Os desafios do Regulamento Geral de Proteção de Dados diante da nova tecnologia blockchain

Maria Paulo Rebelo*

Resumo: A criação e o surgimento de novos *softwares* baseados em tecnologia *blockchain*, caracterizada por ser altamente decentralizada, transparente e imutável, lançam desafiantes perguntas ao novo Regulamento Geral de Proteção de Dados, criticado por ter sido criado tendo apenas em vista realidades virtuais centralizadas de controlo de dados. Sem prejuízo de quer o Regulamento europeu, quer a *blockchain* desejarem objetivos comuns, como o aumento da transparência e da confiança na troca de dados *online*, demonstraremos que, na verdade, em vários aspectos os desentendimentos entre ambos são reais. Em todo o caso, é possível adequá-la ao Regulamento: identificando a figura do responsável pelo tratamento ou subcontratante; reajustado certos direitos, como o direito ao apagamento, à realidade da *blockchain*, entre outros. O trabalho fez uso de metodologia bibliográfica e documental, de cunho dogmático-jurídico.

Palavras-chave: *blockchain; Regulamento Geral de Proteção de Dados*

Abstract: The creation and emergence of new software based on blockchain technology, characterized by their highly decentralized, transparent and immutable systems, challenge the recent General Data Protection Regulation to new questions, as it is severely criticized for bearing in mind only virtual realities based on centralized data control. Despite both the General Data Protection Regulation and blockchain share common interests in increasing transparency and confidence in online data exchange, the truth is that in several ways misunderstandings between the two are real. Nonetheless,

* Doutoranda em Direito Público pela Universidade Federal da Bahia; Investigadora Convidada pelo Max Planck Institute Luxembourg for International, European and Regulatory Procedural Law; Mestre em Direito Intelectual, Pós-Graduada em Direito do Trabalho e Licenciada em Direito pela Faculdade de Direito de Lisboa; Pós-Graduada em Direito Empresarial pela Faculdade de Direito da Universidade de Coimbra. Professora de Pós-Graduação em Direito Processual Civil na UNIFACS (Brasil). Auditora de Justiça.

adjustments are feasible to adapt it to the Regulation: it is possible to identify the data controller and processor, to readjust; certain rights, such as right to erasure, among others. This work made use of bibliographical and documentary methodology of juridical and dogmatic nature.

Keywords: *blockchain; General Data Protection Regulation*

Introdução ao problema

O presente artigo vem questionar a articulação que uma das mais badaladas tecnologias dos últimos anos enfrenta com a chegada do novo RGPD.

A tecnologia *blockchain* tem vindo a assumir grande protagonismo nos últimos anos, no contexto de técnicas de computação em rede. Tem, inclusivamente, sido referenciada como uma das principais tecnologias integrantes da quarta revolução industrial[1]. Com efeito, os utilizadores da *blockchain* operam com base na lógica *P2P* (entre si), acabando por possuir uma cópia de toda a *DLT* (tecnologia de *distributed ledgers*, i.e., de dados/ /registos distribuídos/descentralizados) no seu próprio computador.

A principal questão que aqui se coloca, então, é a de saber qual o nível de impacto que esta tecnologia tem em áreas como a da proteção de dados, tradicionalmente voltadas para uma regulação analógica; ou se existe potencial para aplicar a *blockchain* ao serviço daquela mesma proteção. Entre outras coisas, torna-se relevante perceber se a *blockchain* pode ser considerada, *ab initio,* como um *software* que realiza tratamento de dados e perceber se os dados armazenados na *blockchain* são dados pessoais. Se considerarmos que a tecnologia implica a recolha de dados pessoais e o respectivo tratamento, uma terceira questão coloca-se na identificação do *responsável pelo tratamento (data controller)* e do *subcontratante (data processor)* que atuam na cadeia de blocos. Por último, depois de percebermos quais os

[1] A título de exemplo, Aste, Tomaso, Tasca, Paolo, Matteo, T Di. "Blockchain Tecnologies: foreseeable impacto on industry and society", disponível em http://discovery.ucl.ac.uk/10043048/1/Aste_BlockchainIEEE_600W_v3.3_A.doccceptedVersion.x.pdf, (acedido a 20/01/2019) ou Xing, Bo; Marwala, Tshilidzi. "Blockchain and Artificial Intelligence", disponível em https://arxiv.org/pdf/1802.04451.pdf (acedido a 20/01/2019).

principais direitos postos em causa por esta tecnologia, é preciso enfrentar o problema de garantir que eles sejam cumpridos.

1. A emergência de novas "economias digitais": controlo de dados e blockchain

Apesar de a *internet* ter sido originalmente concebida como um fenómeno de livre interligação entre redes a nível mundial, um espaço virtual onde todos os usuários se apresentassem de forma igualitária, a verdade é que, nos dias de hoje, o ciberespaço é uma verdadeira plataforma eletrónica de transação onde os dados pessoais dos seus utilizadores se convertem num dos maiores ativos económicos do mundo *online*, transformando-se na nova "moeda" digital. A grande quantidade, complexidade e variabilidade de informações que hoje circula *online* é inclusivamente apelidada de *Big Data*[2] e tem levantado algumas inquietações, não pela sua própria existência, mas pelo uso que grandes prestadores de serviços *online* como a *Google*, *Amazon*, *Apple* e *Facebook* fazem dela. Hoje em dia, grandes empresas controlam facilmente a forma como cada um de nós pesquisa, compra e se relaciona com terceiros; tudo graças à informação gratuita que lhes passamos e eles armazenam, processam e monitorizam. Para a grande maioria das empresas que estão *online* e para os prestadores de serviços em rede, a troca de serviços e produtos aparentemente gratuitos é feita à custa da

---

[2] Não existe uma informação unívoca em torno da expressão. Como reporta Mauro, Greco e Grimaldi, podem ser identificados vários grupos de posicionamentos na forma como a ideia é concebida: (i) um que se foca nas principais características, a saber, os três V's (Volume, Velocidade e Variedade); (ii) outro que dá ênfase às necessidades tecnológicas exigidas para processar grandes quantidades de informação; (iii) e um terceiro que recorre ao impacto que este tipo de informação tem na sociedade. Por todos, Mauro, Andrea De, Greco, Marco, Grinaldi, Michele. "What is Big Data? A consensual definition and a review of key research topics", in *AIP Conference Proceedings 1644,* 97 (2015), disponível em http://big-data-fr.com/wp-content/uploads/2015/02/aip-scitation-what-is-bigdata.pdf (acedido a 20/01/2019). Uma proposta de definição que agregue todos os traços acima apontados é possível. Nestes termos, *Big Data* pode ser compreendido como uma mais valia económica, sob a forma de informação, que, pelo seu significativo volume, pela velocidade com que são processadas e pela variedade do seu teor, demandam plataformas tecnológicas adequadas ao seu processamento em valor económico (p. 103).

entrega de informação pessoal, que serve de "pagamento" para a obtenção de acessos e serviços *online*. Por ser assim, a partilha de informação e dados pessoais tornou-se algo inevitável no mundo virtual. A centralização deste tipo de informações em poucos provedores *online* tem gerado grandes preocupações[3], já que técnicas de mineração de dados tornam possível a identificação de padrões de consumo e a construção de bancos de dados sobre consumidores, não-raro sem que os cidadãos tenham disso ciência.

