo o estudo mencionado da BlockchainHACKMX, a Estônia serviu como um exemplo ao utilizar a tecnologia *blockchain* para armazenar os registros públicos, inclusive acerca dos registros de saúde, tornando a sua adulteração perceptível. Os indivíduos estonianos detêm um cartão inteligente que armazena seus dados e dá-lhes acesso a mais de 1000 serviços governamentais[408]. Mas esta investigação pretende ir além: de fato, a KSI *blockchain* é referência na prestação de serviços públicos[409], mas o escopo ora almejado é entender como a *blockchain* da Estônia contribui para o combate à corrupção. De acordo com MOUALLEM[410], a resposta reside na forma como a cadeia de blocos funciona, explicando algo que foi bastante desenvolvido na presente pesquisa, de que a ausência de uma entidade única e centralizadora para monitorar as diversas transações. Esta "visão centralizadora favorece a ocorrência de práticas corruptas"[411] o que, na preservação descentralizada da *blockchain,* não ocorre, segundo o mesmo autor que ilustra a opinião com a conclusão do WEF sobre o assunto.

[408] Govierno de Mexico. "Modelo de Gobernanza para implementar la Red Blockchain México". Ibid.
[409] Neste sentido, veja-se Cortizo, Lucas. Cap. "Blockchain e e-Government (paradigmas e perspectivas)". Ibid.
[410] Mouallem, Atie J El. "Countries using blockchain for combating corruption". Disponível em https://atiejelmouallem.com/countries-using-blockchain-for-combating-corruption/ Acesso em 21/06/2020
[411] Tradução livre de "traditional methods of keeping a track of any transaction is prone to fall prey to corrupt practices" in: Mouallem, Atie J El. Ibid.

Segundo o WEF[412], a *blockchain* oferece um nível sem precedentes de integridade, segurança e confiabilidade, reduzindo os riscos associados de haver uma "*single point failure*". Ao eliminar os intermediários, não apenas se reduzem custos, mas também se removem entraves burocráticos e se reduz a margem para atitudes arbitrárias dos agentes públicos. Observou-se, ainda, que todo registro pode ser monitorado e cada transação pode ser rastreada. E, é por tudo isso que a *blockchain,* para o WEF, oferece uma "imutabilidade segura"[413] conferindo, às autoridades e entidades fiscalizadoras de contas, um forte instrumento na luta contra a corrupção que, por mais arquitetada que seja, deixa rastros perenes e criptograficamente marcados de forma inalterável na cadeia de blocos.

Foi neste contexto que a Estônia resolveu adotar nacionalmente esta tecnologia de forma precursora. No caso prático estoniano, é possível atrelar todos os assuntos deste trabalho, que passa por temas centrais de Proteção de dados pessoais, tecnologia *blockchain* e a corrupção na Administração Pública. Consoante MOUALLEM, uma *accountability* baseada no livro-razão distribuído tem dado aos cidadãos estonianos um maior controle sobre seus dados pessoais[414].

Registre-se, neste ínterim, que, conforme os ensinamentos de DATTA[415], a KSI *blockchain* usada na Estônia consegue respeitar garantias de privacidade e proteção de dados, uma vez que a KSI não capta dados dos utilizadores e os dados jamais saem das devidas premissas. Explica ainda que, apesar de registrar dados, a *blockchain* não visa permitir acesso aos mesmos, pois funciona através da já explicada função *hash "one-way"*, o que resulta num código *hash* que unicamente representa os dados e é irreversível. Para DATTA, não se pode partir do *hash* e reconstruir os dados que ele representa, sendo assim uma forma de observar a privacidade dos dados[416]. E é neste modelo que oferece Proteção de dados desde a conceção e por defeito, consoante as previsões do artigo 25 do RGPD, ao mesmo tempo que se gera mais transparência com repercussões na prevenção e combate às práticas corruptas no contexto da atividade da Administração Pública.

Ou seja, idealiza-se um processo de empoderamento do titular dos dados através de um registro público transparente que, ao invés de ficar confiado a um órgão público dotado de fé pública[417], irá distribuir a base de dados através de cópias fidedignas e simultâneas para cada cidadão, visando

---

[412] Santiso, Carlos. "Can blockchain help in the fight against corruption?" World Economic Forum. Disponível em https://www.weforum.org/agenda/2018/03/will-blockchain-curb-corruption/ Acesso em 21/06/2020

[413] Resgata-se neste momento a ressalva anteriormente estabelecida que não existe imutabilidade absoluta, mas apenas questões probabilísticas de uma difícil adulteração. World Economic Forum. Ibid.

[414] El Mouallem, Atie J. Ibid.

[415] Datta, Anwitaman. "Blockchain in the government technology fabric." Singapura: School of Computer Science and Engineering, NTU. arXiv. 2019.

[416] Datta, Anwitaman. Ibid.

[417] Conforme a definição jurídica em Lopes, J. de Seabra. Ibid

evitar a corrupção. Seria uma maneira da tecnologia escalar o processo de registro e fiscalização, sobre o qual atualmente a burocracia estatal é desenhada, via de regra, a permitir um órgão para armazenar de forma centralizada os registros, e outro para realizar a fiscalização das contas públicas de maneira centralizada.

Contudo, a *blockchain* é desenhada para uma mudança de paradigma em que a tecnologia retira de uma entidade centralizadora e torna o cidadão ou cidadã comum um registro vivo da inteira cadeia de blocos, tornando os cidadão ou cidadã um verdadeiro ponto de fiscalização. Se uma entidade de fiscalização em busca da probidade administrativa pode ser um obstáculo contrário à corrupção[418], quanto mais obstáculos existir, melhor se conseguir atingir tal objetivo; afinal, o agente corrupto precisaria corromper todas estas entidades fiscalizadoras.

Um dos anseios de uso efetivo da KSI *blockchain* na Estônia é no âmbito da Saúde Pública. Conforme preceitua o *paper* oficial da Guardtime Federal: "*There is no other sector where corruption-free data matters more than in Healthcare/Healthcare IT"*[419]. E, usando o exemplo da KSI *blockchain*, afirmou-se que a integridade dos dados que a *blockchain* permite um complemento às soluções de prestação de cuidados de saúde que já existem e não uma substituição total, sendo a assinatura KSI uma ferramenta capaz de assegurar assinaturas digitais por cada transação e paciente do sistema de saúde e, segundo o estudo, tem permitido uma ligação com o "Nationwide Interoperability Roadmap" para fins de uma interoperabilidade de sistemas. Afinal, a KSI estoniana é desenvolvida de forma a ser escalável, interoperável e facilmente controlada e integrada nos e integradora dos demais sistemas já existentes[420].

Em outros termos, uma descentralização dos registros de saúde estonianos, por mais sensível que pareça ser, foi possível através da tecnologia *blockchain,* já que esta descentralização permitiu aos indivíduos acessarem seus registros usando apenas o cartão de identificação. A rede permite diferentes naturezas de acesso (também por médicos em casos de emergência) e qualquer acesso ilegítimo transparecerá uma violação dos dados pessoais[421] suscetível de redundar num risco para os direitos e liberdades das pessoas (com o agravante de envolver categoria especial de dados pessoais), o que recai na previsão do artigo 33 do RGPD.

---

[418] Ressalva-se que a existência de uma ou várias entidades de fiscalização não significa um impedimento para que ela aconteça.

[419] Guardtime Federal LLC. "Keyless Signature Infrastructure® (KSI™) Technology". Disponível em https://www.guardtime-federal.com/guardtime-federal-background/ Acesso em 26/06/2020

[420] Guardtime Federal LLC. "Keyless Signature Infrastructure® (KSI™) Technology". Ibid.

[421] El Mouallem, Atie J. Ibid.

Não obstante, além de um controle transparente quando houver uma violação do RGPD, a cadeia de blocos torna o trabalho de fiscalização de contas públicas mais fácil, à medida que uma só cadeia de registro vai reunir todos os gastos em recursos de saúde. Nestas circunstâncias, a tendência é assegurar uma responsabilidade na gestão fiscal[422], para cumprimento das normas do Direito Financeiro, mas também um controle aberto sobre como ocorreu cada gasto orçamentário a representar um desafio ainda maior para quem deseja esconder operações ilícitas e corruptas.

Para corroborar a ligação entre transparência e combate à corrupção, AARVIK da instituição norueguesa Chr. Michelsen Institute (CMI)[423], que possui o U4 (grupo voltado ao desenvolvimento internacional contra a corrupção), ao analisar a *blockchain* estoniana como uma ferramenta no combate à corrupção, fez um importante atrelamento entre a corrupção no setor público com a falta de confiança dos cidadãos, onde a transparência e a existência de registros públicos abertos seriam um caminho para facilitar a monitoração do uso dos recursos públicos e, ao mesmo tempo, vocacionado a reduzir o risco de atos corruptos. E, para tanto, o CMI elegeu a *blockchain* como uma ferramenta que oferece registros inalteráveis que agentes corruptos e burocratas não poderão modificar, já que a forma distribuída do livro-razão e seus mecanismos de consenso "torna[m] difícil que uma entidade realize falsas entradas"[424].

Importante estabelecer um contraponto: não se deve generalizar o encontro da *blockchain* estoniana com o combate à corrupção, uma vez que nem toda solução tecnológica apresentada pelo governo da Estônia corresponde a uma *blockchain*. E também, por outro lado, não se pode afirmar que foi possível erradicar completamente a corrupção da Administração Pública estoniana. Afinal, de acordo com estudo liderado pela GAN Integrity, apesar de a prestação de serviços públicos decorrer quase na totalidade de forma *online*, encontrou-se um "moderado risco de corrupção" [425].

Apesar de nenhuma empresa entender que conceder vantagens ilícitas para obter uma licença é possível (GCR 2015-2016), outra pesquisa apontou que 2 em cada 5 empresas concordaram que, na Estônia, o suborno ainda é a maneira mais fácil de obter a prestação de serviços públicos (Flash Eurobarometer 2017) e, na mesma proporção, 40% dos entrevistados acreditam que a corrupção é

---

[422] Parte da doutrina defende que a responsabilidade na gestão fiscal é necessária ao combate da corrupção. Neste sentido Oliveira, Robson Ramos. "Contabilidade, controle interno e controle externo: trinômio necessário para combater a corrupção." Rio de Janeiro: Pensar Contábil, vol. 8, n. 31, 2008.

[423] Aarvik, Per. "Blockchain as an anti-corruption tool (Case examples and introduction to the technology)". Bergen, Noruega: U4 Issue, 2020

[424] Aarvik, Per. Ibid. p. 10.

[425] GAN Integrity. "Estonia Corruption Report". Disponível em https://www.ganintegrity.com/portal/country-profiles/estonia/ Acesso em 23/06/2020.

comum entre os agentes públicos[426]. Segundo a GAN ainda, a maioria dos casos de corrupção resultam da atividade de autoridades nacionais, sobretudo se comparado com os desvios de finalidade a nível municipal, já que aqui o fenómeno parece estar diminuindo (SGI 2017). Ainda assim, é conhecido o caso que envolveu o prefeito de Tallinn, Edgar Savisaar, que foi acusado de ter recebido suborno, envolvendo diversos outros políticos e partidos[427].

