

DIREITO À CRIPTOGRAFIA COMO DIREITO FUNDAMENTAL?

Victor Hugo Pereira Gonçalves¹

Sumário: 1. O Sigilo: o conceito e técnica de esconder coisas e pessoas; 2. Segredo: o reconhecimento do eu; 3. Privacidade: reação às disciplinas e saberes; 4. Direito à Criptografia como Direito Fundamental? 4.1. Integridade, Autenticidade e Confiabilidade: A Criptografia como Tecnologia da Transparência; 4.2. Criptografia como Direito à Memória do Esquecimento? 5. Referências Bibliográficas.

Existem muitos estudos sobre as interconexões entre direito e tecnologia. Nestes estudos existem análises mais tecnológicas, outras mais jurídicas, mas sem compreender efetivamente como elas se entrecruzam, se complementam, se retroalimentam. O estudo eminentemente interdisciplinar deve buscar as aproximações e afastamentos contínuos entre estes conceitos, suas definições e suas práticas. Nas relações entre direito e tecnologia, envolvem-se outras práticas relacionadas aos modelos econômicos da sociedade, sua história e cultura, que interferem no entendimento dos fenômenos que se pretendem compreender. Deve-se reconhecer atualmente a existência de um sujeito/cidadão digital que se constitui de práticas tecnológicas e jurídicas de ampliação do seu empoderamento numa configuração revista e remodelada. O cidadão deve ser recolocado como centro do processo de produção de seus dados, informações, memórias e esquecimentos. Somente assim, possuindo autonomia legal e tecnológica, o cidadão ilumina-se pelas práticas de formação de verdades sobre si e com os outros, estabelecendo conexões e referências mais fidedignas com uma realidade mais controlável, palpável.

Deve-se permear a análise das mudanças estruturais da sociedade com base na ideia dos pluralismos jurídicos. Apoiar-se em maiores camadas de direitos a serem manipulados diretamente pelo cidadão digital e, mediatamente, com base no modelo tradicional que depende do aparato do direito estatal para garantir a proteção deste cidadão. O exercício

¹ Bacharel em Direito pela Pontifícia Universidade Católica de São Paulo – PUCSP (2004), em História pela Universidade de São Paulo – USP (2005), Professor da FATEC Carapicuíba em Direito Empresarial (2006-2008) e Segurança Empresarial. Pesquisador do Grupo de Perícia Forense em Sistemas Informatizados do CnPq. Vice-Presidente da Comissão de Responsabilidade Social da OAB/SP (2006-2008). Professor do INFI FEBRABAN (2015). Perito do IBRAPPI – Instituto Brasileiro de Árbitros e Peritos em Propriedade Intelectual. Mestre em Direitos Humanos pela Faculdade de Direito da Universidade de São Paulo (USP). Doutorando em Direito Comercial pela Faculdade de Direito da Universidade de São Paulo (USP).

dos direitos seria viabilizado pelos meios tecnológicos diretamente manuseados pelo cidadão digital, que acessaria, controlaria, distribuiria e gerenciaria os seus dados e informações.

Da liberdade de poder acessar e gerenciar os seus arquivos de memória, torna-se questão importante analisar a condição de veracidade deles. Não é porque o cidadão digital tem o controle das tecnologias que isto se realiza de forma fidedigna ou relacional ao que está sendo retratado no arquivo memória. Mais especificamente, o que garante que aquele arquivo memória representa uma atualidade? E o que está se protegendo naquele arquivo memória? Assim, criam-se dois movimentos de forças, direções e relações diferenciadas, o que não significa que sejam contrários, e que devem ser expostos e analisados. Por mais empoderado que o cidadão digital seja, ele pode não possuir as condições cognitivas para entender e compreender o que o envolve e as significações das tecnologias de informação e comunicação, os seus processos, os seus *softwares* e *hardwares* e seus pressupostos de validade, autenticidade e confiabilidade. A partir do conhecimento distanciado do objeto, percebe-se que o cidadão digital se desloca para o espaço do segredo, daquilo que, mesmo tendo acesso direto, não compreende o significado do que está manuseando. Por outro lado, o cidadão digital, ao ter o controle direto das ferramentas tecnológicas, pode estabelecer regras de segredo e sigilo para o acesso aos seus arquivos memória, o que impediria, em tese, o acesso por terceiros, resguardando-os. Contudo, as suas regras de segredo e sigilo poderão estar sobrepostas a um meio que, talvez, seja ao cidadão inacessível ou construído por meio de sistemas que lhe são inviáveis de verificação de seus pressupostos de autenticidade, confiabilidade e validade.