Paralelamente a esta "monetarização" da informação e do controlo sobre dados *online*, outra grande "moeda" digital que surgiu em 2008/2009 foi a criptomoeda conhecida como *Bitcoin*. Desenhada por Satoshi Nakamoto[4], funciona através de um sistema de protocolos que operam *P2P*, oferece um sistema financeiro de pagamento *online* sem a intervenção de uma entidade central que gerencie todas as operações. Ao operar desta forma, a *Bitcoin*, que é construída sobre a técnica da *blockchain*, chama à atenção pela transparência com que promove entre privados (*peers*) comunicações e transações. A sua arquitetura descentralizada tem sido apontada como uma das maiores valias desta tecnologia, permitindo a redistribuição do poder a todos os navegadores da comunidade digital e impedindo o processamento e armazenamento de dados em servidores centrais localizados.

As atividades desenhadas em rede entre indivíduos são, assim, efetuadas puramente com base no consenso de todos os seus intervenientes e a correspondente transparência e publicidade de toda essa informação devolve-lhes o poder sobre si mesmos e a confiança que resgatam dos servidores *online*, para depositar no funcionamento imparcial dos algoritmos matemáticos.

É neste ponto que a tecnologia *blockchain* e a regulamentação europeia revelam os seus interesses comuns: tal como aquela *DLT* promete a descentralização do tratamento de dados, garante a confiança e transparência nas redes *P2P*, a eliminação do domínio dos grandes blocos sobre dados

---

[3] Filippone, Roberta. "Blockchain and individuals' control over personal data in European data protection law", 2017, disponível em http://arno.uvt.nl/show.cgi?fid=143638 (acedido a 20/01/2019).

[4] Depois do domínio "bitcoin.org" ter sido registado online em 2008, um artigo da autoria de Satoshi Nakamoto foi publicado poucos meses depois (Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System", disponível em https://bitcoin.org/bitcoin.pdf (acedido a 20/01/2019), com as bases daquilo que seria a tecnologia *Bitcoin* e o fenómeno das criptomoedas. O nome Satoshi Nakamoto, porém, foi um pseudónimo usado para esconder a(s) sua(s) verdadeira(s) identidade(s), que permanece(m) até aos dias de hoje desconhecida(s).

pessoais dos usuários e a devolução desse controlo aos próprios, também o RGPD compartilha ideias paralelas de devolução do controlo sobre os dados aos seus titulares, para os quais consagra uma série de direitos, entre os quais o direito ao apagamento (art.º 16º e 17º do RGPD)[5].

Todavia, por mais tentador que pareça ser esta devolução de controlo aos titulares dos dados sobre as suas informações, importa não perder de vista que a *blockchain* é uma tecnologia que tem como mais-valia garantir, precisamente, a autenticidade de informações mediante a sua imutabilidade, pelo que, só por si, e enquanto desacompanhada de ferramentas (*rectius,* tecnologias *by desin*) complementares que as compatibilizem com os direitos dados pelo RGPD aos titulares, o seu uso é minimamente comprometedor[6].

2. A tecnologia *blockchain*

A tecnologia *blockchain*, tal como a terminologia sugere, é uma concatenação de "blocos", cada um deles composto por um certo número de *data* (dados), relacionados entre si de tal modo que cada novo bloco que se acrescenta à sequência contém uma imagem criptográfica do anterior. Por outras palavras, é uma base de dados digital, partilhada, descentralizada e sincronizada que se mantém à base de um algoritmo consensual e armazenado em diversos *nodes* (computadores individuais/usuários). Por ser assim, esta tecnologia tem a particularidade de não poder ser manipulada a partir do momento em que a informação é armazenada no bloco, pois assim que

---

[5] EDPS, Parecer 9/2016 "EDPS Opinion on Personal Information Management Systems, Towards more user empowerment in managing and processing personal data", 2016, disponível em https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf (acedido a 20/01/2019); Ramsay, Sebastian. "The General Data Protection Regulation vs. The Blockchain – A legal study on the compatibility between blockchain technology and the GDPR", Tese de Mestrado apresentada à Universidade de Estocolmo, 2018, p. 6, disponível em http://www.diva-portal.org (acedido a 20/01/2019).

[6] Fabiano, Nicola. "Internet of Things and Blockchain: legal issues and privacy. The challenge for a privacy standard", in *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)*, 2017, p. 730, disponível em https://ieeexplore.ieee.org (acedido a 20/01/2019).

entra neste é anexada à sequência já pré-existente. Apesar do termo ser por vezes usado para identificar qualquer *DLT*, independentemente de armazenar ou não dados em blocos, a verdade é que a noção de *blockchain* pode apenas designar a modalidade de *DLT* que efetivamente armazena informação em blocos, que por sua vez são "acorrentados" ou "ligados" (*hashed*) uns aos outros numa cadeira ininterrupta (*chained*).

Basicamente esta *DLT* funciona por um processo de dois momentos: cada utilizador tem uma chave pública (sequência alfanumérica) que o representa e à sua conta, e que é a que partilha com terceiros para poder celebrar transações; e uma chave privada (também alfanumérica) que representa basicamente uma senha/*password* própria que mantem sigilosa perante terceiros. As chaves relacionam-se através de operações matemáticas, que basicamente permitem à privada desencriptar dados através da chave pública.

O teor da informação que entra na sequência tem ainda a sua integridade salvaguardada graças a um mecanismo de "consenso" que subjaz a esta tecnologia. Como é que isto é possível? Cada bloco contém aspectos fundamentais da transação que ocorreu no bloco anterior e o respetivo *hash*[7]; se toda a rede e todos os *nodes* chegarem a consenso sobre a validade de uma nova transação, então um novo bloco será cronologicamente agrupado ao precedente, naquilo que se tornará uma cadeia de históricos validados. Uma vez adicionados, os blocos não podem ser removidos. E assim é porquanto a *blockchain* funciona numa rede descentralizada de computadores que periodicamente se sincronizam por forma a confirmar, repetidas vezes, que todos partilham das mesmas bases de dados, assegurando e

---

[7] O *hash*, que é uma técnica que solidifica praticamente todo o funcionamento da *blockchain*, é basicamente uma cadeia/código alfanumérico que permite a qualquer pessoa verificar que determinada informação digital é idêntica à informação que foi objecto de um *hash*; o que facilita em muito, por exemplo, a autenticação de documentos, i.e., a prova de que determinado documento é idêntico ao que foi atribuído um *hash*. Todavia, esta técnica só funciona num sentido, o que passa do documento original para o *hash*; já não no sentido contrário, i.e., do *hash* para o documento original. Ou seja, o *hash* não permite a chamada retroengenharia (*reverse-engineering*) para encontrar o documento original. Ainda assim, não deixa de ser possível estabelecer uma ligação entre o documento inserido na *blockchain* pelo *hash* e o titular do mesmo; desta forma, mesmo que em si mesmo não permita *reverse-engineer*, o *hash* de um documento de identidade, de um título de propriedade, ou de um plano de saúde do seu titular pode ser considerado dado pessoal.

veracidade das informações contidas no *ledger* que circula em toda a rede. São os mineiros (*miners*) que ficam encarregues de resolver os problemas matemáticos que transformam as informações (texto) contidas em cada bloco em sequências alfanuméricas designadas de *hashes*; que mais não são do que uma impressão digital única que confirma a correspondência de informação registada no *ledger* ou na *blockchain*. Desta forma, quanto mais usuários (*nodes*) integrarem a rede, menos os utilizadores precisam de confiar uns nos outros ou em terceiros intermediários para garantir transações seguras. Isto quer dizer que, na *blockchain*, a prova criptográfica e os algoritmos digitais substituem a confiança tradicional depositada em intermediários.