Se não se pode afirmar que a Estônia, mesmo na vanguarda de uma regulação digital, como a precursora na adoção da *blockchain* a nível nacional, conseguiu erradicar por completo a corrupção, ao mesmo tempo, não é possível afirmar que todas as soluções que envolveram tecnologia (ou sequer envolveram uma forma de registro baseada em criptografia) corresponde a um uso da tecnologia *blockchain*. Para citar como exemplo, pode-se mencionar o X-road: um software que dá acesso a serviços digitais. Projeto antigo que desejava conceder acesso digital aos serviços públicos pelos cidadãos, a baixo custo de implementação, mas de forma transparente e responsável. Se existem diversas bases de dados para cada setor do Estado (educação, segurança pública, saúde, eleições...), o X-road dá acesso a essas bases de dados, sendo uma *"digital highway"*[428] em termos de soluções de interoperabilidade.

É verdade que as conexões através do software são criptografadas de ponta a ponta e utilizam-se códigos *hash* para identificar e aceder à informação; no entanto, o NIIS (*Nordic Institute for Interoperability Solutions*) expressamente defende que o X-road não é baseado na *blockchain*[429]. Apesar de KIVIMÄKI[430], no seu artigo do The New Yorker, tratar o X-road como uma *blockchain*, tal artigo trata-o como dois institutos distintos e, inclusive usa de metáforas didáticas para explicar que o X-road funciona como uma travessia de barco[431] e já a *blockchain* é como se fosse uma "versão digital de um cachecol que usa um novelo de lã contínuo e cada ponto depende do ponto anterior"[432].

Inclusivamente, HELLER traz uma informação relevante no debate da *blockchain* em face da Proteção de dados levantado ao longo deste estudo ao lecionar que a KSI *blockchain* torna cada rastro imediatamente noticiável sem revelar dados pessoais da fonte. Para o autor, não é possível uma "*back*

---

[426] GAN Integrity. Ibid.

[427] Prosecutor, lawyers appeal Savisaar corruption ruling to Supreme Court. Disponível em https://news.err.ee/1143148/prosecutor-lawyers-appeal-savisaar-corruption-ruling-to-supreme-court Acesso em 23 de junho de 2020.

[428] Aarvik, Per. Ibid. p. 16.

[429] Kivimäki, Petteri. "There is no blockchain technology in the X-Road." Noruega: Nordic Institute for Interoperability Solutions, 2018.

[430] Ibid.

[431] "X-Road, vincula servidores individuais através de caminhos criptografados de ponta a ponta, permitindo que as informações sejam exibidas localmente. Seu a prática do dentista mantém seus próprios dados; o mesmo acontece com sua escola e seu banco. Quando um usuário solicita uma informação, ela é entregue como uma travessia de barco um canal através de fechaduras". Tradução livre. Veja-se em Heller, Nathan. "Estonia, the digital republic". Nova York: The New Yorker, v. 18, 2017. p. 5.

[432] Tradução livre. Heller, Nathan. Ibid. p. 5

door" (ou algum privilégio indevido), porque a KSI guarda segredos - leia-se dados - ao proteger e conceder acessos específicos, sem, entretanto, enxergar a informação *per si*[433].

E esses avanços tecnológicos, evidenciados pela adoção nacional da *blockchain*, são demonstradas pelo sentimento popular em geral, e apesar de o *Eurobarometer* 2017 acima analisado demonstrado que ainda existe corrupção na Estônia[434], precisa-se vislumbrar a corrupção sob um panorama mais amplo, e até comparativo entre Estados-Membros, a fim de entender o fenômeno e o trabalho estoniano em face do mesmo.

A União Europeia realiza pesquisas a cada 2 anos que mostram diversos questionamentos relacionados com a corrupção, em nome da sua determinação em combater a corrupção no seu seio e em estabelecer uma política sólida de diálogo com as ordens jurídicas de cada Estado-Membro. O estudo do Eurobarometer[435], iniciado em 2013 e repetido em 2015 e em 2017, teve sua última versão publicada em dezembro de 2019, e mostra uma impressão real de práticas corruptas como suborno encarado por empresas e fraudes em licitações e contratos públicos.

A Comissão Europeia[436] listou diversas configurações que a corrupção pode assumir, quais sejam o suborno, a troca de influências, o abuso de função, sem excluir as práticas de nepotismo, os conflitos de interesse ou até a confusão patrimonial entre setor público e privado. Os indicadores desta investigação realizada pela UE, apesar de mostrarem o ponto de vista de cidadãos e empresários, e não números absolutos ou quantias desviadas, caracterizam a corrupção também como um sentimento social, no qual um dos piores efeitos vai ser a falta de confiança que gera um sentimento de impunidade, este que é um modelo perigoso para a harmonização das instituições sociais.

E diante desta problemática, o mesmo relatório da União Europeia indica que a implementação massiva da *blockchain* por parte da Administração Pública não foi capaz de erradicar a corrupção sequer do sentimento popular. Ainda existe resquícios do ideal comum de que a corrupção faz parte da Administração Pública, mas merece destacar que, segundo a mesma pesquisa, o Governo estoniano está bem avaliado sob o ponto de vista dos cidadãos. Para ilustrar, uma das perguntas da pesquisa foi a possível existência do conflito de interesses na avaliação dos lances de licitações públicas, o que significa uma violação de vários princípios do Direito Administrativo. Assim como em diversas outras

[433] Heller, Nathan. Ibid.
[434] GAN Integrity. Ibid.
[435] Europeia, União. Flash Eurobarometer 482. "Businesses' attitudes towards corruption in the EU". Directorate-General for migration and home affairs, Comissão Europeia. 2019.
[436] Europeia, União. Flash Eurobarometer 482. Ibid.

perguntas desta pesquisa, a Estônia aparece como uma das melhores marcas, conforme se depreende abaixo:

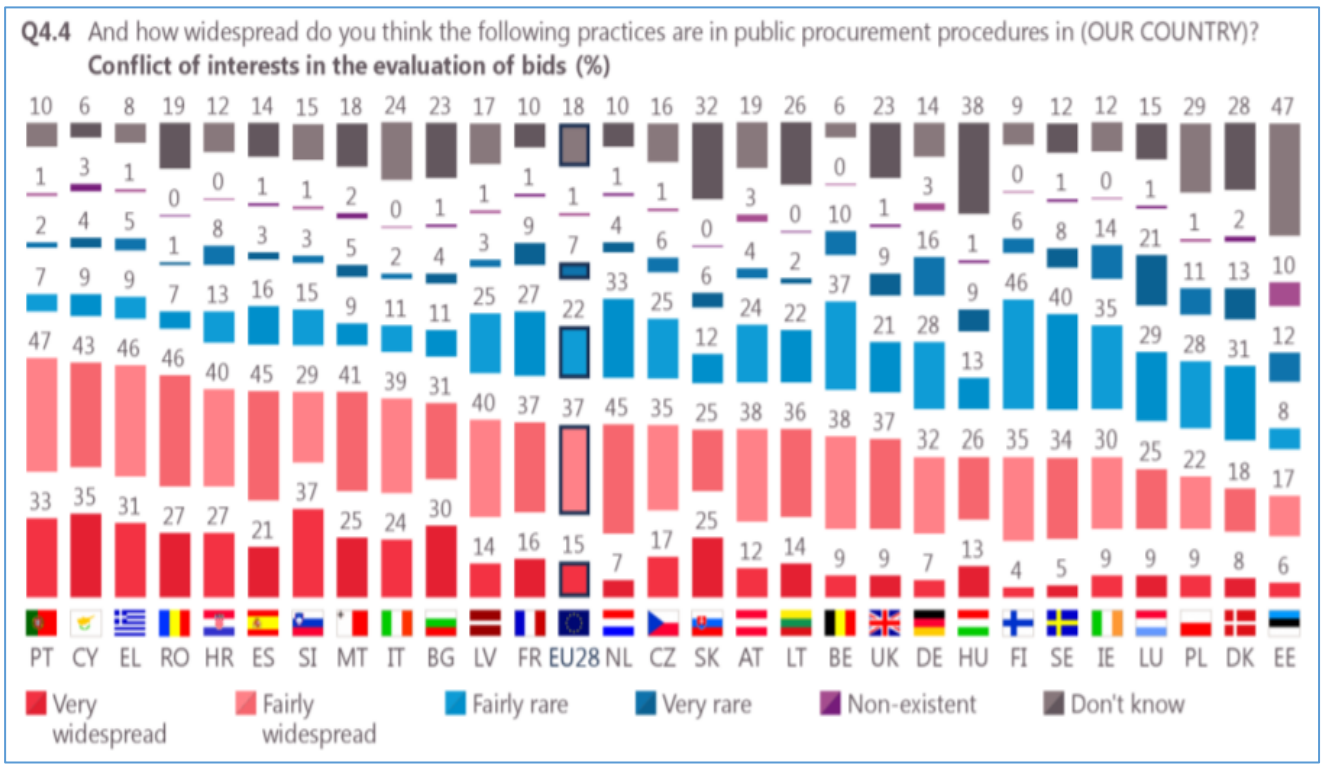


Figura 3: Flash Eurobarometer pela Comissão Europeia[437]

Em contraponto, nota-se que a população portuguesa enxerga esta prática, quase que de forma unânime, como uma regra na Administração Pública e Portugal obteve o pior indicador na União Europeia - ao contrário da Estônia, tendo em conta que poucas pessoas afirmaram que o conflito de interesses nas licitações era um ato amplamente praticado.

Seguindo a mesma lógica, outro medidor apresentado foi abuso em procedimentos de negociação, o que causa sérios prejuízos ao Erário público, e acaba por ser um grande desafio no combate à corrupção, sobretudo no que diz respeito a atos administrativos discricionários em que a própria lei concede um poder de juízo para o agente público. Ao serem indagados se a prática era amplamente desenvolvida, Romênia e Portugal apresentaram os índices mais pessimistas, com mais de 70% dos indivíduos entendendo que o abuso é amplamente comum, ao contrário da Estônia que apresentou o melhor índice, com apenas 14% neste sentido (resultados indagados a propósito da análise conduzida da imagem abaixo):

[437] Europeia, União. Flash Eurobarometer 482. "Businesses' attitudes towards corruption in the EU". Directorate-General for migration and home affairs, European Commission. 2019. P. 118

