Revista de Bioética y Derecho
Perspectivas Bioéticas
www.bioeticayderecho.ub.edu - ISSN 1886-5887

DOSSIER SOBRE INTELIGENCIA ARTIFICIAL, ROBÓTICA E INTERNET DE LAS COSAS

Os desafios do RGPD perante as novas tecnologias *blockchain*

Los desafíos del RGPD ante las nuevas tecnologías *blockchain*

The challenges of RGPD in face of blockchain technology

Els desafiaments del RGPD davant les noves tecnologies *blockchain*

MARIA PAULO REBELO *

* Maria Paulo Rebelo. Doutora (C) em Direito Público pela Universidade Federal da Bahia. Investigadora Convidada pelo Max Planck Institute Luxembourg for International, European and Regulatory Procedural Law. Email: mariapaulorebelo@gmail.com.

Resumo

O surgimento de novos softwares baseados em tecnologia *blockchain* lançam novas preguntas ao novo RGPD, criticado por ter sido criado tendo apenas em vista realidades virtuais centralizadas de controlo de dados. Apesar de quer o RGPD, quer o *blockchain* desejarem objetivos comuns, como o aumento da transparência e da confiança na troca de dados online, a verdade é que em vários aspetos os desentendimentos entre ambos são reais: certas noções, como a de responsável pelo tratamento ou subcontratante, dificilmente se adequam; certos direitos, como o direito ao esquecimento ou à transferência de dados, correm o risco de perder conteúdo útil; ou mesmo certos princípios, como o da limitação de tratamento, dificilmente se compatibilizam com esta nova tecnologia.

Palavras-chave: blockchain; dados pessoais; DLT; RGPD; tecnologia.

Resumen

La creación y el surgimiento de nuevos programas informáticos basados en la tecnología *blockchain* desafían el reciente GDPR con nuevas cuestiones, ya que se le critica tener en cuenta sólo las realidades virtuales basadas en el control centralizado de datos. A pesar de que tanto el RGDP como la *blockchain* comparten intereses comunes para aumentar la transparencia y la confianza en el intercambio de datos en línea, lo cierto es que, en varios aspectos, los malentendidos entre ambos son reales: algunas nociones como la de controlador o procesador de datos, son poco adecuadas; ciertos derechos, como el derecho al olvido o el derecho a la portabilidad de los datos corren el riesgo de perder su aplicación; o incluso ciertos principios, como la minimización de datos, son difícilmente compatibles con esta nueva tecnología.

Palabras clave: blockchain; datos personales; DLT; RGPD; tecnología.

Abstract

The creation and emergence of new software based on blockchain technology challenge the recent GDPR to new questions, as it is severely criticized for bearing in mind only virtual realities based on centralized data control. Despite both RGDP 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: certain notions, such as data controller or processor, hardly adequate; certain rights, such as right to be forgotten or the right to data portability risk losing their enforcement; or even certain principles, such as data minimization, are hardly compatible with this new technology.

Keywords: blockchain; personal data; DLT; GDPR; technology.

Resum

La creació i el sorgiment de nous programes informàtics basats en la tecnologia *blockchain* desafien el recent GDPR amb noves qüestions, ja que se li critica tenir en compte només les realitats virtuals basades en el control centralitzat de dades. A pesar que tant el RGDP com la *blockchain* comparteixen interessos comuns per a augmentar la transparència i la confiança en l'intercanvi de dades en línia, la veritat és que, en diversos aspectes, els malentesos entre tots dos són reals: algunes nocions com la de controlador o processador de dades, són poc adequades; certs drets, com el dret a l'oblit o el dret a la portabilitat de les dades corren el risc de perdre la seva aplicació; o fins i tot certs principis, com la minimització de dades, són difícilment compatibles amb aquesta nova tecnologia.

Paraules clau: blockchain; dades personals; DLT; RGPD; tecnologia.