A tecnologia *blockchain* costuma dividir-se em duas principais classificações: as *public blockchains*, sempre que qualquer usuário lhe pode aceder e fazer uso para efeitos transacionais[8]; e *private blockchains*, sempre que a cadeia de blocos é controlada por uma determinada entidade e o acesso é autorizado apenas a determinados *nodes*[9]. Para exemplificar, podemos tomar em consideração a *Bitcoin*: como o seu sistema foi pensado para permitir que qualquer cidadão que entre na rede possa celebrar transações *online*, ele é, naturalmente, um sistema amparado numa *public blockchain*. Em sentido contrário, as *blockchain* autorizadas ou privadas processam-se como uma rede privada tipo *Intranet*, com um administrador centralizado de cuja autorização/permissão é necessária para poder passar a operar na *blockchain*. Pense-se na gestão de um setor de recursos humanos por um sistema de *private blockchain*, que faz uso desta tecnologia precisamente para obter um registo auditável de todos os seus dados sem que o público, em geral, e os funcionários, em particular, possam ter acesso. Estas tecnologias de *blockchain* privadas em pouco se distinguem de bases de dados privadas; a verdadeira revolução que esta tecnologia trouxe para o plano digital centra-se, verdadeiramente, nas cadeias de blocos públicas e na possibilidade de tornar qualquer registo imutável.

---

[8] Segundo os dados do Relatório elaborado pela *EU Blockchain Observatory and Forum* ("*Blockchain and the GDPR;* disponível em https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (acedido a 20/01/2019) 80% de todas as aplicações *blockchain* existentes são públicas.

[9] Ainda existem outras variações possíveis, como *blockchains* públicas, mas sujeitas a autorização.

Na *blockchain,* é possível armazenar qualquer tipo de dados (documentos, arte, registos, etc.) no *ledger* de três formas diferentes: texto, de forma criptográfica ou por *hashing.* A forma mais fácil de o fazer é com recurso a texto corrente; de resto, só não será a forma mais desejável do ponto de vista da privacidade já que qualquer pessoa pode arbitrariamente ler esses dados (no caso de *public blockchains*).

Em vez disso, o conteúdo lançado em blocos no *ledger* pode ser encriptado. A maioria dos *DLT*'s acaba por abarcar dois tipos de dados/informações: a) o *header* (cabeçalho) que contem o registo da data e hora, a fonte dos dados (a identidade é representada normalmente por um endereço IP) e o *hash* do bloco anterior; b) o conteúdo da transação em si, i.e., os dados a serem efetivamente armazenados na *blockchain* (designado por *payload*). A diferença entre um e outro prende-se com o fato de o *header* normalmente não ser encriptado, ao contrário do *payload*[10]. Alternativamente à encriptação do texto lançado no *ledger*, os usuários também podem transformar esse conteúdo em *hashes* e depois lançar estas (e não o próprio texto/informação) na *DLT*. Os *hashes*, que são sequências criptográficas unidirecionais, não podem ser objeto de retroengenharia (*reverse engineering*), pelo que não podemos recorrer a chaves privadas para os desencriptar; aquilo que permitem, pelo contrário, é verificar se determinado documento com certas características foi armazenado ou não num banco de dados e atestar a sua correspondência.

Várias têm sido as aplicações possíveis desta tecnologia. Além da já aqui mencionada crucial importância no funcionamento de *criptomoedas*, a blockchain foi ainda mote para desassossegar o mundo dos contratos civis com a criação da figura dos *smart contracts*[11] e, além de muitas outras, pode

---

[10] Sempre que os dados são encriptados, só o utilizador que tenha a chave privada poderá desencriptar os mesmos. A criptografia surge, assim, como técnica para garantir uma assinatura digital única que permite a reversão dos dados ao estado anterior e o desbloqueamento do documento. Pessoas que não tenham esse acesso autorizado, deixam de poder ter acesso à informação encriptada.

[11] Costuma atribuir-se a Nick Szabo a autoria da criação destes "contratos inteligentes" (*smart contracts*), nos anos 90. Szabo quis reformular a forma como pensamos os contratos e fê-lo através da criação de um software de computador semelhante a cláusulas contratuais que se baseassem na confiança de protocolos criptográficos. O uso de contratos inteligentes amparados na tecnologia blockchain permite, hoje em dia, aos seus usuários celebrar relações jurídicas vinculantes com recurso a códigos criptográficos e fazendo uso daquele software

vir a ter significativa relevância no setor dos registos públicos, apesar das questões que a temática já tem levantado[12].

3. O novo Regulamento Geral de Proteção de Dados

Como acima mencionado, o debate em torno do problema aqui colocado não pode ser deslocado do novo RGPD, que entrou em vigor no espaço europeu em Maio de 2018[13].

---

para garantir o cumprimento do contrato. Em determinada medida, não podemos dizer que os contratos tal como os conhecemos hoje sejam significativamente diferentes *smart contracts*, já que antes da execução deste, também lhe precede um momento de negociação prévio entre os contraentes para registar o seu teor em *smart contract* code. A grande mais-valia desta tecnologia e que faz dos contratos inteligentes um marco no mundo digital e novas tecnologias, prende-se com a sua força autoexecutória, i.e., na capacidade que este tem de vincular o cumprimento de obrigações contratuais. O código presente no *smart contract* é executado diretamente, sem necessidade de recorrer a quaisquer intermediários para o efeito, tais como ações declarativas, executivas, recurso a advogados, etc. Enquanto programas digitais formatados sob a tecnologia do consenso blockchain, quaisquer mudanças não autorizadas na sua estrutura encontram-se necessariamente inviabilizadas e todas as condições previamente acordadas são objeto de uma implementação e controlo estritos, automatizados pelo código computacional trazido pelo software. Ambas as partes sabem destas condições e aceitam-nas. O comprador sabe que o não pagamento do preço no prazo acordado implica a imediata perda de controlo sobre o bem; o credor sabe que se o mesmo não for efetuado, a verificação da *compliance* é imediata e automático o procedimento executório de cessação contratual, sem custos adicionais relacionados (*v.* Belo, José. "Smart Contracts: Possível Solução Para A Relutância Em Entrar Num Contrato Em Ambiente Online?", *Cyberlaw,* v. 1, n. 5, 2018, disponível em https://www.academia.edu/36701400/Smart_contracts_poss%C3%ADvel_solução_para_a_relutância_em_entrar_num_contrato_em_ambiente_online (acedido a 20/01/2019).

[12] Assim, e apenas a título de exemplo, discute-se como compatibilizar a blockchain com serviços de cartório, já que (i) o funcionamento *P2P* da *blockchain* seria incompatível com a necessária a presença de funcionários que façam a leitura e análise da documentação apresentada pelas partes, qualifiquem os títulos etc.; (ii) a vantagem da consensualidade que a tecnologia traz nada acrescentaria ao princípio do trato sucessivo (coerência na cadeia de transmissões) que já existe no sistema de registos; (iii) além de que a imutabilidade da *blockchain* seria também supostamente incompatível com a necessidade de introduzir retificações aos registos.

[13] A nível internacional, destaco ainda (i) a modernização da Convenção 108 de 1981 (Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal) levada a cabo desde Maio de 2018 pelo Conselho da Europa e já assinada

Porque o nosso propósito não é o de fazer uma análise exaustiva deste diploma, vamos apenas referenciar alguns aspectos relevantes que desafiam a temática da *blockchain*[14]: (i) os principais conceitos-chave envolvidos, (ii) os princípios que maior potencial têm de ser afetados, (iii) que direitos atribuídos aos titulares dos dados pessoais poderão ser ofendidos.