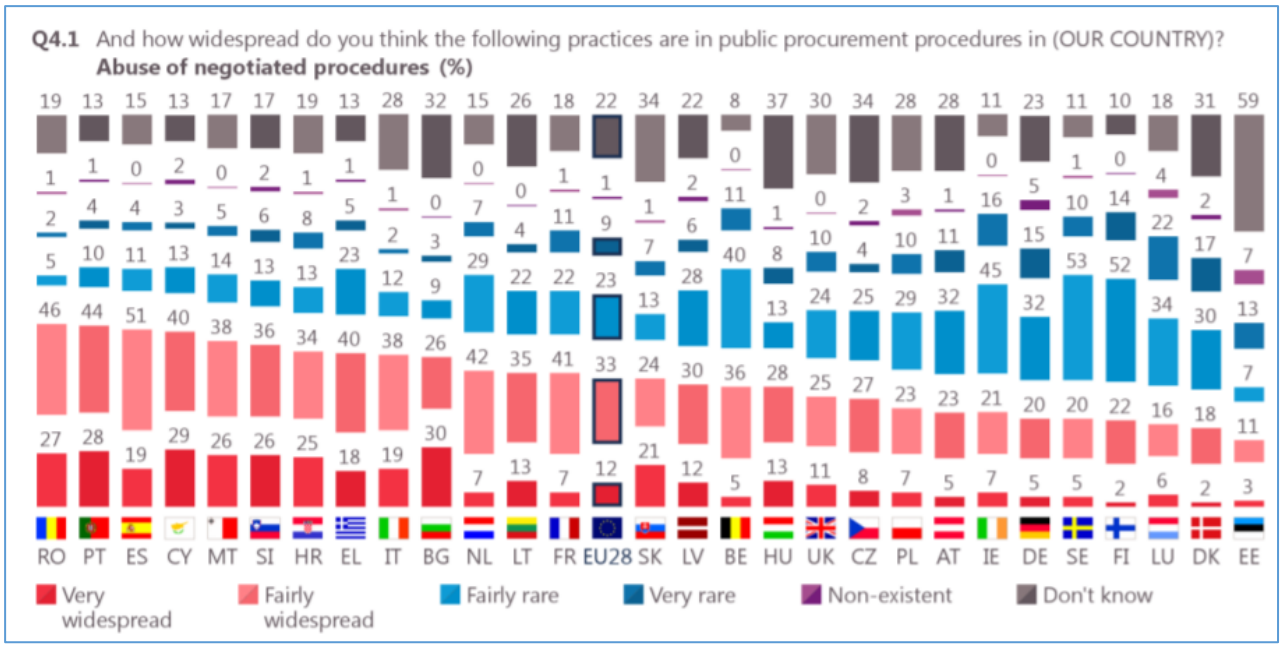


Figura 4: Flash Eurobarometer pela Comissão Europeia[438]

Diante destes resultados, não se pode afirmar que uma Administração Pública baseada na *blockchain* é *"corruption free"* por não haver evidência científica para realizar tal declaração mas, ao mesmo tempo, segundo a pesquisa, o setor privado apresentou índices que transparecem um descrédito que a corrupção seja a regra na Estônia, e a adoção da *blockchain* é circunstância relevante neste sentimento social de segurança jurídica. Consequentemente, a segurança jurídica nos processos administrativos vai favorecer a confiança da iniciativa privada em desenvolver negócios e obter a atrativa "*e-residency*"[439] na Estônia. Os números da Estônia, apesar de não serem absolutos, como a GAN Integrity bem fez o contraponto, em comparação com os outros Estados-Membros inseridos no contexto da União Europeia, demonstra uma interessante confiabilidade por parte dos indivíduos em relação à Administração Pública.

É verdade que muitos indivíduos desconhecem algumas das práticas ilícitas indagadas e, mais ainda, desconhecem a relação de uma *blockchain* com o combate a tal corrupção, mas num macropanorama das circunstâncias, a Estônia assume um protagonismo a nível da União Europeia no que concerne à busca por uma solução do anteriormente mencionado complexo público-privado[440]

[438] Europeia, União. Flash Eurobarometer 482. Ibid. p. 124

[439] A Estônia é o primeiro país a oferecer a e-Residency, o que permite empreendedores digitais começarem uma empresa online, baseada na UE, através de uma identificação e status provido pelo Governo para realizar todos os atos, até a abertura, de forma digital. Disponível em https://e-resident.gov.ee/ Acesso em 26 de junho de 2020.

[440] Neste sentindo, veja-se: García-Pelayo, Manuel. Ibid.

através de plataformas tecnológicas que buscam promover a transparência administrativa, mas ao mesmo tempo, em conformidade com o RGPD.

Falou-se que a crise dos tempos atuais passava pela "ausência de mecanismos eficientes"[441], o que causa uma incongruência latente na relação "administrado-administrador", já que esta estaria mais frágil pelo fato do cidadão não mais enxergar uma voz nos seus representantes. A tranquilidade do setor privado estoniano é um indicativo de que a demora do Estado em incorporar novas tecnologias contribui para esta incongruência. Esta que muitas vezes, inclusive, não é perceptível. Sendo o paradigma estoniano o de um país de histórico econômico não favorável e de recente desenvolvimento, vê-se uma Administração Pública em linha que consegue transparecer uma maior segurança jurídica e transparência aos seus cidadãos, em consequência de um Estado que favorece a Proteção de dados pessoais e que se baseia num modelo de regulação tecnológica. A Estônia é um exemplo de que a tecnologia incorporada na prestação dos serviços públicos é uma tendência a ser seguida: se os recursos tecnológicos promoverem a transparência administrativa, isto será importante para combater a corrupção administrativa, seja através da tecnologia *blockchain* ou não, criando forte segurança nos particulares para encontrarem, nesse espaço, um ambiente favorável a se estabelecerem e contribuírem proativamente para o desenvolvimento da economia.

[441] Neste sentindo, veja-se: Limberger, Têmis. Ibid.

CONCLUSÃO:

Ante o exposto, o presente estudo passa por diversos conceitos em um momento primordial, para após longo percurso conceitual acerca da Proteção de dados e da tecnologia *blockchain*, traçar uma interseção entre os dois conceitos, de forma a ver quais particularidades de um potencial uso desta tecnologia apresentariam uma ameaça aos direitos e princípios enunciados no enquadramento normativo da União Europeia em relação à Proteção de dados pessoais.

Posteriormente, e depois de conduzido este debate de adequação e conformidade, passa-se a trazer a *blockchain* sobre um desígnio específico, qual seja a geração de transparência na Administração Pública para fins de mitigar práticas corruptas (processo este que demandou o entendimento do fenômeno da corrupção e seu funcionamento para averiguar se o uso da *blockchain* pode oferecer uma solução plausível, em determinado contexto).

Primeiramente, concluiu-se, a partir da interpretação literal da norma, que a Proteção de dados é um princípio fundamental que preceitua amparo de natureza universal, pertencente a todas as pessoas que se encontrem sujeitas ao âmbito de aplicação das normas jurídicas europeias. É estabelecido que a Proteção de dados é direito originário da União, fruto de um amadurecimento jurisprudencial e de uma evolução legislativa que conduziram a este padrão de jusfundamentalidade imposto. Seja por força do artigo 8.1 da CDFUE, seja também pelo TFUE em seu artigo 16, é reconhecido por previsão expressa a Proteção de dados, quer enquanto princípio geral, quer enquanto direito fundamental. Por isso, esta já havia recebido *status* de direito fundamental anteriormente ao RGPD. A atribuição de força vinculativa idêntica aos tratados à CDFUE, em virtude da literalidade do artigo 6º do TUE e da própria prática e jurisprudência da União Europeia, conduziram a tal proteção, ainda antes da adoção do atual RGPD.

No mesmo sentido do referido posicionamento legislativo a nível europeu, a Carta Magna portuguesa, em seu artigo 35 da CRP, passa a ser pioneira a tratar da chamada autodeterminação informativa, concedendo, ao titular dos dados, o direito de conhecer a finalidade do tratamento de suas informações pessoais. E por isso é que a Proteção de dados, seja a nível da União, seja a nível nacional português, possui um caráter jusfundamental preliminar ao RGPD.

E foi a partir desta construção que se culminou na adoção do RGPD. O RGPD passa a ser considerado um padrão dotado de um âmbito material para fins de tratamento de dados pessoais, conforme inserido expressamente na definição do seu artigo 4.1. As possíveis técnicas de

anonimização servem como uma forma de, apesar das metodologias legislativas diferentes, oferecer uma solução lícita ao tratamento de dados pessoais, à luz da Constituição Portuguesa e do Regulamento 2016/679.

Uma das primeiras distinções conceituais que foi feita consistiu na conclusão de que a noção de privacidade, conceito norte-americano, não constitui direito autônomo para o Ordenamento dos EUA, uma vez que a privacidade decorre da própria pessoa e a doutrina americana passou a seguir a histórica obra de Warren e Brandeis. Portanto, os EUA definiram que a privacidade é uma esfera que decorre de uma visão centrada no indivíduo. Por outro lado, há a ótica europeia, cujo triunfo foi após longa evolução legislativa deixar expressamente declarado que a Proteção de dados é um direito autônomo que tem natureza de garantia fundamental, seja a nível nacional português (consoante o artigo 35 da CRP), seja no nível europeu conforme a CDFUE e TFUE. Por isso, pode-se afirmar que a Proteção de dados é direito autônomo e não uma esfera, o que a difere da privacidade, apesar de que em diversas circunstâncias haja pontos em comum entre esses dois conceitos.

Essa distinção privacidade e Proteção de dados foi importante ao estudo em face de toda a construção teórica que foi feita. Em diversos momentos são consideradas tecnologias que envolvem a problemática do sigilo da informação pessoal, ponto crucial na diferenciação dos institutos. De um lado a visão americana da privacidade acaba por ser um reflexo jurisprudencial, baseado na "*Fourth Amendment*" da Suprema Corte dos Estados Unidos que sustenta a ideia de que se uma questão apresenta completa ausência de sigilo, ela deixa de ser privada. Do outro lado, pode-se citar o RGPD que inclusive protege também informações que já saíram do domínio pessoal e sofreram um vazamento, por não vincular o direito fundamental à Proteção de dados como esfera da vida privada, mas sim um direito autônomo constitucionalmente estabelecido.

E após traçar esta diferenciação, foi frutífero realizar uma evolução temporal da Legislação, a fim de comprovar esta presunção de que a Proteção de dados é um pilar do Estado Democrático de Direito, uma vez que, em seguida, parte-se para analisar uma tecnologia tendente a oferecer soluções a este valor assente na observância da legalidade. Em outras palavras, a *blockchain* não poderia ser analisada no contexto de uma Administração Pública da qual não se sabe como ela é pautada, e pelo fato da *blockchain* ser basicamente registro de informações, foi imperioso discutir qual a trajetória até chegar ao RGPD como uma normativa paradigma para fins de regulação administrativa.

E, nesta evolução, foi trazida uma das primeiras tutelas internacionais, a saber a Declaração Americana dos Direitos e Deveres do Homem de 1948 que demandava o direito à proteção da lei sobre a vida particular. Logo em seguida, aprovada foi a Declaração Universal dos Direitos do Homem.

Esta também declarou, no seu artigo 12, a proteção da privacidade, passou-se então pela Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais, cujo artigo 6º fala no direito à intimidade da vida privada, e ainda, a elaboração da Recomendação 509 da Assembleia Consultiva do Conselho da Europa, cujo destaque foi dado aos direitos da personalidade, trazendo, de forma inovadora, questões acerca da vida privada em relação a interceptações telefônicas e à captura de imagens sem autorização, mostrando-se relevante para esta evolução legislativa.

Não suficiente, além do curso legislativo que foi aprimorando a conceção da proteção de dados, em 1968 houve uma importante decisão do Tribunal Constitucional Federal alemão: esta ficou estabelecido o direito à autodeterminação informativa (*Recht auf Informationelle Selbstbestimmung*) com reconhecimento e elevação ao justo status constitucional. Esta decisão considerou, portanto, a proteção dos dados pessoais como direito autônomo aos direitos de personalidade. E esta foi a base europeia para ser adotada a Diretiva 95, um marco histórico para o livre fluxo de informações pessoais no mercado interno em condições de segurança para os titulares dos dados. A fim de que as legislações ficassem mais homogêneas, a Diretiva de 95 buscou uma harmonização com o escopo de orientar os Estados-Membros a um nível de proteção equivalente.