Introdução

A tecnologia *blockchain* ("cadeia de blocos") é uma concatenação de blocos, sendo cada um deles composto por um certo número de *data*, relacionados de tal modo que cada novo bloco que se acrescenta à sequência contém uma imagem criptográfica do anterior. Noutras palavras, é uma base de dados digital, partilhada e sincronizada – *distributed ledger techonoly (DLT)* – que se mantem à base de um algoritmo consensual e armazenado em diversos *nodes* (computadores/usuários). Por ser assim, esta tecnologia tem a particularidade de não poder ser manipulada a partir do momento em que a informação armazenada no bloco, pois assim que entra neste é anexada à sequência já pré-existente. Apesar do termo ser por vezes usado para identificar qualquer *distributed ledger*, independentemente de armazenar ou não dados em blocos, a verdade é que a noção de *blockchain* pode apenas designar a modalidade de DLT (*distributed ledger technology*) que efetivamente armazenam informação nos chamados blocos (*blocks*), que por sua vez são "acorrentados" ou "ligados" (*hashed*) uns aos outros numa cadeira ininterrupta (*chained*).

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 isso é possível? Cada bloco contem aspetos fundamentais da transação que ocorreu no bloco anterior e o respetivo *hash*; 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 o *blockchain* funciona numa rede descentralizada de computadores que periodicamente se sincronizam e atualizam, por forma a confirmar, repetidas vezes, que todos partilham das mesmas bases de dados, assegurando e veracidade das informações contidas na *ledger* que circula em toda a rede. São os *miners* ("mineiros") quem 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 na *ledger* ou na *blockchain*. Desta forma, quanto mais *nodes* (usuários) integrarem a rede, menos os utilizadores precisam confiar uns nos outros ou em terceiros intermediários para garantir transações seguras. Isto quer dizer que, no *blockchain*, a prova criptográfica e os algoritmos digitais substituem a confiança tradicional depositada em intermediários.

A tecnologia *blockchain* costuma dividir-se duas principais classificações: as *public blockchains*, sempre que qualquer usuário lhe pode aceder e fazer uso para efeitos transacionais; e *private blockchains*, sempre que a cadeia de blocos é controlada por uma determinada entidade

e o acesso é autorizado apenas a determinados *nodes*. Para exemplificar, podemos tomar em consideração o *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 num *public blockchain*. Em sentido contrário, os sistemas *blockchain* autorizados ou privados de processam-se como uma rede privada tipo *Intranet*, com um administrador centralizado carecendo de autorização e permissão para operar na *blockchain*.

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.* O conteúdo lançado em blocos na *ledger* pode ser encriptado, senão vejamos. A maioria dos *DLT*'s acaba por abarcar dois tipos de dados/informações: a) o *header* (cabeçado) 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, ie, os dados a serem efetivamente armazenados na *blockchain* (designado por *payload*). 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) num *distributed ledger*. Os *hash*, que são sequências criptográficas unidirecionais, não podem ser objeto de *reverse engineering,* pelo que não podemos recorrer a chaves privadas para os desencriptar; aquilo que eles permitem, pelo contrário, é verificar se determinado documento com certas características foi armazenado ou não num banco de dados e atestar a sua correspondência.

1. O novo Regulamento Geral de Proteção de Dados

À imagem e semelhança das boas práticas europeias, o Regulamento Europeu (EU 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016), que entrou em vigor no espaço europeu desde Maio, veio adotar uma técnica inicial de uso de definições para esclarecer noções fundamentais à compreensão do documento. Entre outras, destacam-se os conceitos de (i) *dados pessoais* (art.º 4º, n.º 1 do RGPD); (ii) de *dados pseudonimizados* (art.º 4.º, n.º 5 do TGPD); (iii) *responsável pelo tratamento* (art.º 4º, n.º 7 do RGPD), (iv) *subcontratante* (art.º 4.º, n.º 8 do RGPD), (v) *tratamento de dados* (art.º 4º, n.º 2 do RGPD).