À imagem e semelhança das boas práticas europeias, o RGPD veio adotar como técnica legislativa o uso de definições para esclarecer noções fundamentais à compreensão do documento. Entre outras, destacam-se os conceitos de (i) *dados pessoais*: qualquer informação/dado que se relacione com uma pessoa identificável (art.º 4º, n.º 1 do RGPD); (ii) de *dados pseudonimizados*: o tratamento de dados que, apesar de à partida não poder ser atribuído a um titular específico, admite essa hipótese com recurso a informações suplementares (art.º 4.º, n.º 5 do RGPD); (iii) *responsável pelo tratamento*: entidade que decide a finalidade do tratamento (art.º 4º, n.º 7 do RGPD), (iv) *subcontratante:* entidade que procede ao tratamento de dados por conta do responsável do tratamento (art.º 4.º, n.º 8 do RGPD), (v) *tratamento de dados*: qualquer operação que se faça com uso de dados pessoais, que vão desde a simples recolha/coleta, passando pelo seu processamento, armazenamento, transferência ou mesmo eliminação (art.º 4º, n.º 2 do RGPD).

Relativamente aos princípios previstos no RGPD, destacam-se (i) o princípio da *limitação das finalidades*: qualquer dado pessoal só pode ser

---

por Portugal desde Outubro desse ano (modificações que vieram adequar a Convenção aos diplomas internacionais existentes e, assim, (i) reajustaram conceitos e incorporaram as noções de *data controller* e *data processor*, (ii) reforçam-se princípios como o da proporcionalidade e da minimização do uso de dados; (iii) acrescenta-se disposição específica para regulamentação do consentimento do titular dos dados; (iv) alarga-se o catálogo de dados considerados sensíveis, (v) reforçam-se as exigências em matéria de segurança e proteção de dados; (vi) novos direitos são atribuídos aos titulares dos dados, (vii) criam-se novas obrigações etc.); e (ii) a Lei 13.709, de 14 de Agosto (Lei Geral de Proteção de Dados), que instituiu as novas regras brasileiras em matéria proteção de dados pessoais, ainda que este venha apenas a entrar em vigor em 2020 (18 meses após a sua promulgação) redigida sob notória influência daquilo que já se professava nas regulações europeias nesta matéria e, portanto, sem grandes novidades jurídicas regulatórias,).

[14] Como os principais problemas de compatibilização desta tecnologia com o RGPD não se colocam em abstrato para todas as técnicas *blockchain*, mas sobretudo quando o tipo de sistema *blockchain* é de acesso público; a análise aqui efetuada parte desta premissa e dirige-se sobretudo à análise destes, e não de outros (v.g. privados) sistemas.

recolhido e tratado com propósitos legítimos, concretos e determinados, que sejam devidamente comunicados ao respetivo titular, e sem que possam ser usados para outras ou além das finalidades recolhidas (art.º 5º, n.º 1, al. b) do RGPD); (ii) princípio da *minimização dos dados*: o tratamento tem que ser compatível com as finalidades declaradas para a sua recolha e limitadas ao necessário para a sua prossecução (art.º 5º, n.º 1, al. c) do RGPD); (iii) princípio da *transparência*: que garante ao titular dos dados que todas as informações são dadas e de forma clara e precisa (art.º 5º, n.º 1, al. a) e 12º do RGPD); (iv) o princípio dos *limites da conservação:* que visa garantir que todos os dados são conservados adequadamente, por forma a permitir sempre a identificação e acesso dos seus titulares (art.º 5º, n.º 1, al e) do RGPD); (v) princípios da *integralidade e confidencialidade*: acompanhados de medidas técnicas de proteção desses mesmos dados, que impeçam o acesso não autorizado, a perda, etc., sob pena de responsabilidade administrativa ou mesmo penal (art.º 5º, n.º 1, al f) do RGPD).

Por último, destacamos ainda alguns direitos atribuídos ao titular dos dados que o RGPD veio revisitar e/ou incorporar: (i) direito de *acesso* aos dados (art.º 15º do RGPD), que poderá ser efetuado sem quaisquer constrangimentos e a qualquer tempo desde que efetuado mediante requerimento prévio; (ii) direito de *retificação e apagamento*, que se traduz no direito do titular dos dados a, por ex., ver revogado o seu consentimento, exigir do responsável pelo tratamento a destruição dos seus registos no banco de dados, a sua a total exclusão, a mera oposição ao tratamento, ou correção (art.º 16º e 17º do RGPD); (iii) direito à *portabilidade dos dados* (art.º 20º do RGPD), i.e., o direito solicitar ao responsável pelo tratamento a transmissão dos seus dados pessoais para outra entidade.

4. Âmbito de aplicação do RGPD, dados pessoais e tratamento de dados

Saber se a tecnologia blockchain deve passar pelo crivo das restrições das leis de proteção de dados exige a resposta a duas perguntas: (i) será que os dados armazenados na cadeia de blocos se configuram dados pessoais?; (ii) se assim for, será que a *blockchain* realiza tratamento de dados de alguma forma?

4.1. Dados pessoais

Sabemos que dados pessoais constituem qualquer tipo de informação associada a uma pessoa identificada ou identificável (nome, número de identificação fiscal, agência e conta bancária, escola que frequentou, notas que tirou, idade, etc.)[15]. Sabemos também que (i) o RGPD só se aplica caso estejamos perante um dado considerado como "pessoal" e não a qualquer tipo de dado; e que (ii) dados anónimos não entram no escopo da regulamentação europeia. Para saber se a *blockchain* lida com dados pessoais, precisamos perceber que dois são os tipos de dados que nela interagem: aquilo a que se chama de *transactional data*[16] e as *public keys*.

Dados financeiros, médicos, de identificação, comportamento de consumo *online* são informações pessoais que se costumam designar por *transactional data* e sobre os quais costumam girar as transações *online*. Como vimos acima[17], há três formas de armazenar dados na *blockchain*: texto, criptografia ou *hashing*; pelo que a resposta a esta pergunta exige uma apreciação sob todas estas alternativas. A primeira hipótese não levanta grandes dúvidas: quando os dados são armazenados na *DLT* sob a forma de texto simples, estão necessariamente em causa dados pessoais que permitem identificar uma pessoa, pelo que colhe aplicação o RGPD. Já relativamente aos dados armazenados sob a forma criptográfica, como permanece possível o seu acesso mediante o uso de uma chave privada, o seu rastreamento até ao respetivo titular permanece viável e, portanto, não podem ser considerados como anónimos, mas pseudonimizados.

---

[15] Nos termos do artigo 4.º, n.º 1 do RGPD, deve entender-se por dado pessoal uma "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

[16] Finck, Michèle. "Blockchains and Data Protection in the European Union", in *Max Planck Institute for Innovation and Competition Research Paper,* n. 18-01, p. 9 e ss., disponível em https://papers.ssrn.com (acedido a 20/01/2019).

[17] *Supra*, 3. II.

Por último, e com as necessárias reservas[18], se os *transactional data* forem transformados em *hashes*, ainda poderão ser considerados como dados pessoais. É verdade que o nível de privacidade oferecido por um *hash* é significativamente maior que a mera criptografia, pois este não pode ser objeto de retroengenharia. Todavia, não é outra a conclusão que se pode extrair do parecer do Grupo de Trabalho sobre o Artigo 29 (GT29)[19], ao concluir que também os *hashes* são formas de pseudonimização (e não de anonimização) de dados pessoais, na medida em que uma pessoa pode ainda ser rastreada e identificável[20].

As chaves públicas (*public keys*) não são dados transacionáveis, mas um conjunto alfanumérico que identifica de forma pseudonimizada um usuário que pretende fazer transações ou comunicações[21]. Vimos acima a noção de dados *pseudonimizados*. Ora, as transações/comunicações na *blockchain* que são efetuadas através da publicação de uma chave pública estão irremediavelmente associadas a um endereço de *IP*. Todavia, se por um lado é certo que esta chave pública se encontra criptografada para que se consiga um certo anonimato na operação *online*, não menos certo é ser possível identificar indiretamente a entidade/sujeito que representa

---

[18] Nomeadamente, se, com o tempo, avanços tecnológicos no mundo da criptografia revelarem ser efetivamente possível tornar estes dados anónimos, como promete o SHA-256 ou SHA-3. Por outro lado, e como se dirá *infra*, algumas técnicas têm permitido que estes dados transacionais não sejam diretamente lançados na *blockchain*, das quais é maior exemplo o armazenamento de dados fora da *blockchain* vinculados à cadeia de blocos por meio de um *hash* (*cf.* Finck, Michèle. *Max Planck Institute for Innovation and Competition Research Paper*, n. 18-01, pág. 11, disponível em https://papers.ssrn.com (acedido a 10/01/2019).