O presente estudo chega enfim no grau de maturação promovido pelo RGPD, a fim de promover uma aplicação uniforme do direito da União Europeia em virtude de a Diretiva antecedente ter demonstrado uma finitude na consecução plena da proteção de dados pessoais, ao promover apenas uma tendencial harmonização do seu regime. E dentre as benesses de um Regulamento Europeu nesta matéria, há um reflexo no que concerne a adoção da *blockchain* – como uma tecnologia baseada em fluxo e registro de dados. Se este trabalho optou por vislumbrar o uso desta tecnologia pelo Estado para gerar mais transparência e dificultar a corrupção, averiguar a possibilidade de aplicação do Regulamento sobre usos da *blockchain* se faz relevante para fins de pensar na Administração Pública – regida pela legalidade - que utiliza a *blockchain* em conformidade com toda esta estrutura normativa que protege o Direito fundamental à proteção de dados.

Por isso, a uniformização da execução e aplicação da legislação, no que se refere ao tratamento dos dados pessoais, surgiu para garantir segurança jurídica a uma devida atividade econômica, sem entraves e com livre concorrência. Mas, ao mesmo tempo, o setor público precisa observar o RGPD, não apenas porque também pode ser sujeito passivo das obrigações decorrentes do RGPD, reputando-se como responsável pelo tratamento à luz dos seus termos literais, mas também porque o Regulamento é fruto de uma evolução doutrinal e jurisprudencial que dá ainda mais

significância ao direito fundamental da Proteção de Dados. Este contexto deve ser o primeiro passo numa implementação de sistema de registro público baseado na *blockchain*.

Conforme foi dito, o RGPD vai ser um desígnio padrão para qualquer uso da *blockchain* e, dentre os diversos conceitos trazidos, e conforme foi antecipado ainda no início da dissertação, o âmbito normativo, seja material, seja formal, é essencial para a análise de conformidade, uma vez que é um dos escopos é o de adequar os usos de uma tecnologia, em especial a *blockchain*, aos desígnios de um possível ajustamento para implementação pela Administração Pública, em especial no combate à corrupção. E este paradigma de uma *blockchain* estatal passou a ser encarado à luz, por exemplo, do n.º 2 do artigo 2 RGPD que elenca hipóteses nas quais irá haver tratamento de dados pessoais que legalmente foram excepcionadas do enquadramento da proteção da norma.

O primeiro capítulo deste trabalho concluiu que, apesar de aprofundamentos posteriores, os antecedentes jurisprudenciais ajudaram na percepção de traçar a dificuldade de inserir uma *blockchain* pública no contexto da exceção do exercício de atividades exclusivamente pessoais ou domésticas, uma vez que é clara a opção legislativa em normatizar uma moldura de largo âmbito material, para fins de assegurar um elevado nível de proteção. Fora que a letra expressa da lei não esgota a matéria, que vem sendo construída jurisprudencialmente a nível europeu, desde casos pretéritos como *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* (C-131/12), *Weltimmo v NAIH* (C-230/14), *Verein für Konsumenteninformation v Amazon EU* (C-191/15) e *Wirtschaftsakademie Schleswig-Holstein* (C-210/16).

A partir do segundo capítulo, trouxe-se uma conceituação e detalhamento da tecnologia *blockchain*. Detalhes desta tecnologia precisaram ser desenvolvidos para buscar uma possível adequação da mesma ao arcabouço jurídico criado para fins de Proteção de dados pessoais, pois na *blockchain* ocorre tratamento de dados por definição. Na verdade, os exemplos de utilização de *blockchain* mais famosos (desde as criptomoedas aos sistemas de rastreamento de alimentos pela cadeia logística) mostram que a definição simples seria considerá-la uma forma de inserção de dados em uma base de dados distribuída que obedecerá a regras de temporalidade, parentesco entre os blocos e descentralização.

Buscando traçar as problemáticas da sociedade atual à luz da evolução histórica, o exemplo do mecanismo de apropriação ilegal de terras públicas mostrou o quão desejadas e praticadas são, ao longo dos séculos, a burla aos registros públicos e falsificação de documentos estatais. E este foi o embrião da linha de pensamento que permeou o curso da presente investigação no entendimento do uso da *blockchain* na Administração Pública como uma possível solução para problemas de ausência

de transparência e práticas corruptivas no seu seio: solução esta não apenas por apresentar uma forma diferente de registro relativamente ao modelo tradicional mas, ao mesmo tempo, por impor dificuldades para aqueles que buscam violar estes registros públicos.

Conforme demonstrado, a base registral do Estado Moderno ocidental foi a matemática importada pelo Liber Abaci de Fibonacci, assim como com o registro de partidas dobradas desenvolvida por Luca Pacioli criando o livro-razão de partidas dobradas, que representou não apenas o prelúdio das Ciências Contábeis, mas também os alicerces da burocracia e da Administração Pública. A *ledger* baseada nas partidas dobradas impulsionou – de imediato – práticas econômicas inovadoras, uma vez que surgiram intermediários para desenvolver uma atividade bancária incipiente e usar esta forma de registro para creditar e debitar transações à distância. E a História indica que a *blockchain* tem potencial de realizar uma repetição cíclica, afinal também é uma forma de registro, primeiramente adotada no contexto econômico (criptomoedas), mas em processo de adoção pelos Estados para prestação de serviços públicos.

Por estar no meio de um processo de adoção, não se pode afirmar agora se a *blockchain* vai virar uma regra da Administração Pública do futuro, mas ela trata de um quesito efetivo: a promoção da confiança e, consequentemente, imprime maior transparência à atividade administrativa. Se o registro de partidas dobradas ofereceu a estrutura necessária para desenvolver o papel de intermediários (sejam bancos, sejam órgãos públicos), a *blockchain* retira intermediários para que a confiança seja baseada na própria tecnologia.

As propriedades técnicas da *blockchain* mostram uma potencial segurança jurídica e confiabilidade que promove a retirada de intermediários, podendo diminuir a corrupção que ocorre justamente no seio das instituições dotadas de dizer "a verdade" dos registros. Constata-se que, por mais que um órgão público teoricamente obedeça a princípios de legalidade, transparência e imparcialidade, o agente público que o representa poderá utilizar o sistema estatal em favor pessoal. Isto representa um desvio da finalidade pública, a qual passa a ser facilitada quando a forma de registro for facilmente alterável e dificilmente auditável.

Dentre as propriedades técnicas da *blockchain*, a propriedade do parentesco entre blocos e a criptografia aplicada mostram que o registro na *blockchain* é dificilmente adulterado. Seja a presença do código *hash digest* referente ao bloco exatamente anterior, seja o *hash digest* de todas as transações que forem registradas naquele bloco, ou ainda o *timestamp* funcionando como prova temporal de quando o bloco foi validado; resta matematicamente baixa a probabilidade do registro na

blockchain ser ilicitamente alterado, uma vez que, para haver uma violação do bloco, precisa haver uma necessária "revalidação" de toda a cadeia de blocos subsequente.

Só isto já seria uma mais-valia no combate à corrupção (prática esta que necessita comumente contrafazer registros para esconder desvios), mas além da estruturação dos blocos, a *blockchain* ainda descentraliza o registro em tempo real, sendo um livro-razão praticamente impossível de adulterar, afinal todas as entidades do sistema serão um registro autônomo e simultâneo do livro-razão, restando infrutífera uma adulteração centralizada. Portanto, além de tudo acima, ainda foi mencionado que a *blockchain* pode ser auditável e oferecer anonimização das entidades que dela fazem parte. A conclusão que se chega é que a confiança é dada pela própria tecnologia.

Sabendo que a tecnologia segue protocolos, os possíveis protocolos relacionados com a *blockchain* foram equacionados. Dentre eles, foi delineada a prova de conhecimento zero (ZKP), a qual pode ser utilizado no registro de dados da *blockchain*, cujo método de provar informações é lastreado em compromissos criptográficos firmados de maneira simultânea entre as partes, e sem revelar informações adicionais. E este método apresentou uma mitigação da problemática da privacidade no momento de validar um registro na *blockchain*. Esta preocupação da proteção de dados neste sistema, faz da *blockchain* uma tecnologia, além de segura, que possa oferecer soluções de tratamento lícito de dados àqueles que validam suas transações, conforme aquele direito fundamental.

Ante o exposto, a forma regulatória da *blockchain* demonstrou ser essencial para fins de conformidade, afinal o RGPD concede ao responsável pelo tratamento a opção (e riscos) de definir tais peculiaridades. No desenho específico da *blockchain* no contexto da Administração Pública, foi crucial notar que, nas *blockchain* públicas, as chaves criptografadas de acesso são amplamente acedidas, seja qual for a operação: consultar ou realizar operações propriamente ditas. Em contraponto, foi apresentado, como recomendado, o modelo regulatório de uma *blockchain* a ser desenvolvida por parte de um órgão público, a *blockchain* permissionada, à luz das opiniões das Autoridades de controlo e do próprio Comité Europeu.

Este protocolo sob permissão possui como característica principal o controle das chaves de acesso e obrigação de solicitar autorização para as escrever dados na *blockchain*. Este modelo regulatório mostra-se promissor para uma adoção escalável da tecnologia *blockchain* por parte da Administração Pública perante a necessidade de promover uma Proteção de dados pessoais, caso seja possível, em certos casos, registrar dados através de protocolos de conhecimento zero.

A debatida dicotomia *blockchain* e RGPD mostrou-se uma contenda de várias nuances, que passa pelo âmbito material do Regulamento e também por hipóteses de tratamento lícito. Como o

desígnio deste trabalho foi pensar uma *blockchain* para a Administração Pública, restou afastada a aplicação da exceção do artigo 2.2 (c) RGPD que delimita o âmbito de aplicação do RGPD para tratamentos de dados pessoais para fins estritamente pessoais ou domésticos por parte de pessoa singular, além do mais porque *design* distribuído e descentralizado dificulta a suposição de algum uso desta tecnologia que seja estritamente particular.

Todavia, um caminho encontrado em busca de conferir confidencialidade ao uso da *blockchain* foi a cifragem da informação a ser registrada através de um algoritmo e chave, permitindo que o texto literal dos dados pessoais apenas seja lido pela entidade que detenha a chave privada utilizada na cifragem. E a verdadeira anonimização, fruto da cifragem, mostra-se uma suficiente forma de retirar o tratamento do âmbito de aplicação do RGPD, sob a condição de que os titulares não sejam mais identificáveis, à luz do Considerando 26 cuja estipulação sedimentou que o RGPD não diz, por isso, respeito ao tratamento dessas informações anónimas.

O esforço ao tentar afastar o uso da *blockchain* do âmbito material do RGPD consiste no desafio em compatibilizar certos direitos dos titulares, bem como a necessidade de promover a observância de determinados princípios. Dos direitos, os mais suscitados como potencialmente potenciadores de problemas são o da retificação e o do apagamento. Tendo em vista as particularidades informáticas já explicadas, não é tecnicamente possível modificar um bloco específico e manter a integridade da rede *blockchain* como um todo. O caminho de utilização, em conformidade com o direito de oposição, e consequentemente o direito de apagamento, mostrou-se ser a adoção de uma arquitetura (seja modelo de governança, protocolos de validação, etc.) que ressalte a privacidade desde a conceção e por defeito, em atenção ao artigo 25 RGPD.