É neste processo contínuo de segredos e sigilos construídos no entorno e pelo cidadão digital que se deve entender o sentido das tecnologias de informação e comunicação. A ideia não é fazer um apanhado das tecnologias existentes e demonstrá-las. Longe disto. Entender o sentido das tecnologias é mostrar as suas possibilidades axiológicas de transformar, constituir e sujeitar os cidadãos digitais. Ao final, após inúmeros questionamentos, recorrentes e reiterados, formatar uma moldura de direitos, desenvolvidas a partir dos conceitos de memória, esquecimento e verdade.

Houve, por conta das tecnologias de informação e comunicação, um interesse ainda maior em relação ao sigilo, o segredo e, principalmente, à privacidade, em razão das possibilidades infinitas de se amealharem informações e dados sobre os sujeitos sem que eles saibam. Contudo, as técnicas de vigilância não são novidades nem surgiram com estas tecnologias de informação e comunicação atuais. As técnicas de vigilância foram sendo

aperfeiçoadas por meio de práticas sociais, religiosas, econômicas e culturais, a partir da reificação de costumes, tradições, discursos, interdições, oposições e exclusões.

Contudo, estes deslocamentos não foram somente motivados por alterações tecnológicas, e sim são uma parte de um processo histórico e social mais amplo e complexo. A noção de distinção entre vida privada e vida pública sempre existiu. O efeito desta distinção, historicamente contextualizada, é que aumentava ou não a força da vida privada em favor da pública ou vice-versa.

Por uma série de fatores, muitos deles ligados a própria sobrevivência do núcleo social, historicamente, sempre se entendeu que o indivíduo deveria ser obliterado, quase que totalmente, em favor da *res publica*. A necessidade da força de todos, principalmente em momentos de caos e invasões constantes por outros povos, forçaria uma mitigação da individualidade em face do interesse público.

Mas isto não significa que não existia vida privada do indivíduo. Sócrates em seu julgamento já fazia a distinção entre vida pública e vida privada². Em *Oeconomicus*, Pseudo Xenofonte reconhece estas diferenciações entre o privado e o público e constrói a economia e os procedimentos que devem ser desenvolvidos no lar de um cidadão grego. Dentre outros ensinamentos, Xenofonte institui que cabe ao homem a organização da vida fora do lar e à mulher a administração da vida privada, os quais são funções delimitadas e definidas, a fim de gerar prosperidade³. Aristóteles entendia que o povo era unido por uma ética universal em que o indivíduo só poderia existir socialmente integrado.

A estas concepções de recrudescimento ou não da vida pública em relação à vida privada que foram se desenvolvendo com seus avanços e retrocessos, com seus deslocamentos, e acabaram por desembocar em concepções diferentes, ao longo da história e por vários povos, perspectivas do que seria sigilo, segredo e, por fim, privacidade.

² “— Olha — retorquiu Sócrates — se esse caminho, tal como não passa nem pelo comando nem pela escravatura, também não passasse pelo meio dos homens, o que tu dizes poderia estar certo. Só que, se vivendo no meio dos homens, não estás interessado nem em governar, nem em ser governado, nem em servires de livre vontade aqueles que governam, parece-me que deves ter em conta que os mais fortes sabem servir-se dos mais fracos como escravos, maltratando-os quer na vida pública quer em privado. Ou não te apercebes como eles colhem os cereais que outros semearam e cortam as árvores que outros plantaram e cercam por todos os meios aqueles que são mais fracos e que não estão dispostos a servi-los, até os terem persuadido a preferir a escravatura a uma guerra contra os mais fortes? E, por sua vez, na vida privada, não sabes que os corajosos e os poderosos escravizam e tiram proveito dos cobardes e sem recursos?”. (Xenofonte, 2009, p. 118)

³ No prefácio da obra *Econômico*, Anna Lia Amaral de Almeida Prado ressalta a separação para Xenofonte de vida pública e vida privada: “Enquanto a pólis é o âmbito do político e do público, *oikos* é o âmbito do privado, o espaço em que o indivíduo age como membro de uma família e, como tal, defende seus interesses particulares, tendo deveres a cumprir em relação aos membros de sua família, às suas tradições e também em relação aos seus bens. Nesse sentido, como membro de uma família, o indivíduo insere-se em seu *oikos* como o cidadão em sua pólis e assim pode-se dizer que o indivíduo está para o seu *oikos* assim como o cidadão está para sua pólis”.