[19] GT29, Parecer 05/2014 sobre técnicas de anonimização, disponível em https://www.gpdp.gov.mo (acedido a 10/01/2019). Como se pode ser no Parecer: "a utilização de uma função *hash* com uma variável criptográfica (em que um valor aleatório, designado por 'variável criptográfica', é adicionado ao atributo a ser dividido [*hashed*]) é passível de reduzir a probabilidade da determinação do valor de entrada mas, ainda assim, continua a ser possível de efetuar, mediante os meios razoáveis, o cálculo do valor original do atributo escondido por detrás do resultado de uma função *hash* com uma variável criptográfica" (cit. pág. 22).

[20] Neste sentido, Finck, Michèle. *Max Planck Institute for Innovation and Competition Research Paper*, n. 18-01, p. 11, disponível em https://papers.ssrn.com (acedido a 10/01/2019).

[21] Ramsay, Sebastian. *The General Data Protection Regulation vs. The Blockchain – A legal study on the compatibility between blockchain technology and the GDPR*, Tese de Mestrado apresentada à Universidade de Estocolmo, 2018, p. 41, disponível em http://www.diva-portal.org (acedido a 10/01/2019).

aquele usuário pela reutilização daquela chave-pública e correspondente associação a determinado endereço de *IP*[22]. A não ser assim e mal se conceberia um sistema que usa precisamente a técnica da cadeia de blocos para garantir a unicidade da operação entre determinados sujeitos, i.e., para garantir que aquela operação em concreto foi efetivamente realizada por aqueles indivíduos em particular.

Sendo então possível associar aquela chave pública – leia-se, aquele dado pessoal (realização de uma transação, promoção de um registo, realização de uma operação de voto, etc.) – a determinado usuário, então teremos de concluir que também as chaves públicas se qualificam como dados pessoais para efeitos da aplicação da regulamentação europeia de dados pessoais[23].

Também paralela a esta discussão, encontra-se o acórdão C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* de 19 de Outubro de 2016, relacionado a endereços de *IP* dinâmicos (*dynamic IP addresses*); e isto porque aqui o TJ vem discutir o conceito de "dados pessoais" de forma muito relevante para o contexto da *blockchain*. Não obstante o acórdão ser anterior ao RGPD, como o conceito de dados pessoais deste se manteve inalterado, a referência mantém a sua pertinência.

---

[22] Reid, Fergal; Harrigan, Martin. "An analysis of anonymity in the bitcoin system", *arXiv:1107.4524v2*, 2011; e Biryukov, Alex; Khovratovich, Dimitry; Pustogarov, Ivan, "Deanonymisation of clients in Bitcoin P2P network", *arXiv:1405.7418v3*, 2014, ambos disponíveis em https://arxiv.org (acedido a 10/01/2019).

[23] Como clarifica Finck, uma chave pública é um dado que não pode ser imputado a determinado titular excepto se complementado com informações adicionais (tal como nome, endereço IP etc.). Quando essas informações se reúnem a identificação de usuários torna-se possível pelo que chaves públicas não podem ser consideradas dados anónimos. Para além dessas informações serem, não-raro, divulgadas voluntariamente pelos próprios usuários, a Autora também reporta que estudos académicos já demonstram que chaves públicas podem ser usadas para localizar endereços de *IP* se levar em conta informação adicional (cf. Finck, Michèle. *Max Planck Institute for Innovation and Competition Research Paper*, n. 18-01, p. 13, disponível em https://papers.ssrn.com (acedido a 10/01/2019). No mais, diz-nos De Filippi que "While good privacy norms would require people to constantly generate a new address before performing a new transaction, only a minority of people actually engage in these practices. In the Bitcoin space, most non-tech savvy people simply reuse their Bitcoin address without realizing that, by doing so, they are publicly disclosing valuable personal information" (Primavera, De Filippi. "The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies", in *Journal of Peer Production*, v. 9, 2016, p. 11, disponível em https://papers.ssrn.com (acedido a 10/01/2019).

Alguns *sites* de serviços federais alemães para se protegerem de ataques *online* e permitir ações penais, guardam em registo todas as consultas de usuários que acedem aos seus sítios (sessão, nome do sítio, ficheiro consultado, dados transferidos, endereço *IP* do computador do utilizador etc.). P. Breyer, um desses usuários, deu entrada de uma ação contra a República Federal Alemã alegando que a conservação do seu endereço *IP* era desnecessária para os propósitos alegados. Ora, os *IP's* são conjuntos numéricos que permitem identificar computadores ligados à *internet* e que são transmitidos ao servidor do *site* visitado para que os dados consultados possam ser transferidos ao destinatário. Entre esses *IP's*, encontra-se uma modalidade designada "IP dinâmico" que, ao contrário do "IP estático", muda a cada nova conexão à *internet* e, assim, impede que, por ficheiros públicos, se consiga encontrar diretamente determinado computador sem antes recorrer ao respetivo fornecedor de acesso à *internet*. Em resposta à questão prejudicial colocada ao TJ sobre saber se esse *IP* dinâmico poderia ou não ser considerado dado pessoal, foi considerado que a noção de dado pessoal da então Diretiva 95/46 deveria ser interpretada no sentido de incluir esse endereço, mesmo quando careça de informações de terceiro (neste caso o fornecedor de acesso à *internet*) para prestar informação complementar necessária à identificação do computador usuário (§31); entendendo que um dado pessoal pode ser assim considerado mesmo que nem todas as informações necessárias para identificar o seu titular se encontrem na posse da mesma pessoa (§44) e desde que "não seja proibido por lei ou inexequível" (§46) a um fornecedor de serviços transmitir diretamente ao prestador aquelas informações suplementares necessárias à identificação do titular dos dados.

Algumas tentativas têm sido postas em prática para ultrapassar esta situação e retirar estes dados da alçada do RGPD. Relativamente aos *transactional data*, caso os dados sejam armazenados fora da cadeia pública), mas vinculados ao *ledger* através de um *hash*, seria possível encriptar os dados de forma segura, já que protegidos por um *hash* irreversível. No *ledger* apenas um dado aleatório alfanumérico ficaria visível enquanto os verdadeiros dados a que o *hash* se referia ficariam armazenados fora da cadeia de blocos. O principal risco associado a esta alternativa prende-se com a necessária implicação de um terceiro na gestão desse banco de dados editável fora da cadeia. Nesta situação, um dos potenciais motivos que teria conduzido à opção pela *blockchain* – a descentralização de informação

– seria diretamente afetada pela reunião do controlo/confiança dos dados numa entidade centralizada.

Ao contrário daqueles, porém, as *public keys* não podem ser transferidas para fora da cadeia por serem parte integrante do funcionamento da própria *blockchain* e necessárias para que a validação de transações ocorra. Apesar de a tarefa ser mais árdua, algumas tentativas têm, não obstante, se destacado na doutrina mais recente[24].

4.2. Tratamento de dados

Nos termos do art.º 4, n.º 2, do RGPD, o tratamento de dados é considerado como qualquer operação que é executada com dados pessoais, "(...) 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".