A tempo, faz-se a ressalva que todos os estudos disponíveis até o momento, sejam doutrinários ou documentos oficiais disponibilizados por órgãos de controlo, são apenas recomendações que não podem ser consideradas definitivas, ou soluções de tamanho único, considerando que o *"risk-based approach*", consagrado pelo RGPD, exige uma análise caso a caso e uma opção por parte do responsável pelo tratamento. E é por este motivo que implementar uma solução baseada na *blockchain* deve ser decisão final após uma análise de risco, lastreada em uma "Avaliação de impacto sobre a proteção de dados", prevista no artigo 35 RGPD. Tal instrumento contribui para o ajuizamento da necessidade e proporcionalidade da pretendida solução que utilize a tecnologia *blockchain*, que pode ser ou não a alternativa mais adequada para os fins específicos.

Dito isto, as possíveis arquiteturas e particularidades de cada modelo de aplicação concreta da *blockchain* podem oferecer maior ou menor segurança jurídica – a levar em consideração o

oferecimento de medidas técnicas e organizativas que vislumbram a aplicação com eficácia dos princípios e direitos da Proteção de dados. Então, é de concluir que a *blockchain* apresenta potencial de ser a base tecnológica de uma solução legítima para a Administração Pública. Esta que, por essência, precisa seguir o princípio da legalidade, abrangendo a norma positivada através do RGPD. E para não debater todo e qualquer uso, o presente trabalho precisou limitar-se a pensar à tecnologia *blockchain* promovendo mais transparência e segurança de dados e registros públicos.

Mesmo que a incorporação de um uso concreto da *blockchain* obedeça ao arcabouço normativo da Proteção de dados pessoais, conforme debatido, foi visto que a conformidade não seria o único obstáculo para uma adoção massiva da *blockchain* com fins de basear uma Administração Pública em linha. Manifestou-se que o setor público apresenta um problema crônico em incorporar novas tecnologias no ritmo que o setor privado o faz.

Considerando que, por um lado, as demandas sociais estão cada vez mais céleres, e que, por outro lado, o processo de inovação estatal passa pela edição de leis e regulamentos por parte do Legislativo, além da implementação de políticas públicas que orientem os processos administrativos, verifica-se que esta complexidade estatal afeta a introdução de novas tecnologias por parte da Administração Pública.

O descompasso das necessidades dos administrados, somado à lentidão de resposta por parte da Administração, acaba por ser um dos motivos de afastamento entre cidadania e democracia participativa. Não obstante, ao discorrer sobre demais motivos para esta problemática, em que a Administração Pública acaba por oferecer um afastamento, concluiu-se que a falta de transparência na Administração Pública acaba por conduzir a um aumento do fenómeno da corrupção e, bem assim, uma afetação da capacidade participativa do administrado.

A relação direta encontrada entre falta de transparência e prática de corrupção administrativa deve-se ao fato de que um Estado insuficientemente transparente acabar por facilitar desvios de finalidades, onde os patrimônios do agente público e a coisa pública confundem-se e o interesse particular passa a guiar as políticas públicas, em prol deste e de outros favorecimentos ilícitos.

E desta evolução conceitual resultou que a falta de transparência é um sintoma externo, que até funciona como catalisador da corrupção. De qualquer forma, a corrupção é entendida, por essência, como sendo um desvio de finalidade. Portanto, a corrupção mostrou-se uma inversão de valores que poderá atingir um patamar de ser institucionalmente aceita. Quando a sociedade chega a tolerar práticas corruptas, ela passa a ser refém desse desvio pelo agente público.

Diante desta celeuma, as soluções centradas nesta tecnologia *blockchain* oferecem particularidades possíveis na busca por aperfeiçoar a Administração Pública, seja na promoção de transparência, responsabilidade, democratização da informação e, principalmente, diminuição da probabilidade de alteração indevida dos dados governamentais que na cadeia de blocos sejam registrados.

Feita as devidas ressalvas - que a *blockchain* não deve ser acreditada como uma fórmula pronta a ser aplicada por todo órgão público - outrossim sua adoção deve ser posterior a uma análise de risco feita pelo administrador público. O desafio de implementação desta tecnologia reside também na mudança de paradigma estrutural: a Administração Pública funciona consoante o método do livro-razão das partidas dobradas e cada registro vai ser centralizado em uma dessas instituições ou órgãos. A prometida ruptura (anunciada desde o segundo capítulo) tem um alvo certo, retirar o monopólio da confiança e verdade de intermediários, contudo a um custo de mudar a estruturação registral e contábil estatal, com a finalidade de proteger o Erário público de atos corruptos que desviem a finalidade basilar do interesse público.

Se a mudança para *blockchain* pode representar um ônus - desde custos de pesquisa, análise de impacto e implementação - o presente trabalho trouxe o contraponto de que significativa parte do maquinário público é incumbido da tarefa de, onerando o Erário público, exercer a função de intermediário de confiança no registro de dados e transações. Se a *blockchain* afasta a necessidade de certos órgãos públicos serem intermediários com função de registrar livros de forma centralizada e certificar registros consoante o sistema das partidas dobradas, a redução de custos estruturais possui uma boa perspectiva neste contexto.

Ante todo o exposto, precisou-se passar pelos diversos princípios que regem a Administração Pública para o caso em que um protótipo que utilize a *blockchain* seja adotado pelo Estado. E um desses princípios foi a Legalidade que rege e vincula o poder estatal, cujo entendimento demonstrou que iniciativas utilizadoras da *blockchain* pela Administração Pública devem ser viabilizadas através de lei. A inteligência deste princípio elucidou um dos questionamentos prévios relativos a saber quando ocorre o tratamento de dados pessoais através da *blockchain*: se uma lei obrigar um órgão público a registrar dados num sistema *blockchain*, a base legal para tal tratamento será o artigo 6, n.º 1, c) do RGPD, o qual fundamenta o tratamento de dados para fins de cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito.

Restou conceituado que a corrupção seria o uso da máquina estatal para fins diversos dos que juridicamente são esperados, configurando uma forma de desvio administrativo. Em outras palavras, os

atos de corrupção (por defeito e no contexto da Administração Pública) significam alterar mandamentos legais vocacionados à prossecução do interesse público para fins diversos ou até particulares, podendo ou não provocar vantagens ilícitas por parte de quem os prática.

E a partir disto, superadas questões conceituais, foram trazidos casos autênticos de implementação da *blockchain* como paradigmas práticos de projetos a nível nacional que visam combater a corrupção.

Primeiramente, o caso do Peru que se viu em uma crise institucional por escândalos de desvios de recurso público através de licitações. Diante disto, o governo peruano encontrou na *blockchain* a tecnologia capaz de desenvolver um sistema de compras públicas que ofereça rastreabilidade desde a conceção, para que os gastos públicos sejam facilmente auditáveis e sem possibilidade de adulteração. Se as licitações públicas são historicamente um procedimento utilizado para "legalizar" práticas corruptas, a agência governamental "Peru Compras", na incumbência de regular todas as compras eletrônicas do país, desenvolveu a *LAC-Chain*, uma *blockchain* permissionada que conseguiu corresponder às expectativas de segurança e transparência, gerando no país um sentimento de estímulo para adoção da *blockchain* por outros órgãos públicos.

Outro caso concreto apresentado, a fim de corroborar o que foi desenvolvido, foi a BlockchainHACKMX desenvolvida no México. Em resumo, o Governo mexicano preocupou-se em combater a corrupção através dos *smart contracts* que utilizam *blockchain*, à luz de estudos que apresentaram um potencial de serem programadas auditorias e medidas de segurança nestes programas autoexecutáveis. Esta característica dos *smart contracts* foi considerada uma mais-valia na limitação do comprometimento de fraude e prática de corrupção. O estudo da instituição *Transparency International* foi mencionado para elucidar a noção de que se um *smart contract* contiver um código escrito de maneira apropriada, poderá limitar a prática da corrupção e, conforme estabelecido pelo Governo Mexicano, a confiança e segurança da informação pública restariam asseguradas neste contexto da iniciativa BlockchainHACKMX.

Um dos detalhes que mereceu destaque desta iniciativa foi a estrutura regulatória do sistema. O arrojo da *blockchain* mexicana reside na ausência de hierarquia, corroborando a descentralização do poder estatal, uma vez que os participantes estão organizados em conselhos, respectivamente representando cada um dos 3 setores: o setor público, privado, acadêmico/organização da sociedade civil (OSC).

Ainda que ocorra no seio de uma descentralização, o BlockchainHACKMX foi proveniente de um protótipo da Presidência da República Mexicana, o que demonstra a natureza nacional e

estratégica da iniciativa. E ainda sobre a governança, optou-se por utilizar uma plataforma de código aberto já comumente utilizada, nomeadamente a *Ethereum* (dentre várias outras opções analisadas). Foi feita uma expressa ressalva de que deveria haver a criação de uma rede *blockchain* permissionada desvinculada das demais redes da *Ethereum*.

Ou seja, os *nodes* que integrarem a BlockchainHACKMX não estarão conectados à rede principal da *Ethereum*, mas sim registrados em uma rede reservada e separada. Esta adoção corrobora um entendimento trazido anteriormente que, à luz dos princípios e direitos inerentes às dinâmicas de Proteção de dados pessoais, é mais aconselhável a adoção de uma *blockchain* permissionada pela Administração Pública, o que aconteceu neste caso mexicano, ao invés do protocolo público não permissionado.

Ante todo o exposto, a BlockchainHACKMX quebrou paradigmas e criou uma rede de combate à corrupção baseada em uma *blockchain* permissionada, a fim de utilizar a tecnologia disponibilizada pela *Ethereum* apenas para estruturar uma rede à parte - sob o propósito de executar transações e registros estatais de forma automática, através dos *smart contracts*.

E, por fim, seguindo a ideia de descentralização trazida pela BlockchainHACKMX, discorreu-se um exemplar em estágio mais avançado, qual seja a KSI *blockchain* e sua importância não apenas na prestação de serviços públicos, mas no escopo ora almejado que é o combate à corrupção. Mostrou-se um paradigma frutífero, pois envolve os temas do presente estudo, qual seja uso da *blockchain* para gerar transparência administrativa e limitar a corrupção, aliado ao contexto da Proteção de Dados, uma vez que a Estônia é Estado-Membro da União Europeia, e portanto sujeita ao âmbito de aplicação do RGPD e da proteção jusfundamental, principiológica e jurisprudencial de dados pessoais.

A interconexão entre os assuntos é latente ao se concluir que a KSI *blockchain* demonstrou oferecer uma adequada atenção ao princípio da responsabilização, o que representa uma utilização da *blockchain* que, ao mesmo tempo concede aos cidadãos estonianos um maior controle sobre seus dados pessoais[442], mas também representa um obstáculo para práticas corruptas. A doutrina majoritária considerou, neste caso em concreto, que a retirada de uma entidade centralizadora torna o *node* utilizado pelo cidadão em um registro vivo da inteira cadeia de blocos - tornando o mesmo cidadão um ponto ativo de fiscalização.

Além do mais, a KSI estoniana demonstrou ser desenvolvida a ponto de ser escalável, interoperável e facilmente controlada e integrada aos demais sistemas da Administração Pública já

[442] Observando diversos princípios do RGPD, nomeadamente transparência e a proteção de dados desde a conceção e por defeito do artigo 25

existentes. E, por tudo isto, sistemas baseados na *blockchain*, com diferentes abordagens e estruturas vêm sendo a aposta de muitos Estados para o desenvolvimento de uma gestão administrativa mais transparente, facilmente auditável e com menos chances de corrupção.