Igualmente importante nos auspícios destas novas regulações, são os princípios instituídos e reforçados pelo Regulamento no espaço europeu. Entre eles destacam-se (i) o princípio da *limitação das finalidades*: qualquer dado pessoal só pode ser tratado com propósitos legítimos, concretos e determinados e sem que possam ser usados para outras ou além das finalidades recolhidas (art.º 5º, n.º 1, al. b) do RGPD); (ii) princípios da *minimização dos dados*: o

tratamento dos dados 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) o princípio dos *limites da conservação:* todos os tratamentos de 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); (iv) princípios da *integralidade*: acompanhados de medidas técnicas de proteção desses mesmos dados, que impeçam o acesso não autorizado, a perda, etc. (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 atribuir: (i) direito de *acesso* aos dados coletados (art.º 15º do RGPD), desde que feito mediante requerimento prévio; (ii) direito de *eliminação* (ou "direito ao esquecimento"), que se traduz no direito à revogação do consentimento, à destruição dos seus registos no banco de dados, ou sua total exclusão ou à oposição ao tratamento (art.º 16º e 17º do RGPD); (iii) direito à *portabilidade dos dados* (art.º 20º do RGPD), i.e., o direito solicitar ao controlador a transferência dos seus dados pessoais para outra entidade.

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

2.1. Dados pessoais

Sabemos que dados pessoais constituem qualquer tipo de informação associada a uma pessoa identificada/-ável. Sabemos também que (i) o Regulamento europeu só se aplica caso estejamos perante um dado considerado como "pessoal"; 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: *public keys* e aquilo a que se chama de *transactional data*[1].

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, há três formas de armazenar dados na *blockchain*: texto, criptografia ou *hashing*; pelo que a resposta a esta pergunta exige uma apreciação sob todas aquelas 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.

[1] FINCK, Michèle, "Blockchains and Data Protection in the European Union", in Max Planck Institute for Innovation and Competition Research Paper No. 18-01, págs. 9 ss, disponível em https://papers.ssrn.com.

Já relativamente aos dados armazenados sob a forma criptográfica, como permanece possível o seu acesso mediante o uso de uma chave privada, então não podemos dizer serem anónimos e, portanto, acabem por permitir o seu rastreamento até ao respetivo titular dos mesmos.

Por último, 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 projetado reversamente. Mas para efeitos da recente jurisprudência europeia, quer a criptografia, quer o *hashing* são uma forma de pseudonimização (e não de anonimização) de dados pessoais, já que a pessoa pode ainda ser rastreada e identificável. Ganha relevo aqui o Parecer do GT 216 (*Opinion 05/2014*) sobre o artigo 29 a respeito da diferente conceção dos dados como pseudonimizados ou anónimos.

As *public keys*, não são dados transacionáveis, mas um conjunto alfanumérico que identifica de forma pseudonimizada um usuário que pretende fazer transações ou comunicações[2]. Nos termos do 4.º, n.º 5 do RGPD, a pseudonimização corresponde ao tratamento de dados pessoais que não pode ser atribuído a uma pessoa específica sem recorrer a informações suplementares. Ora, as transações/comunicações na *blockchain* que são efetuadas através da publicação de uma chave pública (*public key*), estão irremediavelmente associadas a um *IP address*. Todavia, se por um lado é certo que esta *public key* se encontra criptografada para que se consiga um certo anonimato na operação *online*; não menos certo é que é possível identificar indiretamente a entidade/sujeito que representa aquele usuário pela reutilização daquela chave-pública e correspondente associação a determinado *IP address*[3]. 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, *ie*, para garantir que aquela operação em concreto foi efetivamente realizada por aqueles indivíduos em particular.

A ser assim, *ie*, conseguindo 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 *public keys* se qualificam como dados pessoais para efeitos da aplicação da regulamentação europeia de dados pessoais.

---

[2] 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. 41, disponível em http://www.diva-portal.org

[3] REID, Fergal; HARRIGAN, Martin, *An analysis of anonymity in the bitcoin system*, *in* arXiv:1107.4524v2, 2011; e BIRYUKOV, Alex; KHOVRATOVICH, Dimitry; PUSTOGAROV, Ivan, *Deanonymisation of clients in Bitcoin P2P network, in* arXiv:1405.7418v3, 2014; ambos disponíveis em https://arxiv.org

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

Alguns *sites* de serviços federais alemães para se protegerem de ataques *online* e permitir ações penais, guardam em registo todas as consultas (sessão, nome do sítio, ficheiro consultado, dados transferidos, indicação do endereço IP do computador do utilizador, etc.) de usuários que acedem aos seus sítios. 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. Em resposta à questão prejudicial colocada ao TJUE 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 (*dinamic IP address*), 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).