Há que se diferenciar e pontuar os usos e conceitos destas três palavras, tanto em seu caráter cronológico como epistemológico. Sigilo e segredo são conceitos desenvolvidos a partir de práticas sociais, econômicas, culturais, históricas e tecnológicas, que não interferem na concepção e desenho do que seja vida privada ou vida pública. Somente com o desenvolvimento do conceito de privacidade que o grande campo indiferenciado, interconectado e nebuloso, construído por estes duplos conceitos segredo-sigilo e vida privada e vida pública, tornam-se mais definidos e visíveis.

A partir destes cruzamentos, deve-se construir um caminho que se possa responder as seguintes indagações: como o sigilo, o segredo e a privacidade estão definindo e remodelando sujeitos digitais? Existem possibilidades para estes conceitos funcionarem em toda a sua potência e viabilizarem direitos? Nas suas contradições e complementariedades, sigilo, segredo e privacidade enredam que tipos de combates e lutas? Para caminhar nos enfrentamentos destas indagações há que se construir os deslocamentos destes conceitos que, não raro, são utilizados, equivocadamente, como sinônimos ou semelhantes. Na grande profusão de obras e estudos publicados nos últimos anos, é recorrente a falta de cuidado metodológico e conceitual para diminuir as borras indistintas que unem estas ideias arqueológica e genealogicamente distintas, com consequências próximas, mas que não são iguais ou autorreferentes. Faz-se necessário apontar estas dubiedades e construir um caminho que o conhecimento não fique tão distante do que é a realidade das práticas, dos usos sociais e dos valores que deverão ser protegidos através das ideias de sigilo, segredo e privacidade.

1. O Sigilo: o conceito e técnica de esconder coisas e pessoas

O sigilo é um conceito inerente a uma condição humana civilizatória decorrente do deslocamento de uma estrutura nômade para uma sedentária, fixa, estável. Não é concebível uma ideia de sigilo em sociedades comunitárias, abertas e coletoras. O sigilo é fruto de um processo de isolamento, de solidão e do ensimesmar humano.

As práticas do sigilo atingem dois aspectos da condição humana: afastar as prescrições sociais, morais e jurídicas; e manter, sub-repticiamente, a diversidade e a pacificação social. As análises teleológicas acabam por olvidar deste direcionamento do sigilo como requisito importante para o desenvolvimento social, qual seja, a utilização do sigilo como ferramenta de empoderamento e enfrentamento da dominação, do pensamento harmonizante, daquele conhecimento do óbvio. É nesta função positiva que o sigilo foi utilizado ao longo da

História: como luta de existência e de reconhecimento. O sigilo é ferramenta de combate de um saber que produz diferenciações, iniquidades e acessos diferenciados da e sobre uma realidade. Ao enfrentar estas diferenciações, a prática do sigilo acaba por realizar as transformações no meio ambiente social e da natureza.

Impõe-se, diante destes desafios, para implementação do sigilo, uma nova arquitetura da existência, uma ampliação do sentido espaço-temporal para além do seu núcleo presente. O sigilo, a partir do seu recorte estrutural e da comunicação segmentada, produz um presente sempre passado a ser descoberto no futuro. Uma ideia sempre em suspensão, deslocada e fugidia de uma dominação.

A despeito de muitos doutrinadores crerem que a informação na sociedade esteja somente relacionada com práticas existente e criadas no séc. XX, num total desvario histórico metodológico, olvidam de que a troca de dados e informações ocorre desde a invenção do conhecimento e da criação da cultura. A linguagem e, posteriormente, a informação como valor, impulsionou o desenvolvimento social e econômico dos homens. Reflexo destas práticas sociais, históricas, econômicas e tecnológicas é a consolidação do conceito de sigilo com fulcro em manter algo ou alguém escondido ou longe do alcance de outrem, o que pode envolver coisas, pessoas ou ideias. O sigilo refere-se, por isto, ao externo do homem que não deve ser conhecido somente àquele escolhido ou escolhidos, o que pode envolver autoria, conteúdo e destinatário do que está a se resguardar. O entendimento desta perspectiva do que é sigilo, e que não raro é motivo de polissemia, diferencia-o do que seja segredo e privacidade.

