

BITCOIN: UMA SOLUÇÃO PARA A DISTORÇÃO DO SIGILO BANCÁRIO (COMO REFLEXO DO DIREITO À RESERVA DA INTIMIDADE DA VIDA PRIVADA)?

Bitcoin: Uma solução para a distorção do sigilo bancário (como reflexo do direito à Reserva da Intimidade da Vida Privada)?

O presente artigo pretende analisar sumariamente o regime legal aplicável ao sigilo bancário e as críticas que lhe podem ser tecidas no âmbito das suas derrogações, de modo a ponderar a necessidade e a adequação de uma alternativa no que diz respeito à tutela da reserva da intimidade da vida privada dos clientes bancários. Pretende abordar-se, de forma crítica, a alternativa oferecida pela Bitcoin, analisando sumariamente a possibilidade que esta solução pode implicar (ou não) para a tutela da privacidade.

Bitcoin: A solution for the distortion to banking secrecy rules (as a reflex of the Right to Privacy)?

This article aims to briefly analyze the applicable framework to banking secrecy rules and the criticism regarding its derogations, in order to consider the necessity and adequacy of an alternative in relation to the protection of the privacy of bank customers. Bitcoin as an alternative is to be critically addressed as well as an analysis of the advantages that this solution may involve (or not) for the protection of privacy.

PALAVRAS-CHAVE

Sigilo bancário; direito à reserva da intimidade da vida privada; Bitcoin; blockchain

KEY WORDS

Banking secrecy; right to privacy; Bitcoin; blockchain

Fecha de recepción: 01-12-2019

Fecha de aceptación: 09-12-2019

INTRODUÇÃO

O direito à reserva da intimidade da vida privada, que pertence a todos os indivíduos na qualidade de titulares de um direito geral de personalidade, encontra-se hoje em discussão, não na sua existência inegável, mas na sua extensão, na medida em que se questiona o bem jurídico a tutelar e a melhor forma de o fazer. É neste contexto que se estabelece uma relação lógica entre o direito à reserva da intimidade da vida privada e o sigilo bancário. Mas que relação existirá entre esta realidade e a *Bitcoin*? O leque de informações transmitidas a uma instituição financeira (especialmente a um banco) é de uma amplitude muitas vezes desconhecida, particularmente tendo em conta os avanços tecnológicos que facilitam o fluxo de informações –como será exemplo a nível nacional o MB WAY– e permitem que praticamente qualquer transação, por valor mais ínfimo que tenha, se possa fazer imediatamente através de uma transferência bancária. Não é, por isso, de estranhar que os bancos possuam registos cada vez mais detalhados de todas as transações que são realizadas pelos seus clientes, desde valores gastos, locais, período temporal, bens ou serviços adquiridos, etc, permitindo, desta forma, um maior rastreamento dos fluxos financeiros entre contas bancárias e um maior conhecimento do perfil de clientes que existem em cada instituição.

Se é verdade que, por um lado, a informação detida

pelos bancos sobre os seus clientes e as suas transações não constitui, à partida, um problema, já que a mesma se encontra tutelada pelo sigilo bancário, por outro, o regime atualmente aplicável apresenta algumas vicissitudes, desde logo ao nível das derrogações, que podem colocar em causa o direito à reserva da intimidade da vida privada dos clientes, especialmente se tivermos em conta que, como afirmado no Acórdão n.º 278/95 do Tribunal Constitucional, de 31 de maio, “*uma conta corrente pode constituir a biografia pessoal em números*”.

O objetivo deste artigo é o de tentar encontrar uma possível resposta para a tutela efetiva da reserva da intimidade da vida privada dos clientes bancários através de uma inovação tecnológica, a *Bitcoin*, que tem, na sua base, uma tecnologia igualmente inovadora: a *blockchain*.