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 mesmos dados sejam armazenados *off-chain* (fora da cadeia pública), mas vinculados ao *ledger* através de um *hash*, seria possível encriptar os dados de forma segura pois estes estariam protegidos por um *hash* irreversível. No *ledger* apenas um aleatório dado 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 o fato de implicarem o chamamento de um terceiro para fazer a gestão desse banco de dados editável *off-chain*, o que acabaria por precisamente em causa o principal fator que os levaria a recorrer à *blockchain*: não depositar o controlo/confiança em entidades centralizadas.

Ao contrário daqueles, as *public key* não podem ser transferidas para fora da cadeia por serem parte integrante do funcionamento do próprio *blockchain* e necessárias para que a validação de transações possa ocorrer.

2.2. 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". Resta saber que ações são executadas nos dados que são carregados para o *blockchain* como dados pessoais. Aqui a análise uma vez mais ponderará quer as *public keys* e *transactional data*, quer os próprios *nodes*.

Para 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 dado pelo RGPD, mesmo que o tratamento seja autonomizado e se processe pela via de um algoritmo matemático, é possível de qualificar como tal esta operação de verificação da validade de transações através de chaves públicas.

No que respeita aos *transactional data*, os dados da transação são validados também através de certos algoritmos: são armazenados num determinado bloco, que é posteriormente anexado ao *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 possam ser qualificados como tratamento de dados[4].

3. Potenciais conflitos com princípios da regulação legal

Como sucede na grande maioria das vezes, os administradores de *blockchain* não controlam, nem sabem, necessariamente, que dados pessoais estão a ser inseridos na cadeia de blocos,

[4] 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. 43-44, disponível em http://www.diva-portal.org

muito menos se esses dados são ou não sensíveis. Isto porque, e como mencionámos acima, o *blockchain* apenas se revela através de *hashes* (códigos alfanuméricos). Um sistema genérico *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 sua grande diversidade de usos possíveis, os *public blockchain* acabam ter grande dificuldade em conseguir construir medidas de proteção do tipo requerido por lei. Mas será que o máximo a que podem aspirar, nestes casos, é a regulamentação privada que determinem e exijam o consentimento expresso para conseguir o respeito às políticas europeias de proteção de dados?

O RGPD surgirau num contexto em que o *blockchain* não era ainda um fenómeno no mundo digital; as suas principais preocupações centravam-se nos serviços em *cloud* e nas redes sociais, que se organizam sobretudo por sistemas centrais com as quais os usuários interagem e assume normalmente o papel de *data processor/controller*. A chegada de *public blockchains* traz consigo um sistema que foge a este mundo centralizado na medida em que funciona com protocolos descentralizados. E isto porque, nestes sistemas, toda a informação é partilhada e replicada por toda a rede, o que torna a eliminação de dados e a tutela da privacidade um verdadeiro pesadelo para os seus usuários. 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 esquecimento 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 determinada, o que dificulta a compreensão dos sujeitos obrigados às regras previstas no Regulamento, o apuramento de responsabilidades e a aplicação das respetivas sanções.

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

3.1. Direito ao esquecimento

Nestes sistemas, assim que transações são registadas na cadeira, 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 e 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, caso 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 no *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 TJUE determinou que os cidadãos da UE têm direito a remover dos motores de busca qualquer conteúdo recuperável nos índices de resultados de pesquisa. Na sua justificação, o tribunal europeu 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). Desta jurisprudência, retirou o legislador europeu o "direito ao esquecimento" para o plasmar no mencionado art. 17º e no art.º 5.º, n.º 1, al. d) do RGPD.

Naturalmente que o direito ao esquecimento 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. 17º, n.º1, al. a) do RGPD); (ii) o titular retire o seu consentimento (art. 17º, n.º1, al. b) do RGPD); (iii) o titular oponha-se ao tratamento sem que haja interesses legítimos prevalecentes que o justifiquem (art. 17º, n.º 1, al. c) do RGPD); ou (iv) tenham sido tratados ilicitamente (art. 17º, n.º 1, al. d) do RGPD). Mas independentemente disto, outros problemas práticos também 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, por não ter 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 "esquecimento" / "*erasure*". 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* uma *erasure* é tecnicamente impossível 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[5], 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 *transatctional data* e *public keys*.