Otimismo à parte, ressalta-se a importância da análise de risco para evitar implementações inadequadas da *blockchain,* sendo recomendado o uso precedente do instrumento previsto no artigo 35 do RGPD, qual seja a avaliação de impacto, dentre outros mecanismos adequados.

A corrupção é um fenômeno antigo que ainda não parece congregar uma solução absoluta, embora a *blockchain* possa – aliada a outros institutos – oferecer uma solução para que desvios de finalidade na Administração Pública sejam devidamente conhecidos por um sistema que respeite, sobretudo, dois princípios fundamentais elucidados ao longo deste trabalho: a Proteção de dados pessoais e a prossecução da necessária transparência administrativa.

REFERÊNCIAS BIBLIOGRÁFICAS

Bauman, Zygmunt. “Modernidade líquida”. Rio de Janeiro: Jorge Zahar, 2001.

Bell, Daniel. “O advento da sociedade pós-industrial: uma tentativa de previsão social”. São Paulo: Cultrix, 1977.

Camisão, Isabel; Abreu, Joana, et al. “Enciclopédia da União Europeia”. Coimbra: Editora Petrony. 2017.

Canotilho, José Joaquim Gomes et al. “Constituição da República Portuguesa Anotada”, vol. 1, n. 4, Coimbra: Editora Coimbra, 2007.

Di Pietro, Maria Sylvia Zanella. "Direito administrativo". São Paulo: Atlas, vol. 11, 1999.

Di Pietro, Maria Sylvia Zanella. “Da constitucionalização do direito administrativo: reflexos sobre o princípio da legalidade e a discricionariedade administrativa. Supremacia do interesse público e outros temas relevantes de Direito Administrativo”. São Paulo: Editora Atlas, 2010.

Di Pietro, Maria Sylvia Zanella. “Direito administrativo”. São Paulo: Atlas, vol. 8, 2010.

Di Pietro, Maria Sylvia Zanella; Ribeiro, Carlos Vinícius Alves. "Supremacia do interesse público e outros temas relevantes do direito administrativo". São Paulo: Atlas, 2010.

Dotti, René Ariel.” Proteção da vida privada e liberdade de informação: possibilidade e limites”. São Paulo: Revistas dos Tribunais, 1980.

García-Pelayo, Manuel. “Las transformaciones del Estado contemporâneo”. Madrid: Alianza, vol. 3, 1982.

Heidenheimer, A. J. “Political corruption - readings in comparative analysis”. Nova York: Holt, Rinehart and Winston, 1970.

Heller, Nathan. "Estonia, the digital republic". Nova York: The New Yorker, v. 18, 2017.

Johnston, Michael. “Political corruption and public policy in America”. Monterey: Brooks/Cole Publishing Company, 1982.

Kossow, Niklas; Victoria Dykes. “Blockchain, bitcoin and corruption, A review of the linkages”. Berlin: Transparency International Anti-Corruption, 2018.

Lopes Porto, Manuel e Gonçalo Anástácio. "Tratado de Lisboa, Anotado e Comentado" Coimbra: Almedina, 2012.

Lopes, J. de Seabra. “Direito dos Registos e do Notariado”. Coimbra: Almedina, vol. 2, 2003.

Mañas, José Luis Piñar. Transparencia y protección de datos: las claves de un equilibrio necesario. In: “Derecho administrativo de la información y administración transparente”. Madri: Marcial Pons, 2010.

Meirelles, Hely Lopes. “Direito Administrativo Brasileiro”. São Paulo: Editora Malheiros, vol. 30, 2005.

Motta, Fabricio. “Função normativa da administração pública”. São Paulo: Editora Fórum, 2007.

Nagel, Thomas. “The Shredding of Public Privacy”. Londres: Times Literary Supplement, 1998.

Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system”. Manubot, 2019.

Negrão, Ricardo. “Direito Empresarial-Estudo Unificado”. São Paulo: Saraiva Educação SA, 2008

Nelson, Deborah. “Pursuing Privacy in Cold War America xii-xiii”. Nova York: Columbia University Press, 2002.

Pacioli, Luca et al. Summa de Arithmetica geometria proportioni: et proportionalita. Tokyo: Yushodo Co, 1989.

Parks, Tim et al. “Medici money: banking, metaphysics, and art in fifteenth-century Florence”. Nova York: WW Norton & Company, 2005.

Pérez Luno, Antonio-Enrique. “¡Ciberciudadanía@ o Ciudadanía@.com?” Barcelona: Editorial Gedisa, 2004.

Piñar Mañas, José Luis (Coord.). “Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidade”. Madrid: Editorial Reus, 2016

Pinheiro, José Alexandre Guimarães de Sousa. “A vida na sociedade de vigilância: privacidade hoje”. Rio de Janeiro: Renovar, 2008.

Pinheiro, José Alexandre Guimarães de Sousa. “Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional”. Lisboa: AAFDL, 2015.

Posner, Richard A. “The economics of justice”, Cambridge Massachusetts: Harvard University Press, vol. 5, 1983.

Posner, Richard A. “The economics of justice”, Cambridge Massachusetts: Harvard University Press, v. 5, 1983.

Ramsay, G. D.; John Isham Mercer. “Merchant Adventurer: Two Account Books of a London Merchant in the Reign of Elizabeth I”. Durham: Northamptonshire Record Society. 1962. p. 53

Romanini, Anderson Vinicius; Márcia Pinheiro Ohlson. "De elos bem fechados: o pragmatismo e a semiótica peirceana como fundamentos para a tecnologia blockchain utilizada no combate às fake news." São Paulo: Communicare, 2018.

Ruaro, Regina Linden. “A tensão entre o Direito Fundamental à proteção de dados pessoais e o livre mercado”. Brasília: Repats, v. 4, 2017.

Schwab, K. “A quarta revolução industrial”. São Paulo: Edipro, vol. 1, 2016.

Silveira, Alessandra e Mariana Canotilho (Coord.). “Carta dos Direitos Fundamentais da União Europeia Comentada”. Coimbra: Almedina, 2013.

Silveira, Alessandra. “Princípios de direito da União Europeia: doutrina e jurisprudência”. Coimbra: Quid Juris, 2011.

Solove, Daniel J. “Understanding privacy”, Massachusetts: Harvard University Press, 2010.

Sousa, Domingos Pereira de. “Direito da União Europeia”. Coimbra: Quid Juris, 2018.

Swan, Melanie. “Blockchain: blueprint for a new economy” Sebastopol: O’reilly, vol. 1, 2015.

Vasconcelos, Álvaro de et al. “Portugal no centro da Europa”. Lisboa: Quetal Editores, 1995.

Vilaça, José Luís da Cruz et al. “The internal market and the digital economy”. Vol. 1, Lisboa: Almedina, 2018

Voigt, Paul; Von Dem Bussche, Axel. “The EU general data protection regulation (GDPR). A Practical Guide”. Cham: Springer International Publishing, vol. 1, 2017.

West, Darrell M. “Digital government: Technology and public sector performance”. Nova Jersey: Princeton University Press, 2005.

William J. Stuntz, “Privacy’s Problem and the Law of Criminal Procedure,” Michigan: 93 Michigan Law Review, 1995.

Trabalhos Acadêmicos

Aarvik, Per. “Blockchain as an anti-corruption tool (Case examples and introduction to the technology)”. Bergen, Noruega: U4 Issue, 2020.

Abreu, Joana Covelo; Silveira, Alessandra. “Interoperability solutions under Digital Single Market: European e-Justice rethought under e-Governance paradigm”. European Journal of Law and Technology, v. 9, n. 1, 2018.

Abreu, Joana Rita Covêlo de. “Digital Single Market as the new world to the European Union: repercussions in social and institutional regulatory structure–the universal service and the Body of European Regulators for Electronic Communications’(BEREC) redefinition”. UNIO–EU Law Journal, v. 4, n. 2, 2018

Aho, James A. “Rhetoric and the invention of double entry bookkeeping”. Rhetorica: A journal of the History of Rhetoric, v. 3, n. 1, 1985

Ávila, Humberto. "Repensando o princípio da supremacia do interesse público sobre o particular." Revista trimestral de direito público, vol. 24, 1999.

Baliga, Arati. "Understanding blockchain consensus models." Persistent, vol. 4, 2017.

Balinha, Hélio, et al. "O RGPD: a articulação entre a gestão de informação e a gestão de segurança da informação." Actas do Congresso Nacional de Bibliotecários, Arquivistas e Documentalistas. n. 13, 2018

Basu, Dr Paritosh. "Emerging Dimensions of Blockchain Technology." AIMA Journal of Management Research, n. 3, 2018.

Böhme, Reiner and Paulina Pesch. “Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie”. Datenschutz und Datensicherheit (DuD). 2017

Brei, Zani Andrade. “Corrupção: dificuldades para definição e para um consenso”. Revista de Administração Pública, vol. 30, n. 1, 1996.

Brown, Richard Gendal; James Carlyle; Ian Grigg; Mike Hearn. “Corda: An introduction”. R3 CEV, 2016.

Buterin, Vitalik et al. “A next-generation smart contract and decentralized application platform”. Ethereum White paper, v. 3, n. 37, 2014.

Camilo, Juan. “Blockchain-based consent manager for GDPR compliance”. Open Identity Summit 2019, 2019.

Cardoso, Bruno Campos. "Algoritmos como ‘máquinas de cultura’: Notas sobre política e produção de consenso no sistema peer-to-peer Bitcoin." Anais da ReACT-Reunião de Antropologia da Ciência e Tecnologia, vol. 4, n. 4, 2019.

Carqueja, Hernâni O. "O livro de ‘m. Barrême (1721)’, em francês, e os dois primeiros livros em português sobre partidas dobradas." Revista Portuguesa de Contabilidade, v. 3, 2011.

Carruthers, Bruce G.; Espeland, Wendy Nelson. “Accounting for rationality: Double-entry bookkeeping and the rhetoric of economic rationality”. American journal of sociology, v. 97, n. 1, 1991.

Castro, Catarina Sarmento. “40 anos de ‘Utilização da Informática’: O artigo 35. º da Constituição da República Portuguesa”. e-Pública: Revista Eletrónica de Direito Público, vol. 3, n. 3, 2016.

Chicarino, V. R., et al. Ibid. "Uso de blockchain para privacidade e segurança em internet das coisas." VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Brasília: SBC, vol. 28, 2017.

Christidis, Konstantinos; Devetsikiotis, Michael. “Blockchains and smart contracts for the internet of things”. Ieee Access, v. 4, 2016

Cortizo, Lucas. Cap. “Blockchain e e-Government (paradigmas e perspectivas)” in: Silveira, Alessandra, Joana Rita Sousa Covelo Abreu, and Larissa Coelho. "UNIO Ebook Interop 2019: O Mercado Único Digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir", Braga: Universidade do Minho, 2019

Crescenzo, G. Di; J. Katz; R. Ostrovsky; A. Smith. “Efficient and non-interactive non-malleable commitment”. International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2001.

Crosby, Michael et al. “Blockchain technology: Beyond bitcoin”. Applied Innovation, v. 2, n. 6/10, 2016.

Datta, Anwitaman. "Blockchain in the government technology fabric". Singapura: School of Computer Science and Engineering, NTU. arXiv. 2019.

Dos Santos Gonçalves, Luiz Carlos. "El Ministerio Público Brasileño y el combate a la corrupción." Revista de la Facultad de Derecho de México, vol. 68, n. 272-1, 2018.