REGIME LEGAL DO SIGILO BANCÁRIO

O sigilo bancário pode ser definido como a discrição que os bancos devem observar, através dos seus órgãos e empregados, sobre os dados económicos e pessoais dos clientes, dos quais tenham tido conhecimento através do exercício das respetivas funções (Noel Gomes, *Segredo Bancário e Direito Fiscal*, Almeida, pág. 19). Daqui resulta que todos os agentes das instituições de crédito não possam revelar ou aproveitar-se de informações cujo conhecimento lhes

advenha, exclusivamente, por virtude do exercício das suas funções. Do mesmo modo, impede que terceiros tomem conhecimento de tais informações, na medida em que o procurem ativamente, vedando, por conseguinte, o acesso, a divulgação e a utilização indevida de tais dados (Rabindranath V.A. Capelo de Sousa, *O Direito Geral de Personalidade*, Coimbra Editora, pág. 332, nota 834).

A proximidade entre o sigilo bancário e o direito à reserva da intimidade da vida privada é notória, na medida em que o sigilo bancário tem por objetivo tutelar, no âmbito da atividade bancária, a parcela da vida privada que é exposta perante uma instituição de crédito e que integra zonas pessoais, profissionais e económicas.

O dever de segredo encontra-se expressamente previsto no artigo 78.º do Regime Geral das Instituições de Crédito e Sociedades Financeiras (Decreto-Lei n.º 298/92, de 31 de dezembro, conforme alterado) (“RGICSF”), e refere que “*os membros dos órgãos de administração ou fiscalização das instituições de crédito, seus colaboradores, mandatários, comissários e outras pessoas que lhes prestem serviços a título permanente ou ocasional não podem revelar ou utilizar informações sobre factos ou elementos respeitantes à vida da instituição ou às relações desta com os seus clientes cujo conhecimento lhes advenha exclusivamente do exercício das suas funções ou da prestação dos seus serviços*”. Este mesmo artigo providencia também um leque meramente exemplificativo das informações sujeitas ao dever de segredo, desde logo “*os nomes dos clientes, as contas de depósito e seus movimentos e outras operações bancárias*”, concluindo ainda que “*o dever de segredo não cessa com o termo das funções ou serviços*”. A violação do dever de segredo é punível nos termos dos artigos 195.º e 196.º do Código Penal, sem prejuízo de outras sanções, de natureza civil, disciplinar ou contraordenacional que possam ser aplicáveis.

O artigo 79.º do RGICSF prevê, por outro lado, várias derrogações ao sigilo bancário que permitem aos bancos revelar informações que seriam, em princípio, reservadas. Estas exceções ao dever geral de segredo justificam-se, desde logo, quando existe consentimento do cliente para a divulgação, mas também, por exemplo, quando existem motivos de ordem pública (designadamente de combate ao branqueamento de capitais, financiamento do terrorismo e evasão fiscal) que implicam uma compressão do direito à reserva da intimidade da vida privada dos clientes bancários. E se é legítimo considerar que o direito à reserva da vida privada dos clientes ban-

cários não é absoluto, devendo naturalmente ceder quando outros interesses legítimos se sobreponham, pode levantar dúvidas a questão de saber se o regime atualmente aplicável não prevê um número excessivo de exceções e, ainda, se a extensão destas – tendo em conta a intromissão na vida privada que permitem –, não será ela mesma excessiva. Este ponto é particularmente relevante se considerarmos que para além das exceções ao sigilo bancário previstas no RGICSF, existem também outras derrogações, por exemplo, no âmbito do Direito penal ou do combate ao branqueamento de capitais sendo de particular relevância as que dizem respeito à fiscalização tributária. A Lei Geral Tributária (Decreto-Lei n.º 398/98, de 17 de dezembro, conforme alterada) (“LGT”) prevê um elenco muito amplo de situações de derrogação ao sigilo bancário aplicáveis à atividade da Autoridade Tributária –especialmente quando se trata de apurar a situação tributária dos contribuintes–, que se serve de um conjunto de regras especificamente previstas naquele diploma para aceder à informação que se encontra na posse dos bancos e demais instituições financeiras para exercer os seus poderes de investigação, averiguação e inspeção no sentido de tornar mais eficaz o combate à evasão fiscal.