Quanto aos primeiros, basta que os mesmos sejam armazenados num banco editável e criptografado de dados *off-chain*, para poder 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 no *blockchain*, requerendo a nomeação de entidades responsáveis para as administrar e os únicos com autoridade para editar a cadeia de blocos de acordo com regras predeterminadas. Por outro lado, certas características apontadas como grandes vantagens desta tecnologia, tal como a descentralização de dados *peer-to-peer*, deixarão de poder subsistir, para que se permita a compatibilização da mesma com o regramento europeu. Alternativamente, e como já vimos acima, surge ainda a possibilidade de armazenar a informação/*personal data* 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 na *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, com apenas um e unidirecional *hash* dos dados armazenados no próprio *blockchain* a que se chama de PII (*hash* de informações de identificação pessoal); é esse *hash* que servirá de ponto de referência e link para o banco de dados *off-chain*.

No que respeita às *public keys*, há quem ateste a possibilidade transferir a chave ao titular dos dados para que este se encarregue do controlo sobre os seus próprios dados, o que poderá facilmente eliminar se escolher destruir a mesma, pois ela é a única responsável por desencriptar a respetiva informação. 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. Esta solução, porém, ao confiar numa terceira autoridade/árbitro para realizar o serviço, acaba por voltar ao mesmo problema da própria essência do *blockchain* ser posta em causa.

[5] FINCK, Michèle, "Blockchains and Data Protection in the European Union", in Max Planck Institute for Innovation and Competition Research Paper No. 18-01, pág. 24, disponível em https://papers.ssrn.com.

3.2. Transferência de dados

Nos termos do disposto no art.º 3.º, n.º 1 e 2, o RGPD abrange tratamento de dados efetuados dentro ou fora da União, desde que o estabelecimento do responsável pelo tratamento ou subcontratante se encontre nele; ou, mesmo que não estabelecidos na União, quando respeitarem a residentes desta e o tratamento disser respeito à oferta de bens ou serviços ou ao controlo do seu comportamento dentro da União. Por outro lado, nos termos do art.º 44, as transferências de dados para países terceiros só são possíveis quando respeitadas um conjunto de condições, nomeadamente a existência de um nível de proteção adequado (a definir pela própria Comissão) e a existência 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 no *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 *public blockchains* uma presunção quanto à existência de *nodes* situados ou de tratamentos realizados fora do território europeu torna-se fácil de extrair. Além disso, os *miners* (mineradores), que são quem resolve 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[6]. Na falta da decisão tomada ao abrigo do art.º 45, dispõe o art.º 46 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 poder conceber alterações ao protocolo do *software* para se compatibilizar com estas condições, dificilmente tal será possível. Por ser assim, a maioria da doutrina tem vindo a apontar o consentimento explícito para a transferência dos dados a terceiros, desde que tenha sido informado dos possíveis riscos envolvidos.

[6] FINCK, Michèle, "Blockchains and Data Protection in the European Union", in Max Planck Institute for Innovation and Competition Research Paper No. 18-01, pág. 19, disponível em https://papers.ssrn.com.

3.3. Controlo sobre os dados

Outro problema de compatibilização que encontramos entre *blockchain* e *data protection regulation* prende-se com a identificação do *data controller* ("responsável pelo tratamento", *ie*, aquele que determina as finalidades do tratamento de dados e assume a responsabilidade originária por qualquer violação[7]) e do *data processor* ("subcontratante", *ie* aquela entidade que efetivamente realiza o tratamento de dados conforme instruções do *controller*). E este problema é tanto mais complexo no contexto digital do *blockchain*, quanto mais nos apercebermos de que as mesmas entidades podem assumir, simultaneamente, mais do que um papel. Apesar de ambos os papeis desempenhados não serem livres de obrigações e responsabilidades pelo RGPD, a determinação precisa de cada um não deixa de ser determinante.