A prática do sigilo fundou-se através de modos e meios variados, somente tornando-se viável por meio da virtualização (linguagem) e com técnicas de prestidigitação de pessoas e coisas. Há algo de mágico na arte e práticas do sigilo, pois o não conhecer os meios e modos de carregar a informação ou coisa instiga e produz expectativas por desvelar algo escondido ou escamoteado em determinada situação ou conhecimento. Neste desdobramento do etéreo, torna-se mais fácil ocultar, gerar expectativas, construir novas narrativas, verdades. O sigilo faz surgir inúmeras verdades em relação ao mesmo fato, que não são meias verdades⁴, pois é um ocultamento proposital de uma situação, a fim de preservar e congelar presunções sociais.

⁴ Neste ponto, penso no livro de Foucault, *A Verdade e as Formas Jurídicas*. Foucault, ao investigar o surgimento do inquérito na Grécia Antiga, por meio da obra de Sófocles, *Édipo-Rei*, estabelece uma nova visão sobre as relações instituídas na investigação criminal para descobrir se Édipo matou ou não o seu próprio pai, Lalo. Ao desenhar os saberes poderes instituídos nestas relações construídas, consegue Foucault determinar que a investigação, diferentemente de outras formas mais usuais na Grécia, é feita através de meias verdades que nos

Assim, o sigilo é ferramenta para preservar, construir e definir identidades de pessoas que carregam informações ou dados importantes sobre algo ou alguém, o que vai além de uma concepção de espião ou espionagem. O sigilo, neste ponto, amalgama-se com a dignidade humana. Neste aspecto, instrumentalmente, manter em sigilo a autoria e o conteúdo torna-se crucial para o fluxo contínuo do tráfego de coisas e informações sem que se saiba a origem, aumentando a confiança entre as partes numa relação pessoal, emotiva ou profissional.

O sigilo tornou-se uma necessidade historicamente construída em face dos benefícios percebidos nas relações humanas quando elas eram mantidas longe do alcance de outras pessoas. Não se pode determinar se a prática do sigilo instituiu determinadas consequências sociais ou foi um resultado das prescrições morais, de comportamentos e de condutas. Ao se conectarem estas expectativas em relação aos comportamentos e os valores que foram sendo criados, principalmente como forma de vigilância e coesão social, define-se uma linha do que é normal e atribui-se ao desviado o rótulo de não “desejável”. Para se evitar o desagrado e perseguição social do diferente, do anormal, a apropriação da ferramenta e do conceito de sigilo impulsiona a autodeterminação e a dignidade humana, o que afasta o alcance de sanções sociais, morais e até penais. Neste aspecto, o sigilo, em seu direcionamento privado, é parte crucial em busca de um reconhecimento social e da construção da dignidade. Daí a importância histórica do juramento de Hipócrates em reconhecer no sigilo uma condição de realização dos valores do ser humano: “Àquilo que no exercício ou fora do exercício da profissão e no convívio da sociedade, eu tiver visto ou ouvido, que não seja preciso divulgar, eu conservarei inteiramente secreto”.

Como extensão do governo de si, o sigilo espraia-se para o governo dos homens, reluzindo-se nas práticas governamentais. As teorias de Estado construídas no curso histórico sempre resvalaram ou admitiram o sigilo como ferramenta indissociável de um governo estatal e de si. A ideia do sigilo e de seu antônimo conceitual, a transparência, permeiam todas as teorias de Estado desenvolvidas até hoje e perpassam os conceitos de memória, esquecimento e verdade. O sigilo é a memória suspensa, mas não esquecida, que revelará algo, num futuro, moldando-se verdades até a sua revelação, cujo processo reinicia-se continuamente. De Maquiavel até Bobbio moldaram-se inúmeras teorias

são dadas pelos Deuses, pelos reis e pelos escravos, até chegar a certeza da verdade inteira: de que Édipo havia mesmo matado seu pai e casado com sua mãe. No caso do sigilo, uma certa verdade já é conhecida por inteiro a priori. Ela não é construída, é omitida.

de Estado dentro de perspectivas em que o sigilo é método governamental. Para Hanna Arendt, aliás, o conceito de sigilo está intrinsecamente ligado somente à teoria do Estado:

“Sigilo – diplomaticamente chamado de ‘discrição’ e de *arcana imperii* (os mistérios do governo) – e embuste, ou seja, a falsidade deliberada e a mentira descarada, são usadas como meios legítimos para alcançar fins políticos desde os primórdios da história documentada”. (2004, p. 15)

Hannah Arendt, de maneira bem enfática, determina que o sigilo é uma forma de embuste ou mentira. Num certo sentido pode ser direcionado o sigilo a este aspecto negativo, somente se analisarmos pelo viés moral de uma determinada posição. O sigilo constitui-se, além de uma prática social, de uma estratégia de luta e de combate se pensarmos ele em política como a guerra por outros meios⁵. Assim, dentro desta perspectiva de guerra, o Estado possui e produz informações que ele não pode ou quer compartilhar com todos os cidadãos nem com outros Estados. Ter acesso a informações privilegiadas pode dar vitórias em batalhas, gerar mais lucros em negócios, produzir vantagens sociais e econômicas para o povo ou, principalmente, para a sua elite, pois está embutido no sigilo um custo, que não pode ser suportado pelos mais pobres.

Com as tecnologias de informação e comunicação, ampliou-se, qualitativa e quantitativamente, o fluxo de informações e dados, impulsionando a importância do sigilo, não só como instrumento do Estado, mas também relacionando-se com os valores e direitos de acesso e a liberdade de informação, liberdade concorrência e iniciativa, liberdade de expressão, manifestação do pensamento, liberdade de associação etc. O sigilo implementaria, positivamente, estes direitos fundamentais trazidos, bem como outros que a ele estão interligados, tal como o sigilo profissional, sigilo das telecomunicações, sigilo bancário etc. Neste direcionamento, o sigilo interconecta-se diretamente com os direitos fundamentais, devendo ser pensado como complementar ao direito à privacidade, que possui outra configuração.

Por outro lado, o sigilo possui uma faceta técnica que o viabiliza como prática em todos os seus aspectos. Abrem-se dois caminhos técnicos do sigilo: os processos e procedimentos de se esconder pessoas ou coisas; e os processos e procedimentos de esconder informações ou dados, virtualizados ou não. O sigilo que envolve coisas ou pessoas envolve procedimentos multifacetados, de interdição e ocultação. O objeto ou pessoa a ser escondido envolve técnicas diversas, mas todas elas são direcionadas à retirada da identidade,

⁵ Ver Michel Foucault, Em Defesa da Sociedade.

origem, etnia, condição social etc. Inúmeros são estes casos conhecidos na literatura e na História: Édipo-Rei, o Homem da Máscara de Ferro, Anne Frank, Fernando Pessoa e seus pseudônimos etc. Um exemplo incorporado às leis do sigilo sobre pessoas é o sistema de proteção à testemunha amplamente utilizado pelos Estados modernos⁶.

Com o advento dos códigos e da escrita, que nada mais são do que a virtualização do real, facilitou-se a apreensão dos fatos, agora transformados em linguagem e dados. Assim sendo, torna-se mais difícil a interceptação por outrem do que se quer esconder, resguardando-se por mais tempo a relação sigilosa. Os meios e formas de se realizar o sigilo foram os mais variados. Contudo, os gregos, séculos antes de Cristo, utilizavam-se de uma técnica de escamoteamento da informação e dos dados que perdura até o presente momento: a *esteganografia*, que é a arte de esconder a escrita⁷. As mensagens não são cifradas ou codificadas⁸, que podem ser escondidas utilizando-se objetos ou no próprio corpo⁹. A tecnologia da esteganografia foi muito utilizada por governos e governantes, a fim de enviar mensagens sensíveis de guerra ou administração. Devido a importância do sigilo e das relações que ele protegia, a técnica da esteganografia foi espalhada por toda a sociedade. Inúmeros textos e correspondências pessoais ou profissionais foram mantidas em sigilo sob a técnica da estenografia. A esteganografia é o primeiro passo de um processo que desemboca na criptografia, tal como conhecemos atualmente.

⁶ No mundo é difundido o sistema de proteção às testemunhas. No Brasil, ele foi incorporado na Lei n. 9.807/1999, que pode ser encontrada neste link: http://www.planalto.gov.br/ccivil_03/LEIS/L9807.htm, acessado no dia 29.03.2019, às 16h15min.