Não obstante esta amplitude de poderes, a falta de cooperação com a Autoridade Tributária pode ser legítima em determinadas situações, nomeadamente quando as diligências pretendidas impliquem a violação dos direitos de personalidade ou quando importem o acesso a facto da vida íntima dos cidadãos (artigo 63.º, n.º 5, alíneas c) e d) da LGT), sendo que nestes casos as diligências da Autoridade Tributária apenas se podem realizar mediante autorização judicial com base em pedido fundamentado da administração fiscal. Apesar desta previsão, a verdade é que a amplitude das derrogações ao sigilo bancário no domínio fiscal pode suscitar dúvidas quanto à sua proporcionalidade, especialmente se considerarmos que o combate à evasão fiscal pode muitas vezes ser de difícil concretização e abranger um número indeterminado de pessoas, originando uma verdadeira distorção ao regime do sigilo bancário. Veja-se, a este propósito, a Lei n.º 17/2019, de 14 de fevereiro que prevê a possibilidade de a Autoridade Tributária aceder a todas as contas bancárias com um saldo superior a € 50.000,00.

A BITCOIN COMO SOLUÇÃO ALTERNATIVA?

É no contexto acima descrito que importa refletir sobre uma alternativa ao sigilo bancário que possa

salvaguardar os cidadãos na sua intimidade no âmbito de transações financeiras e bancárias. Destaca-se, assim, uma alternativa não jurídica que nasce da realidade que lhe está subjacente: a Bitcoin.

A *Bitcoin* surgiu com um intuito revolucionário, disruptivo, de ser uma alternativa ao sistema bancário tradicional, procurando soluções para as fragilidades apresentadas, desde a falta de proteção que é concedida às informações pessoais que são divulgadas no âmbito das derrogações ao sigilo bancário, bem como o uso abusivo que, em certos cenários, pode ser feito das mesmas. Procuraremos analisar neste capítulo a viabilidade desta alternativa.

A *Bitcoin* pode ser definida como uma versão de dinheiro eletrónico, puramente *peer-to-peer* (ou seja, com base numa relação que se estabelece diretamente entre as partes que realizam determinada transação financeira), que permite fazer pagamentos *online* sem carecer ou passar por uma instituição financeira ou qualquer outro tipo de intermediário encarregue do tratamento das informações que permitem as transações bancárias (António Vilaça Pacheco, Editora Self, *Bitcoin*, pág. 26), tornando desnecessário o fornecimento de praticamente qualquer informação pessoal à rede *peer-to-peer* que é composta pelo conjunto de utilizadores deste meio alternativo de realização de transações. Se o modelo tradicional centralizado de controlo (*centralized network*) parte do pressuposto que as partes não confiam entre si e, por essa razão, são os bancos o elo de ligação e o garante da legitimidade das transações, o sistema distribuído de *blockchain* em que assenta a *Bitcoin* (*distributed network*) funciona numa base de interligação de todas as partes que compõem a rede *peer-to-peer*, sem a intervenção de uma entidade central que controla e regista todos os movimentos financeiros, sendo que todos os intervenientes da rede *peer-to-peer* têm a função de verificar a veracidade das transações e são responsáveis pela segurança da rede.

A tecnologia de *blockchain* é baseada em algoritmos criptográficos que garantem a integridade e a legitimidade de cada transação e é constituída por uma cadeia de blocos que contêm em si um conjunto de informações. No caso das transações financeiras, cada bloco contém um histórico de transações e um *hash* que funciona como um identificador para garantir que determinado bloco é único, bem como um *hash* de todos os blocos anteriores, para garantir que todos os blocos de uma determinada transação estão ligados entre si. Assim, cada novo bloco que compõe a *blockchain* contém informação sobre a