Doukas, Charalampos, et al. "Enabling data protection through PKI encryption in IoT m-Health devices." 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE). IEEE, 2012

Duranti, Luciana; Rogers, Corinne. “Trust in digital records: An increasingly cloudy legal area”. Computer Law & Security Review, v. 28, n. 5, 2012

Eberhardt, Jacob; Stefan Tai. "Zokrates-scalable privacy-preserving off-chain computations." 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018

Ferreira, Rafael Freire. “Desafios em sede de tutela da personalidade: a autodeterminação informativa e a privacidade na sociedade da informação”. Lisboa: Universidade Autónoma de Lisboa, Tese de Doutorado, 2016.

Fischlin, M.; R. Fischlin. “Efficient non-malleable commitment schemes”. Annual International Cryptology Conference, Springer, 2000.

Friedrich, C. J. “Political corruption”. Political Quarterly, vol. 37, n. 1, 1966.

Gellert, Raphael. "Understanding the notion of risk in the General Data Protection Regulation." Computer Law & Security Review, vol. 34, n. 2, 2018.

Goldreich, O.; S. Micali; A. Wigderson. “Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems”. Journal of the ACM (JACM), vol. 38, n. 3, 1991.

Goldreich, Oded; Hugo Krawczyk. “On the Composition of Zero-Knowledge Proof Systems” SIAM Journal on Computing, vol. 25, n. 1, 1996.

Gonçalves, Pedro Vilela Resende; Rafael Coutinho Camargos. "Blockchain, Smart Contracts e “Judge as a Service” no Direito Brasileiro". II Seminário Governança das Redes e o Marco Civil da Internet: globalização, tecnologias e conectividade. Belo Horizonte: Instituto de Referência em Internet e Sociedade-IRIS, 2017.

Greve, Fabíola et al. "Blockchain e a Revolução do Consenso sob Demanda". Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), 2018.

Grigg, Ian. “Triple entry accounting”. Systemics Inc, 2005.

Hoetjes, B. “Administrative corruption in the Netherlands: recent cases and recent developments. Corruption and Reform”. Países Baixos, vol. 1, n. 2, 1986.

Jiménez, María Nieves Pacheco. "Criptodivisas: del bitcoin al MUFG. El potencial de la tecnología blockchain." Revista Cesco de derecho de consumo, vol. 19, n. 7, 2016.

Johnson, D.; Menezes, A.; Vanstone, S. “The elliptic curve digital signature algorithm (ECDSA)”, International Journal of Information Security, vol. 1, n. 1, 2001.

Jordan A. & Sowerby M. “Preparing for the General Data Protection Regulation – Digest”, Information Security Forum Limited. 2016.

Kaufmann, D.; Siegelbaum, P. “Privatization and corruption in transition economies”. Journal of International Affairs, Vol. 50, n. 2, 1997.

Kiayias, Aggelos, et al. "Ouroboros: A provably secure proof-of-stake blockchain protocol." Annual International Cryptology Conference. Springer, Cham, 2017.

Kivimäki, Petteri. "There is no blockchain technology in the X-Road." Noruega: Nordic Institute for Interoperability Solutions, 2018.

Kuner, Christopher. Et al. “Blockchain versus data protection”. International Data Privacy Law, vol. 8, n. 2. 2018.

Lamport, L.; Shostak, R; Pease, M. “The byzantine generals problem” ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, n. 3, 1982.

Lazzarini, Álvaro. “Abuso de poder x poder de polícia”. Revista de Direito Administrativo, v. 20, n. 3, 1996.

Li, Munan; Porter, Alan L.; Suominen, Arho. “Insights into relationships between disruptive technology/innovation and emerging technology: A bibliometric perspective”. Technological Forecasting and Social Change, v. 129, 2018.

Li, Wenting, et al. "Securing proof-of-stake blockchain protocols." Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, Cham, 2017.

Li, Yang, et al. "EtherQL: a query layer for blockchain system." International Conference on Database Systems for Advanced Applications. Springer, Cham, 2017.

Limberger, Têmis. "Transparência administrativa e novas tecnologias: o dever de publicidade, o direito a ser informado e o princípio democrático." Revista de Direito Administrativo, n. 244, 2007.

Mackenzie, Donald. “Pick a nonce and try a hash”. London Review of Books, v. 41, n. 8, 2019.

Mañas, José Luis Piñar. I. “Introducción. Hacia Un Nuevo Modelo Europeo De Protección De Datos”. Revista del Consejo General de la Abogacía, n. 98, 2016.

Martin-Bariteau, Florian. "Blockchain and the European Union General Data Protection Regulation: The CNIL's Perspective." Blckchn. ca Working Paper, vol. 1, 2018.

Martini, Mario; Quirin Weinzierl. “Die Blockchain-Technologie und das Recht auf Vergessenwerden”. Neue Zeitschrift für Verwaltungsrecht, NVwZ, 2017.

Matzutt, Roman et al. “A quantitative analysis of the impact of arbitrary blockchain content on bitcoin”. International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2018.

Meng, Weizhi, et al. "When intrusion detection meets blockchain technology: a review." Ieee Access 6, 2018.

Merkle, R. C. “A digital signature based on a conventional encryption function”. Berlin: Springer, Heidelberg Proceedings of Advances in Cryptology, CRYPTO 1987, vol. 293, 1988.

Miers, I.; Garman, C.; Green, M; Rubin, A.D. “Zerocoin: Anonymous distributed e-cash from bitcoin” Proceedings of IEEE Symposium Security and Privacy (SP), Berkeley, EUA, 2013.

Modesto, Paulo. "Nepotismo em cargos político-administrativos". Revista Brasileira de Direito Público, vol. 11, 2012.

Moerel, Lokke. “Why blockchain is not inherently at odds with GDPR. Blockchain & Data Protection and Why They Are Not on a Collision Course”. European Review of Private Law 6-2019, Kluwer Law International BV, Países Baixos, 2019.

Momo, F. S.; Schiavi, G. S.; Behr, A.; Lucena, P. “Business models and blockchain: What can change?” Revista de Administração Contemporânea, vol. 23, n. 2, 2019.

Moraes, Juliana Moreira. Blockchain e o compartilhamento de dados na esfera da administração pública federal brasileira: análise do bCPF. Universidade de Brasília. 2019.

Morais, Janaina Jacolina. “Princípio da eficiência na Administração Pública”. Ethos Jus: revista acadêmica de ciências jurídicas. Avaré: Faculdade Eduvale de Avaré, v. 3, n. 1, 2009.

Moura, Luzia Menegotto; Frick de, Daniela; Francisco Brauner; Raquel Janissek-Muniz. "Blockchain e a Perspectiva Tecnológica para a Administração Pública: Uma Revisão Sistemática." Revista de Administração Contemporânea, vol. 24, n. 3, 2020.

Müller, Michael F. "Amazon and Data Protection Law–The End of the Private/Public Divide in EU conflict of laws?." Journal of European Consumer and Market Law 5.5, 2016.

Mylrea, Michael; Sri Nikhil Gupta Gourisetti. "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security." 2017 Resilience Week (RWS), IEEE, 2017.

Nascimento, S.; Pólvora A. (coord.) et al. “Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies”. EUR 29813 EN, Publicações oficiais da União Europeia, Luxemburgo, 2019.

Nesser, Petter; Stenersen, Anne; Oftedal, Emilie. “Jihadi terrorism in Europe: The IS-effect. Perspectives on Terrorism”. vol. 10, n. 6, 2016.

Neto, Orion Augusto Platt, et al. "Publicidade e transparência das contas públicas: obrigatoriedade e abrangência desses princípios na administração pública brasileira." Contabilidade Vista & Revista, vol. 18, n. 1, 2007.

Nguessan, Desire; Jose Sidnei Colombo Martini. "Framework for security and privacy Management for Mobile Middleware Based on tuple.". IEEE Latin America Transactions, vol. 13, n.8, 2015.

Nguyen, Giang-Truong; Kyungbaek Kim. "A Survey about Consensus Algorithms Used in Blockchain”. Journal of Information processing systems vol. 14, n. 1, 2018.

Oliveira, Robson Ramos. "Contabilidade, controle interno e controle externo: trinômio necessário para combater a corrupção." Rio de Janeiro: Pensar Contábil, vol. 8, n. 31, 2008.

Oliveira, Vânia Aparecida Rezende de; José Roberto Pereira. "Interesse público: significados e conexões". Cadernos Gestão Social, vol. 4, n. 1, 2013.

Peters, Gareth W.; Efstathios Panayi. "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money." Banking beyond banks and money. Springer, Cham, 2016.

Priollaud, François-Xavier, and David Siritzky. Le traité de Lisbonne: Commentaire, article par article, des nouveaux traités européens (TUE et TFUE). La documentation française, 2008.

Quelle, Claudia. "Enhancing compliance under the general data protection regulation: The risky upshot of the accountability-and risk-based approach." European Journal of Risk Regulation vol. 9, n. 3, 2018.

Quisquater, Jean-Jacques; Louis C. Guillou; Thomas A. Berson. "How to Explain Zero-Knowledge Protocols to Your Children". Advances in Cryptology - CRYPTO '89: Proceedings, n.435, 1990.

Ramos, Luis Felipe M.; Silva, João Marco C. "Privacy and Data Protection Concerns Regarding the Use of Blockchains in Smart Cities". Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV2019), Melbourne, VIC, Australia, 2019.

Rieger, Craig G.; David I. Gertman; Miles A. McQueen. "Resilient control systems: Next generation design research." 2009 2nd Conference on Human System Interactions. IEEE, 2009.

Rodrigues, João Gaspar. "Nepotismo no serviço público brasileiro e a SV 13". Revista de Direito Administrativo, n. 260, 2012.

Romanini, Anderson Vinicius; Márcia Pinheiro Ohlson. "De elos bem fechados: o pragmatismo e a semiótica peirceana como fundamentos para a tecnologia blockchain utilizada no combate às fake news." São Paulo: Communicare, 2018.

Ruaro, Regina Linden; Machado, Fernando Inglez de Souza. Ensaio a propósito do direito ao esquecimento: limites, origem e pertinência no ordenamento jurídico brasileiro. Revista do Direito Público, Londrina, vol. 12, n. 1, 2017.

Sala, Jorge Francisco Aguirre. "Los límites de la representatividad política y las alternativas de la democracia líquida." Revista Internacional de Pensamiento Político, vol. 10, 2015.

Saleh, Fahad. "Blockchain without waste: Proof-of-stake". SSRN 3183935, 2020.

Salom, Javier Aparicio; Sergio Sanfulgencio Tomé. "El régimen jurídico de las cookies y su aplicación por la agencia española de protección de datos." Revista Aranzadi Doctrinal, vol. 11, 2014.

Sangster, Alan. "The genesis of double entry bookkeeping". The Accounting Review, v. 91, n. 1, 2016.

Sasson, E.B.; Chiesa, A.; Garman, C. et al. "Zerocash: Decentralized anonymous payments from Bitcoin". Proceedings of 2014 IEEE Symposium on Security and Privacy (SP), San Jose, EUA, 2014.

Sigler, Laurence. "Fibonacci's Liber Abaci: a translation into modern English of Leonardo Pisano's book of calculation". Springer Science & Business Media, 2003.

Silveira, Alessandra e Froufe, Pedro. "Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos. UNIO - EU Law Journal". Vol. 4, No. 2, 2018.