Esta compreensão, mais uma vez, não pode desconsiderar as naturezas públicas ou privadas de *blockchain*. Naturalmente que no caso dos *private blockchain,* aquele que se assume destinatário dos dados enviados pelo titular pode facilmente qualificar-se como *controller*. Todavia nos restantes *distributed ledger technology*, verdadeiramente descentralizados em dezenas ou centenas de *nodes*/computadores/usuários, 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 processamento, 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*. Outra alternativa, seria perceber os *nodes* como responsáveis conjuntos pelo tratamento, nos termos do art. 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[8].

Os usuários/*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 destinados ao *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: se para realização de registos, se para a promoção de

[7] Art. 4º, n.º 7 do RGPD.

[8] FINCK, Michèle, "Blockchains and Data Protection in the European Union", in Max Planck Institute for Innovation and Competition Research Paper No. 18-01, pág. 17, disponível em https://papers.ssrn.com.

transações, se para a gestão de propriedade e de ativos financeiros, etc. É neste contexto que surge a possibilidade de onerar os criadores dos vários *DLT's* como *controllers*, visto que são efetivamente estes que constroem algoritmos específicos para a subordinação de determinado *blockchain* a finalidades concretas e a propósitos determinados. Mas encontrar no criador do algoritmo o verdadeiro *controller* nem por isso torna a aplicação do RGPD mais fácil: basta relembrar que o criador do *Bitcoin* (Satoshi Nakamoto) permanece até aos dias de hoje sob anonimato, sendo a sua identidade desconhecida[9].

Será que os usuários/*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 *controllers*, mas ainda assim realizam tratamento de dados "em nome" destes; então teremos forçosamente de concluir que cada indivíduo 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[10]. 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[11]; (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* muitas vezes 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 *controller* 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 RGPD que conceitua o subcontratante como alguém contratado para providenciar soluções técnicas ou processar dados, a qualificação dos *nodes* como *processors* perde muito o seu sentido útil.

---

[9] HODGE, M., "Who is Satoshi Nakamoto? Bitcoin inventor whose identity remains a secret", in The Sun Online, disponível em: https://www.thesun.co.uk/news/5037060/satoshi-nakamoto-bitcoin-inventor-richest-world/

[10] 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

[11] 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.

Conclusões

Conforme ficou visto acima, existem vários pontos no RGPD que precisam ser apreciados com grande cautela, quando aplicados à tecnologia *blockchain*. Depois de concluir que os dados importados para a cadeia de blocos têm necessariamente que ser considerados como dados pessoais (ainda que pseudonimizados), a sujeição deste *DLT* ao RGPD torna-se um fato inegável; independentemente de os vários *nodes* existentes na rede poderem ou não ser encontrados em espaço territorial europeu. Se assim é, e porque esta tecnologia implica o armazenamento e uso de dados por todos os usuários, a conclusão de que no *blockchain* também se processam dados não é igualmente difícil de extrair. Complicado se tornam as respostas para as perguntas a fazer depois disto. Chegámos à conclusão que certos conceitos como o de responsável pelo tratamento ou de subcontratante têm sido um dos pontos mais questionados pela doutrina especializada, precisamente por causa da complexidade em perceber (i) quem é que efetivamente desempenha qual papel e (ii) das dificuldades por detrás da cobrança do cumprimento do Regulamento a qualquer um deles. Por outro lado, vimos também um dos principais direitos consagrados no RGPD encontra-se de alguma forma posto em crise com o sistema *blockchain*; mas que, não obstante os grandes pontos de confronto que ainda têm, começa a ser possível conceber, quer por meios técnicos que modificam o algoritmo ou permitem fugas ao *ledger*, quer por meios legais que atenuam o próprio conceito legal de "eliminação" (que parece agora dever ser lido sob um enfoque atenuante de "esquecimento"), uma luz ao fundo do túnel possa vir a salvaguardar a compatibilização dos dois. Parece-nos que o ponto fundamental a ter em conta ao final deste estudo, é a questão da adequação legislativa que necessariamente se impõe a esta nova realidade virtual, que tem que ser feita com as devidas cautelas e só depois de se perceber, efetivamente, como é que a tecnologia em causa funciona.

Fecha de recepción: 4 de diciembre de 2018
Fecha de aceptación: 13 de marzo de 2019