transação e dois *hash*, um relativo ao próprio bloco e outro *hash* de todo o histórico. Os blocos de uma determinada transação são partilhados e validados pelos próprios participantes da rede (*nodes*), incluindo o histórico de todas as transações válidas. Ou seja, após verificada a validade de determinado conjunto de dados pelos *nodes*, as transações a que os mesmos se referem são registadas num “bloco” que é anexado sequencialmente ao bloco anterior de transações. É importante referir que a partir do momento em que as informações são gravadas na *blockchain*, as mesmas não podem ser editadas ou excluídas. O resultado é uma longa cadeia de blocos (ou *blockchain*) que representa toda a cadeia de transações desde o *genesis block* (Primavera de Filippi, e Aaron Wright, *Blockchain and the Law*, Harvard University Press, págs. 33 a 45). Resumidamente, a *blockchain* mais não é do que um registo completo e descentralizado, baseado em criptografia de incentivos económicos e mecanismos de consenso, que permitem a validação da integridade e legitimidade de cada transação, de informação imutável, replicada e distribuída por cada membro da rede *peer-to-peer*.

Contrariamente ao atual modo de funcionamento dos bancos, em que a informação é confidencial e a identidade dos clientes é conhecida, a *blockchain* funciona de modo diverso, onde a informação é transparente, sendo a identidade dos membros da rede reservada. Isto acontece através da criação de um pseudónimo, em que a parte não será identificada através do seu nome mas pela sua chave pública (sendo que cada utilizador terá também a sua chave privada, que será secreta, e lhe permitirá transacionar as suas *Bitcoins*). Este é um dos pontos mais importantes desta tecnologia, pois permite que transações efetuadas com *Bitcoins* sejam realizadas num regime em que é apenas necessário confiar na rede e na tecnologia criada por esta. Naturalmente que uma solução deste tipo, sem supervisão por parte de uma entidade central, também acarreta problemas, se pensarmos, por exemplo, na utilização que pode ser feita destas redes para a criação de mercados paralelos ilegais.

Como já referimos acima, apesar de os sistemas centralizados apresentarem garantias de confiança na supervisão de uma entidade terceira (i.e., os bancos ou outras instituições financeiras), não é despidendo referir que estas entidades agregam nos seus sistemas, porque isso mesmo é essencial para o seu funcionamento, uma grande quantidade de informação relativa a dados pessoais dos seus clientes e que, muitas vezes, esta informação pode ser

explorada de forma ilícita (por exemplo, por terceiros não autorizados) ou contrária aos fins para os quais foi recolhida. Por outro lado, a complexidade das regras aplicáveis ao próprio sistema bancário e o grau relativamente baixo de literacia da generalidade dos clientes bancários, origina uma opacidade sobre a sua forma de funcionamento que pode subverter a lógica de confiança que lhe está subjacente.

O sistema descentralizado opera sob o princípio basilar da transparência, por oposição ao princípio da confiança do sistema centralizado, numa lógica de que a única forma de obter coordenação entre todas as partes é através da disponibilização de toda a informação necessária por parte dos *nodes*. Assim, a transparência pode ser vista como uma forma de autocontrolo da própria rede, permitindo que os utilizadores verifiquem coletivamente a legitimidade de cada transação. Esta necessidade de transparência é particularmente evidente no caso da tecnologia de *blockchain* em que assenta a *Bitcoin*, onde cada transação é divulgada publicamente à rede para que possa ser simultaneamente verificada e validada por todos os *nodes* (tendo em conta que existem diferentes tipos de *blockchains*, que podem variar, nomeadamente, quanto à modalidade de acesso às informações, se a todos os participantes da rede ou apenas a alguns). Por outro lado, a identidade dos utilizadores das transações efetuadas com recurso às *Bitcoins* parece salvaguardada no sistema descentralizado por recurso a um pseudónimo.