---

[24] Em particular, a criptomoeda *Monero* (que logrou esconder o endereço dos seus usuários, mudando-lhes o endereço e gerando chaves secretas) e as também designadas *zero knowledge proofs ou ZKP* (provas de conhecimento zero) que, sem fornecerem dados concretos, funcionam numa lógica binária de verdadeiro/falso e permitem atestar um acontecimento sem fazer referência a informações sobre o mesmo. Basicamente este ZKP limita-se a atestar se uma transação em que determinada chave pública foi usada teve lugar, sem mencionar dados sobre ela. Ainda numa outra hipótese, mencionam-se as chamadas *ring signatures,* que encontraram uma forma de omitir dados da *key* ao ocultar a transação realizada dentro de outras tantas; basicamente esta *ring signature* atesta que o usuário tem uma chave privada que corresponde a um conjunto de chaves públicas, mas sem revelar qual. Por último, destacam-se ainda técnicas que procuram dispersar a informação disponível, incorporando "ruído" ou "excesso de informação desnecessária": a ideia é garantir que de um ponto de vista externo seja impossível identificar os destinatários/remetentes das transações, tantas são e de forma tão agrupada que se apresentam. Por todos, Primavera De Filippi. "The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies", in *Journal of Peer Production*, v. 9, 2016, p. 14, disponível em https://papers.ssrn.com, (acedido a 11/01/2019). O próprio GT29 já veio reconhecer esta última técnica como uma possível medida aceitável de anonimização. Para uma explicação clara das várias opções cfr. Relatório elaborado pela *EU Blockchain Observatory and Forum* (*Blockchain and the GDPR,* 2018, p. 19-23, disponível em https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (acedido a 11/01/2019).

Resta saber que ações são levadas a cabo nos dados que são lançados para a *blockchain* como dados pessoais. Aqui a análise uma vez mais ponderará quer as *public keys* e *transactional data*, quer os próprios *nodes*.

A cada *chave pública* corresponde uma determinada chave privada que é entregue a todos os usuários da cadeia de blocos, pelo que todos os usuários de uma chave pública se podem controlar mutuamente e verificar a autorização de novas transações. Essas verificações de validade são automatizadas segundo um algoritmo da tecnologia *DLT*. Tendo em conta a amplitude do termo de tratamento de dados no RGPD, mesmo que o tratamento seja autonomizado e se processe pela via de um algoritmo matemático, é possível qualificar como tal esta operação de verificação da validade de transações através de chaves públicas.

No que respeita aos *transactional data*, os dados são validados também através de certos algoritmos: são armazenados num determinado bloco, que é posteriormente anexado à *blockchain* e distribuído por todos os outros usuários. Isto implica que operações de uso e armazenamento são necessariamente realizadas, pelo que também quanto a estes dados se deve considerar existir tratamento de dados para efeitos do art. 4.º, n.º 2, do RGPD.

Quanto aos *nodes*/usuários e respetivo endereço, também vimos que cada um mantém cópia e registo com todos os outros *nodes* com os quais comunica, o que faz com que também eles mantenham uma rede de armazenamento de dados pessoais que possa ser qualificada como tratamento de dados[25].

5. Potenciais conflitos com princípios do RGPD

Como é característico das *blockchain* públicas, os participantes da cadeia normalmente desconhecem que dados (pessoais ou não; sensíveis ou não) estão a ser lançados no *ledger*. Por isso se diz no Relatório apresentado pelo EU *Blockchain Observatory and Forum* que o problema entre *blockchain* e o

---

[25] Ramsay, Sebastian. "The General Data Protection Regulation vs. The Blockchain – A legal study on the compatibility between blockchain technology and the GDPR", *Tese de Mestrado apresentada à Universidade de Estocolmo*, 2018, p. 43-44, disponível em http://www.diva-portal.org (acedido a 12/01/2019)

RGPD não respeita à tecnologia em si, mas ao uso que dela é feito, o que implica uma análise casuística[26]. Isto porque, e como mencionámos acima, a *blockchain* apenas se revela através de *hashes* (códigos alfanuméricos). Um sistema público *blockchain* será usado por uma grande diversidade de usuários e para registar qualquer tipo de documentos, transações, registos, envolvendo indistintamente dados pessoais, dados não pessoais, dados sensíveis, etc. Dada a grande diversidade de usos possíveis, as *public blockchain* acabam por ter grande dificuldade em conseguir construir medidas de proteção do tipo requerido pelo RGPD (art. 25.º). Para fazer face a este problema, muitos talvez procurem transportar o encargo da *compliance* para os próprios utilizadores (proibindo o *upload* de certo tipo de dados, exigindo que os usuários prestem consentimento etc.), o que, claramente, não dá uma resposta satisfatória à situação.

A elaboração do RGPD foi levada a cabo num momento em que o revolucionário sistema descentralizado da *blockchain* se começava ainda a desenvolver, pelo que as principais preocupações a que precisava dar resposta centravam-se sobretudo nos serviços em *cloud* e nas redes sociais, organizadas essencialmente por sistemas centralizados com que os usuários interagem[27]. A chegada de *blockchains* públicas trazem consigo um sistema que foge a este mundo centralizado. Nestes sistemas onde toda a informação é partilhada e replicada por toda a rede, a eliminação de dados e a tutela da privacidade podem representam um problema para os seus titulares. Ora, como em princípio os dados armazenados numa cadeia de blocos se tornam invioláveis, excluí-los dificilmente se torna uma opção e a afetação do direito ao apagamento torna-se uma realidade. Por outro lado, o fenómeno da descentralização que tanto caracteriza o funcionamento desta tecnologia, implica a ausência de um controlo único e centralizado da informação numa entidade concreta, o que dificulta a compreensão dos sujeitos obrigados às regras previstas no Regulamento, o apuramento de responsabilidades e a aplicação das respetivas sanções.

---

[26] Relatório *Blockchain and the GDPR;* p. 16, disponível em https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (acedido a 11/01/2019).

[27] Eichler, Natalie, et. Al. "Blockchain, data protection and GDPR", in *Blockchain Bundesverband,* disponível em https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf (acedido a 28/01/2019).

É inegável a existência de uma grande tensão entre a arquitetura descentralizada desta tecnologia e o novo RGPD, que acaba por refletir um conflito idêntico de objetivos entre, por um lado, a necessidade de proteger dados pessoais e acautelar os direitos dos seus titulares e, por outro, a vontade de promover a inovação tecnológica.

5.1. Direito ao apagamento e retificação

Nestes sistemas de *blockchain* públicas, assim que transações são registadas na cadeia, deixam de poder ser modificadas ou apagadas: uma transação subsequente que anule ou modifique os termos da anterior pode sempre ocorrer, mas fá-lo-á mediante a adição de um novo bloco ao *hash* original que, além de registar a nova transação onde ratifica os dados da anterior, ainda a reproduz. A forma de garantir que a cadeia não é alterada e editável encontra-se na referência que cada bloco subsequente tem necessariamente que fazer do anterior, através de *hash* criptográfico; desta forma, se a informação contida nesse bloco anterior for alterada, assim também o será o respetivo *hash* o que permitirá a detetar a falsificação. Quer isto dizer, então que, em princípio, todos os dados lançados na *blockchain* seriam tendencialmente indestrutíveis, imutáveis e impassíveis de modificação, o que claramente representa um problema na óptica do RGPD.