Silveira, Alessandra; Marques, João. Do Direito a Estar só ao Direito ao Esquecimento. Considerações Sobre a Proteção de Dados Pessoais Informatizados no Direito da União Europeia: Sentido, Evolução E Reforma Legislativa. Revista da Faculdade de Direito – UFPR, Curitiba, vol. 61, n. 3, 2016.

Silveira, Alexandre Marques Albano da. "Prova de conhecimento nulo baseada em isomorfismo de subgrafos". Universidade Federal do Ceará. 2015.

Smyrnaios, Nikos. "Internet oligopoly: The corporate takeover of our digital world". Emerald Group Publishing, 2018.

Stelzer, Joana. "União Européia e Supranacionalidade: Desafio ou Realidade?". Curitiba: Juruá, 2000.

Szabo, Nick. "Smart contracts: building blocks for digital markets". Extropy: The Journal of Transhumanist Thought, v. 18, n. 6, 1996.

Szalachowski, Pawel. "Towards More Reliable Bitcoin Timestamps". 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018.

Thompson, Paul B. "Privacy, secrecy and security", Ethics and Information Technology 3.1, 2001.

Thornton, Ann-Marie. "Hammurabi, Babylonian law". Topic 1, Secondary Source, 2017.

Vaquero, Juan Pablo Aparicio. "La protección de datos que viene: el nuevo Reglamento General europeo." AIS: Ars Iuris Salmanticensis, vol. 4, n. 2, 2016.

Vieira, F. M.; Santos, V. V. B. "Governo eletrônico: A busca por um governo mais transparente e democrático". Brasília-DF: Congresso Consad de Gestão Pública, 2010.

Warso, Zuzanna. "There's more to it than data protection–Fundamental rights, privacy and the personal/household exemption in the digital age". Computer Law & Security Review, vol. 29, n. 5, 2013.

Wirth, Christian; Michael Kolain. "Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data". 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET), 2018.

Wright, Aaron; De Filippi, Primavera, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 2015 in Taufick, Roberto Domingos. "Mercado de Loterias no Brasil: concorrência, governança e responsabilidade social na era de blockchain". Brasília: Escola Nacional de Administração Pública, Diss., 2019

Wüst, Karl; Arthur Gervais. "Do you need a blockchain?." 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018

Xu, Lei, et al. "Enabling the sharing economy: Privacy respecting contract based on public blockchain." Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, 2017.

Yermack, D. "Corporate governance and blockchains". Review of Finance, vol. 21, n.1, 2017.

Zheng, Zibin et al. "An overview of blockchain technology: Architecture, consensus, and future trends". IEEE international congress on big data (BigData congress), IEEE, 2017.

Zheng, Zibin et al. “Blockchain challenges and opportunities: A survey”. International Journal of Web and Grid Services, v. 14, n. 4, 2018.

Zuiderveen Borgesius, F. “Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation” Computer Law & Security Review, vol. 32, 2016.

Legislação e documentos oficiais

BRASIL. Lei Complementar, n. 101, 4 maio 2000. LRF – Lei de Responsabilidade Fiscal, Brasília. 2000.

BRASIL. Lei nº 8.429, de 2 de junho de 1992. Dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências. 1992.

BRASIL, Ministério do Meio Ambiente. “A grilagem de terras públicas na Amazônia brasileira”. Instituto De Pesquisa Ambiental Da Amazônia, 2006.

ESPANHA. González Barroso, Fernando. "Gobernabilidad y Gobernanza. Las relaciones intergubernamentales: concepto y marco teórico. El contexto y el concepto." Espanha: Administración de la Junta de Comunidades de Castilla-La Mancha, 2009.

PORTUGAL. CNPD – Comissão Nacional de Proteção de Dados. Decisões. Disponível em: < https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_495.pdf.

PORTUGAL. Lei n. 58/2019, de 8 de agosto de 2019, a qual assegura a execução do RGPD na ordem jurídica nacional, Disponível em: <https://dre.pt/web/guest/pesquisa/>.

PORTUGAL. Lei n° 26, de 22 de agosto de 2016. Disponível em: <www.dre.pt/pesquisa>.

UNIÃO EUROPEIA. "Carta dos Direitos Fundamentais da União Europeia (2010/c 83/02)". Diário oficial da União Europeia 30 (2010). Disponível em https://www.europarl.europa.eu/charter/pdf/text_pt.pdf

UNIÃO EUROPEIA. “Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679”. Grupo de trabalho do artigo 29.º para a proteção de dados, 2017.

UNIÃO EUROPEIA. “Tratado da União Europeia e do Tratado sobre o Funcionamento da União Europeia” 2012/C. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:12012E/TXT&from=ES

UNIÃO EUROPEIA. Acórdão do TJUE, Bara, de 1 de outubro de 2015, processo C-201/14.

UNIÃO EUROPEIA. Acórdão TJEU, Lindqvist, de 6 de Novembro de 2003, processo C-101/01.

UNIÃO EUROPEIA. Acórdão TJEU, Satamedia, de 16 de dezembro de 2008, processo n.º C-73/07.

UNIÃO EUROPEIA. Acórdão TJEU, Weltimmo v NAIH, de 1 de Outubro de 2015, processo C-230/14.

UNIÃO EUROPEIA. Acórdão TJUE, Peter Nowak, de 20 de dezembro de 2017, processo C-434/16.

UNIÃO EUROPEIA. Acórdão TJUE, Rynes, de 11 de dezembro de 2014, processo n.° C-212/13.

UNIÃO EUROPEIA. Allessie, D.; Sobolewski, M.; Vaccari, L.; Pignatelli, F. "Blockchain for digital government". Luxemburgo: Publicação oficial da União Europeia, 2019.

UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (privacidade e às comunicações eletrónicas"), 2002.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, 1995.

UNIÃO EUROPEIA. Fink, Michèle. "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law?" Estudo do Parlamento Europeu, 2019.

UNIÃO EUROPEIA. Flash Eurobarometer 482. "Businesses' attitudes towards corruption in the EU". Directorate-General for migration and home affairs. Comissão Europeia, 2019.

UNIÃO EUROPEIA. Houben, R.; Snyers, A. "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion". Estudo do Parlamento Europeu, 2018

UNIÃO EUROPEIA. Regulamento (Ue) 2016/679 Do Parlamento Europeu E Do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), 2016

Outros documentos - Links pesquisados

A Estônia é o primeiro país a oferecer a e-Residency. Disponível em https://e-resident.gov.ee/

Bloomberg. Lehman Brothers resurrected? Well almost. Disponível em https://economictimes.indiatimes.com/lehman-brothers-resurrected-well-almost/articleshow/6562620.cms?from=mdr

Commission Nationale de l'Informatique et des Libertés (CNIL). Solutions for a responsible use of the blockchain in the context of personal data. Disponível em https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

Formigoni Filho, J. R., Braga, A. M., Leal, R. L. V. (2017). Tecnologia blockchain: Uma visão geral. Disponível em https://www.cpqd.com.br/wp-content/uploads/2017/03/cpqd-whitepaper-blockchain-impresso.pdf

Gallas, Daniel. "Brazil's Odebrecht corruption scandal explained". Disponível em https://www.bbc.com/news/business-39194395

GAN Integrity. Estonia Corruption Report. Disponível em https://www.ganintegrity.com/portal/country-profiles/estonia/

Globo. "Corrupção no Peru: entenda denúncias envolvendo a Odebrecht e 4 ex-presidentes peruanos". Disponível em https://g1.globo.com/mundo/noticia/2019/04/17/corrupcao-no-peru-entenda-denuncias-envolvendo-odebrecht-e-4-ex-presidentes-peruanos.ghtml

Globo. "Ex-presidente peruano Alan García morre após dar tiro na cabeça". Disponível em https://g1.globo.com/mundo/noticia/2019/04/17/ex-presidente-alan-garcia-morre-diz-imprensa-local.ghtml

Gobierno de Mexico. Iniciativa BlockchainHACKMX. White Paper disponível em https://www.gob.mx/cms/uploads/attachment/file/328774/BlockchainHACKMX__Reporte_de_avances__1_.pdf

Govierno de Mexico. BlockchainHACKMX gana premio en el World Virtual GovHack. Disponível em https://www.gob.mx/cidge/es/articulos/blockchainhackmx-gana-premio-en-el-world-virtual-govhack-147504?idiom=es

Govierno de Mexico. Modelo de Gobernanza para implementar la Red Blockchain México. Comentários a consulta pública. Disponível em https://www.gob.mx/cms/uploads/attachment/file/415646/Consolidacio_n_de_Comentarios_Consulta_Pu_blica_-_Modelo_de_Gobernanza__1_.pdf

Guardtime Federal LLC. Keyless Signature Infrastructure® (KSI™) Technology. Disponível em https://www.guardtime-federal.com/guardtime-federal-background/

Information Commissioner's Office (November 2012), 'Anonymisation: managing data protection risk code of practice' Disponível em https://ico.org.uk/media/1061/anonymisation-code.pdf

Information Commissioner's Office. Anonymisation: managing data protection risk code of practice. Disponível em https://ico.org.uk/media/1061/anonymisation-code.pdf

Information Commissioner's Office. Lawful basis for processing. Disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Lanz, Jose Antonio. “Peru sets its eyes on blockchain to fight government corruption. Decrypt.co”. Disponível em https://decrypt.co/6893/peru-blockchain-government-corruption

Melo Jr, Wilson S., et al. "Uso de Redes Blockchain em aplicações de Metrologia e Avaliação da Conformidade.". Disponível em https://www.researchgate.net/profile/Wilson_Melo_Junior/publication/336071460_Uso_de_Redes_Blockchain_em_aplicacoes_de_Metrologia_e_Avaliacao_da_Conformidade/links/5d8ced5892851c33e9405bb8/Uso-de-Redes-Blockchain-em-aplicacoes-de-Metrologia-e-Avaliacao-da-Conformidade.pdf

Moerel, Lokke. Marijn Storm. Disponível em https://mofotech.mofo.com/topics/why-blockchain-is-not-inherently-at-odds.html

Mouallem, Atie J El. “Countries using blockchain for combating corruption”. Disponível em https://atiejelmouallem.com/countries-using-blockchain-for-combating-corruption/

Prosecutor, lawyers appeal Savisaar corruption ruling to Supreme Court. Disponível em https://news.err.ee/1143148/prosecutor-lawyers-appeal-savisaar-corruption-ruling-to-supreme-court

Ribitzky, Ron, et al. Pragmatic, Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology: Paving the Future for Healthcare. Disponível em https://blockchainhealthcaretoday.com/index.php/journal/article/view/24/21

Santiso, Carlos. “Can blockchain help in the fight against corruption?” World Economic Forum. Disponível em https://www.weforum.org/agenda/2018/03/will-blockchain-curb-corruption/

Schuh, F., Larimer, D.: Bitshares 2.0: General overview. Disponível em http://docs.bitshares.org/downloads/bitshares-general.pdf

Survey on Blockchain Technologies and Related Services FY2015 Report. Nomura Research Institute. 2016. Disponível em https://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf

University College London. Anonymisation and Pseudonymisation. Disponível em https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/anonymisation-and.

World Economic Forum. Partnering Against Corruption Initiative - Infraestructura and Urban Development. Building Foundations for Trust and Integrity. World Economic Forum. 2017. Disponível em http://www3.weforum.org/docs/WEF_PACI_IU_Interim_Report_2017.pdf