Apesar de todas as vantagens apresentadas pelas *Bitcoins*, a verdade é que considerar esta solução como uma alternativa sustentável ao sistema centralizado e às regras que ali existem, em particular as regras aplicáveis ao sigilo bancário, não parece também isenta de críticas. Isto porque se a proteção das informações pessoais, e consequentemente da reserva da vida privada dos seus utilizadores, parece mais garantida à partida, a verdade é que a abertura e a transparência de uma rede descentralizada também tornam a informação mais vulnerável à apropriação de terceiros. Acresce que a utilização de um pseudónimo para a realização de transações com *Bitcoins* apenas significa que a identidade da(s) pessoa(s) associada(s) a essa fonte ou destino específico não pode ser facilmente estabelecida, não sendo impossível a sua identificação, sendo já hoje possível, através de complexos métodos de processamento de uma enorme quantidade de dados (*big data*), determinar, se necessário ou desejado, a identidade por detrás de um pseudónimo.

Neste contexto, conjugando a possibilidade de identificação do utilizador e o facto de *toda* a sua informação ser visível a *toda* a rede de *blockchain*, a reserva da intimidade da vida privada de cada um poderá ficar gravemente comprometida, na medida em que o sistema descentralizado em que assentam as transações efetuadas com *Bitcoins* permite um conhecimento bastante mais generalizado de informações de natureza pessoal do que aquela que resultaria das derrogações ao sigilo bancário. Significa isto que, embora se possa criticar que as derrogações ao sigilo bancário possam ser, por vezes, excessivas, a verdade é que a exposição dos utilizadores de *Bitcoins* (ao abrigo do princípio da transparência) pode, em última análise, prejudicar em maior medida - em vez de promover - a sua privacidade e ser mais gravosa para o seu direito à tutela da reserva da intimidade da vida privada do que aquela que resulta da sua compressão em virtude da aplicação de derrogações ao sigilo bancário. Isto porque apesar de estarmos, em ambos os casos, perante uma divulgação de informação protegida, a disseminação da informação dos utilizadores de *Bitcoins* em contexto descentralizado é muito superior àquela que é compreendida com as derrogações ao sigilo bancário.

CONCLUSÃO

As evoluções tecnológicas que caracterizam o nosso tempo apresentam uma dupla face de inquestionáveis méritos aliados a novos problemas frequentemente imprevisíveis. Se o sigilo bancário e as suas derrogações são uma criação jurídica e a *Bitcoin* foi pensada como uma solução fora do Direito para os casos em que importa proteger e acautelar a privacidade dos clientes bancários, especialmente nas situações em que as derrogações podem revelar-se excessivas tendo em conta o bem jurídico que pretendem proteger, parece-nos de concluir que o recurso a *Bitcoins* não deve ser aceite como alternativa viável ao sistema tradicional das transações financeiras controladas e levadas a cabo pelos bancos, porque ficou demonstrado que esta alternativa é incapaz de cumprir adequadamente o papel que para si proclama. Neste contexto, importa realçar que qualquer alternativa ao regime do sigilo bancário, conforme atualmente configurado, teria efeitos nefastos imediatos, especialmente se considerarmos que as soluções existentes, em particular a que foi abordada no presente artigo, não estão ainda regulamentadas, o que significaria que os interesse públicos e privados que se pretendem tutelar com o regime atualmente vigente ficariam certamente

mais desprotegidos e mais sujeitos a um nível de discricionariedade na sua ponderação em relação ao que é atualmente concedido pelas regras existentes.

Relativamente ao direito à reserva da intimidade da vida privada, mesmo considerando que se verifica, em algumas situações legalmente previstas, uma excessiva compressão do mesmo, a sua proteção

não será atingida pela utilização de *Bitcoins*, pois, como se pretendeu demonstrar, esta solução poderá representar um risco de violação do “*right to be let alone*” comparativamente mais gravosa do que aquela que se verifica nas situações de derrogação da obrigação de segredo.

JOANA MOTA E EVA DALE (*)

(*) Advogada e advogada estagiária na Uría Menéndez Proença de Carvalho (Lisboa).