Veja-se que já desde Maio de 2014, no processo C-131/12 que opôs *a Google Spain* e *Google Inc.* à Agência Espanhola de Proteção de Dados e a Mario González, o TJ determinou que este último, reclamante nos autos que moveu contra a Google, tinha direito a remover dos motores de busca qualquer conteúdo recuperável nos índices de resultados de pesquisa. Na sua justificação, o TJ considerou que esse direito é independente de saber se a manutenção dessa informação em resultados de pesquisa causa, ou não, qualquer prejuízo ao titular dos dados (§96); e que, nos termos dos direitos fundamentais plasmados no art. 7º e 8º da Carta, esse direito se sobrepõe não só sobre qualquer interesse económico do operador do motor de busca, como também de qualquer interesse público em encontrar essa informação em resultados de pesquisa, excepto em circunstâncias muito excepcionais (§97). Amparado no direito ao apagamento e de oposição da Diretiva 95/46 (art.os 12.º, b) e 14.º, a), respetivamente) o TJ veio consolidar o "direito ao esquecimento" no espaço informático, o qual, por sua vez,

foi igualmente reforçado em rúbrica própria pelos art.os 17º e 5.º, n.º 1, al. d) do RGPD.

Naturalmente que o direito ao apagamento não é de natureza absoluta. As circunstâncias em que os titulares dos dados podem fazer uso deste direito restringem-se, entre outras, às situações em que: (i) deixem de ser necessários à finalidade que motivou a recolha (art.º 17º, n.º1, al. a) do RGPD); (ii) o titular retire o seu consentimento (art.º 17º, n.º1, al. b) do RGPD); (iii) o titular oponha-se ao tratamento sem que haja interesses legítimos prevalecentes que o justifiquem (art.º 17º, n.º 1, al. c) do RGPD); ou (iv) tenham sido tratados ilicitamente (art.º 17º, n.º 1, al. d) do RGPD). Mas independentemente disto, outros problemas práticos poderiam advir desta situação. Desde logo, o titular dos dados que pretendesse fazer valer este direito não tinha como reclamar perante todos os outros *nodes* da rede os seus direitos, já que não tinhe como os identificar. Por outro lado, mesmo que o conseguisse, esses *nodes* não teriam como, eles mesmos, conseguir modificar ou apagar qualquer dado armazenado no *DLT*.

Além deste âmbito limitado, também caberá perguntar o que efetivamente constitui a noção de "apagamento" ("*erasure*"), já que o próprio RGPD não o especifica. Será que representa o total desaparecimento dos dados do mundo real e/ou virtual, ou basta que haja técnicas de proteção que tornem os mesmos criptografados de forma irreversível? Já vimos que no âmbito do sistema *blockchain* um apagamento é tecnicamente muito difícil porquanto o sistema foi criado precisamente com o propósito de impossibilitá-lo. No entanto, a criação de alternativas tecnológicas que limitem o processamento dos dados[28], ou que façam referência a dados anteriores como não sendo mais consideráveis, poderá ser questionável como sendo suficiente para efeitos de acautelar este direito.

Já têm sido desenvolvidas ideias que permitem ultrapassar este problema. Mas mais uma vez a análise passa por uma distinção entre *transactional data* e *public keys*[29].

Quanto aos primeiros, basta que os mesmos sejam armazenados num banco editável e criptografado de dados fora da cadeia, para poder

---

[28] Finck, Michèle. "Blockchains and Data Protection in the European Union", *Max Planck Institute for Innovation and Competition Research Paper,* n. 18-01, p. 24, disponível em https://papers.ssrn.com (acedido a 20/01/2019).

[29] *Idem,* p. 24.

corresponder com as exigências do RGPD e permitir a eliminação dos dados sem interferir com a *blockchain*. Todavia, estas modificações ao *software* sempre acarretarão consequências indesejáveis, nomeadamente no plano da integralidade de teor e autenticidade dos documentos registados na *blockchain*, requerendo a nomeação de entidades responsáveis para as administrar. Por outro lado, certas características apontadas como grandes vantagens desta tecnologia, tal como a descentralização de dados *P2P*, deixarão de poder subsistir, para que se permita a compatibilização da mesma com o RGPD. Alternativamente, e como já vimos acima, surge ainda a possibilidade de armazenar dados num banco de dados encriptado e introduzir um *hash* desse mesmo banco na cadeia de blocos; técnica que mantém a integralidade e integridade do teor dos dados sem os tornar visíveis no *ledger*. Esta é, de resto, uma tendência nesta indústria: evitar enviar dados pessoais diretamente na cadeia de blocos, para os armazenar em bancos de dados fora da cadeia, com apenas um e unidirecional *hash* dos dados armazenados na própria *blockchain*; é esse *hash* que servirá de ponto de referência e link para o banco de dados fora da cadeia de blocos.

No que respeita às *public keys*, há quem mencione procedimentos realizados em ambientes supervisionados e seguros onde o próprio titular dos dados possa eliminar a sua chave privada, inviabilizando simplesmente o acesso àqueles dados, já que ela seria a única responsável por desencriptar a respetiva informação[30]. Em alternativa, há quem fale nos chamados *chameleon-hashes* ("*hashes* camaleão") que reescreveriam o teor dos blocos armazenados na *blockchain*, sob determinadas restrições e supervisão de autoridades autorizadas e com transparência[31]. Esta solução, porém, ao

---

[30] Finck, Michèle. "Blockchains and Data Protection in the European Union", in *Max Planck Institute for Innovation and Competition Research Paper,* n. 18-01, p. 24, disponível em https://papers.ssrn.com (acedido a 20/01/2019). No mesmo sentido, também a a *Comission Nationale Informatique & Libertés* (CNIL) reconhece que "(...) la suppression de la clé secrète de la fonction de hachage qui aura un effet similaire. Il ne sera plus possible de prouver ou de vérifier quelle information avait été hachée. L'empreinte ne présentera plus, en pratique, de risque sur la confidentialité. L'information devra, ici aussi, être supprimée des autres systèmes où elle aura été stockée pour le traitement" (p. 10, disponível em: https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf , acedida a 22/01/2019).

[31] Giuseppe Ateniese et al, "Redactable Blockchain – or – Rewriting History in Bitcoin and Friends", pág. 2, disponível em https://eprint.iacr.org/2016/757.pdf (acedido a 23/01/2019): "(...) we argue that an immutable ledger is not appropriate for all new applications

confiar numa terceira autoridade/árbitro para realizar o serviço, acaba por voltar ao mesmo problema da própria essência da *blockchain* ser posta em causa.

5.2. Transferência de dados

Nos termos do disposto no art.º 3.º, n.º 1 e 2 (após a correção linguística levada a cabo pelo Conselho da UE n.º 8088/18[32]), o RGPD aplica-se a tratamentos de dados independentemente da residência do seu titular, desde que este se encontre em território da União. Por outro lado, nos termos do art.º 44º do RGPD, as transferências de dados para países terceiros só são possíveis quando respeitado um conjunto de condições, nomeadamente a existência de um nível de proteção adequado (a definir pela própria Comissão) e de uma autorização específica do titular dos dados.

E é aqui que chegam as perguntas: como podemos determinar em que país determinado *node* se encontra? Como é que na *blockchain* podemos garantir que as transferências de dados se processam com níveis adequados de proteção? No âmbito da contratação digital, será possível estabelecer cláusulas contratuais padronizadas para salvaguardar estes direitos na *blockchain*?

Sucede, porém, que quando estão em causa *blockchain* públicas uma presunção quanto à existência de *nodes* situados – ou de tratamentos

---

that are being envisaged for the blockchain. Whether the blockchain is used to store data or code (smart contracts), there must be a way to redact its content in specific and exceptional circumstances. Redactions should be performed only under strict constraints, and with full transparency and accountability"); Ibáñez Luis-Daniel, O'Hara, Kieron; Simperl, Elena. "On Blockchains and the General Data Protection Regulation", p. 8, disponível em https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf (acedido a 09/01/2019).

[32] Documento do Conselho da UE, n.º 8088/18, de 19 de abril de 2018, disponível em http://data.consilium.europa.eu/doc/document/ST-8088-2018-INIT/en/pdf (acedido a 22/01/2019). Sobre a problemática linguística que antecedeu esta revisão Moniz, Maria Graça, "Finalmente: coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! O fim do enigma linguístico do artigo 3.º, n.º 2 do RGPD", *UNIO – EU Law Journal*, v. 4, n. 2, 2018, disponível em http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%204%20.%20Vol%201/Unio%204%20n.%202%20PT/Graça%20Canto%20Moniz.pdf (acedido a 18/01/2019).

realizados – fora do território da União torna-se fácil de extrair. Além disso, os *miners* (mineradores) – que resolvem os problemas matemáticos que permitem o lançamento de dados para o *ledger* –, são sempre escolhidos aleatoriamente para a tarefa, podendo encontrar-se em qualquer lugar do mundo[33]. Na falta da decisão tomada ao abrigo do art.º 45º, dispõe o art.º 46º que os dados sempre poderão ser transferidos para terceiros, desde que apresentadas "garantias adequadas e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas" eficazes. Ora, apesar de em teoria se poderem conceber alterações ao protocolo do *software* o se compatibilizar com estas condições, dificilmente tal será possível. Por ser assim, a doutrina tem vindo a apontar a necessidade de consentimento explícito para a transferência dos dados a terceiros, com informação prévia acerca dos possíveis riscos envolvidos[34].

5.3. Controlo sobre os dados

Outro problema de compatibilização que encontramos entre *blockchain* e o RGPD prende-se com a identificação do responsável pelo tratamento (*data controller*), *i.e.*, aquele que determina as finalidades do tratamento de dados e assume a responsabilidade originária por qualquer violação[35]) e do subcontratante (*data processor*), *i.e.,* aquela entidade que efetivamente realiza o tratamento de dados conforme instruções do responsável pelo tratamento. E este problema é tanto mais complexo no contexto digital da *blockchain*, quanto mais nos apercebermos de que as mesmas entidades podem assumir, simultaneamente, mais do que um papel. Apesar de ambos os papéis desempenhados não serem livres de obrigações e responsabilidades pelo RGPD, a determinação precisa de cada um não deixa de ser determinante.

Naturalmente que no caso das *private blockchain,* aquele que se assume destinatário dos dados enviados pelo titular pode facilmente qualificar-se

---

[33] Finck, Michèle. "Blockchains and Data Protection in the European Union", in *Max Planck Institute for Innovation and Competition Research Paper*, n. 18-01, p. 19, disponível em https://papers.ssrn.com (acedido a 08/01/2019).

[34] *Idem*, p. 19.

[35] Art. 4º, n.º 7 do RGPD.

como responsável pelo tratamento[36]. Todavia nas restantes *DLT*, verdadeiramente descentralizados em dezenas ou centenas de *nodes*/computadores, todos podem carregar dados para determinada finalidade e tratar os dados de terceiros. Nesta ordem de ideias, ou concluímos que nenhum deles se pode qualificar como responsável pelo tratamento, já que verdadeiramente inexiste um agir autónomo e independente com propósitos de tratamento, nem tão-pouco se poder dizer que eles ajam com propósitos de tratamento relativamente às informações distribuídas na rede por terceiros; ou então que todos o são porquanto nenhum deles está sujeito a instruções de terceiro no momento em que decidem carregar dados para o *ledger*[37]. Outra alternativa, seria perceber os *nodes* como responsáveis conjuntos pelo tratamento, nos termos do art.º 26.º, n.º 1 do RGPD, mas, para isso, eles teriam que determinar conjuntamente as finalidades e meios comuns de tratamento, o que realmente não acontece[38].

Os *nodes* assumem um papel efetivamente importante no tratamento de dados, já que têm total autonomia para entrar e sair da *blockchain*, escolher que dados querem fornecer etc. Todavia, o poder de decisão quanto aos objetivos do *software* não está nas mãos destes. Com efeito, é o criador de cada *blockchain* que determina o tipo de utilidade para o qual ele será requisitado (realizar registos, promover transações, gestão de propriedade e de ativos financeiros etc.). É neste contexto que surge a possibilidade de onerar os criadores dos vários *DLT's* como responsáveis de tratamento, visto que são efetivamente estes que constroem algoritmos específicos para a subordinação de determinada *blockchain* a finalidades concretas e a propósitos determinados. Mas encontrar no criador do algoritmo o

---

[36] Inclusivamente, como recomendado pelo Parecer da CNIL a respeito (2018), os responsáveis pelo tratamento nas redes de *blockchain* privadas devem ser logo identificados nos respetivos projetos (disponível em: https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf (acedido a 15/01/2019)).

[37] Esta parece ser a interpretação do Parecer da CNIL, pág. 2, disponível em https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf (acedido a 15/01/2019): sempre que: "lorsqu'il est une personne physique et que le traitement de données personnelles est en lien avec une activité professionnelle ou commerciale (c'est—à-dire lorsque l'activité n'est pas exclusivement personnelle)".

[38] Finck, Michèle. "Blockchains and Data Protection in the European Union", in *Max Planck Institute for Innovation and Competition Research Paper*, n. 18-01, p. 17, disponível em https://papers.ssrn.com (acedido a 20/01/2019).

verdadeiro responsável pelo tratamento nem por isso torna a aplicação do RGPD mais fácil: basta relembrar que o criador da *Bitcoin* (Satoshi Nakamoto) permanece até aos dias de hoje sob anonimato.

Será que os *nodes* estariam então livres de responsabilidade? Se cada pessoa que atua na rede *P2P* constitui um *node* independente; se, como visto acima, cada *node* realiza tratamentos de dados; se os usuários não podem ser qualificados como responsáveis pelo tratamento, mas ainda assim realizam tratamento de dados "em nome" destes; então teremos forçosamente de concluir que cada *node* que se conecta a uma *blockchain* pode ser qualificado como subcontratante. A ser assim, restaria perceber como é que a responsabilidade dada aos subcontratantes pelo RGPD seria aplicável numa rede como esta[39]. E é aqui que ressaltam uma série de perplexidades: (i) o fato de os *nodes* poderem encontrar-se fisicamente nos mais diversos lugares do mundo ou assumirem uma identidade encriptada pode gerar grandes dificuldades na aplicação de sanções[40]; (ii) o fato de os usuários serem apenas utilizadores de um *software* desenvolvido por terceiros, agindo manualmente segundo as instruções registadas pelos criadores daquele num algoritmo *blockchain*; (iii) o fato destes *nodes* armazenarem cópias dos dados do *ledger* nos seus computadores em versões criptografadas ou em *hashing*, que nem podem ser editados; (iv) o fato de o RGPD exigir dos subcontratantes o fornecimento de garantias relativamente à existência de recursos para implementar soluções técnicas de proteção de dados pessoais; soluções estas que lhes são passadas diretamente pelo responsável pelo tratamento via algoritmo e com o qual estes nem sequer podem interagir ou interferir em caso de necessidade para proceder a alterações às medidas já criadas. Em suma, aos olhos de um Regulamento que conceitua o subcontratante como alguém contratado para providenciar soluções técnicas

---

[39] Ramsay, Sebastian. "The General Data Protection Regulation vs. The Blockchain – A legal study on the compatibility between blockchain technology and the GDPR", *Tese de Mestrado apresentada à Universidade de Estocolmo*, 2018, pág. 48, disponível em http://www.diva-portal.org (acedido a 20/01/2019).

[40] Neste cenário, imensos *nodes* teriam de ser contatados e forçados a cumprir com as disposições do RGDP, o que num cenário normal apenas teria que ser feito perante um único responsável pelo tratamento. No final do dia, poderíamos inclusivamente a uma situação em que o próprio *software blockchain* deixaria de funcionar pela retirada forçada dos *nodes* para poderem cumprir com os direitos de um único titular de dados.