⁷ Stallings (2015, p. 39) apresenta alguns exemplos de técnicas de esteganografia:

“Diversas outras técnicas têm sido usadas historicamente, e alguns exemplos são [MYER91]:

- Marcação de caractere: letras selecionadas do texto impresso ou datilografado são escritas com lápis por cima. As marcas normalmente não são visíveis, a menos que o papel seja mantido contra uma fonte de luz clara.
- Tinta invisível: diversas substâncias podem ser usadas para a escrita sem deixar rastros visíveis, a menos que alguma química seja aplicada ao papel.
- Perfurações: pequenos furos em letras selecionadas normalmente não são visíveis, a menos que o papel tenha uma fonte de luz no fundo.
- Fita corretiva de máquina de escrever: usada entre as linhas digitadas com uma fita preta, os resultados de digitar com a fita corretiva são visíveis apenas sob uma luz forte”.

⁸ “Antes de começar, definiremos alguns termos. Uma mensagem original é conhecida como texto claro (ou plaintext), enquanto a mensagem codificada é chamada de texto cifrado (ou ciphertext). O processo de converter um texto claro em um texto cifrado é conhecido como cifração ou encriptação; restaurar o texto claro a partir do texto cifrado é decifração ou decryptação. Os muitos esquemas utilizados para a encriptação constituem a área de estudo conhecida como criptografia. Esse esquema é designado sistema criptográfico ou cifra. As técnicas empregadas para decifrar uma mensagem sem qualquer conhecimento dos detalhes de encriptação estão na área da criptoanálise, que é o que os leigos chamam de ‘quebrar o código’. As áreas da criptografia e criptoanálise, juntas, são chamadas de criptologia” (STALLING, 2015, p. 21).

⁹ Singh (2014) relata o envio de uma mensagem feita aos espartanos, acerca da invasão dos persas, no couro cabeludo do mensageiro. Ao crescer o cabelo, a mensagem ficou escondida e não pode ser mais vista ou interceptada pelos persas.

2. Segredo: o reconhecimento do eu

O sigilo necessariamente acaba por criar uma relação sigilosa. Ou seja, além de ser externo ao homem, o sigilo deve ser compartilhado por duas ou mais pessoas que são conhecedoras, senão do conteúdo, mas da autoria ou dos objetivos a serem alcançados com o que se esconderá. O segredo possui uma outra configuração e outras possibilidades, que devem ser compreendidas historicamente com a configuração de um outro tipo de sujeito, de ser humano, que não mais precisaria estabelecer relações sigilosas, que eram mais suscetíveis de serem descobertas, reavaliadas ou questionadas. O sigilo torna-se, por sua configuração, uma possibilidade sempre possível de críticas, debates e discussões. Era necessária uma alteração no *modus operandi* do sigilo, a fim de que o humano pudesse sobreviver à normalização, à invasão do seu eu. Assim, o segredo é um outro lugar de combate em face da onipresença do público e das estruturas relacionais do sigilo¹⁰. Aliás, o segredo é também formado quando a estrutura relacional do sigilo se quebra e as partes se desconectam ou deixam de existir.

O segredo, em seu sentido psicológico, é o total ensimesmamento do ser humano que busca o segredo:

“É depois do século XVI, como atesta o dicionário histórico da língua francesa, Le Robert, que o ‘conteúdo escondido’ toma um valor psicológico, no sentido onde ele se aplica à interioridade da pessoa. O segredo propõe-se a designar a vida íntima e não revelada de alguém. As expressões parecem testemunho dessa acepção: ‘os segredos do coração’, ‘ter o segredo de alguém’, ‘confiar um segredo’, ‘fazer parte do segredo’. Como a informação que se pretende manter escondida ou reservada não o é para sempre, existem expressões desdenhosas, tais como: segredo de comédia (uma peça de teatro que o público pode entender), o segredo de Polichinelo (1808, este personagem grotesco da Commedia dell’arte, sendo muito freqüentemente zombado, seus segredos não enganam mais). Sobre esse indivíduo, Arnaud Lévy (1976) nota que a locução pode ser interpretada de vários modos: “- Inicialmente, isso designa o segredo de Polichinelo para si mesmo (aquele que ele guarda) e o segredo que lhe concerne;

- ‘Ter um Polichinelo na gaveta’ evoca o segredo de uma gravidez. Mas a criança não pode ser retida indefinidamente no ventre da mãe e o segredo não pode ser guardado;
- Polichinelo também quer dizer marionete, fantoche, aquele que não tem vontade própria: metáfora da relação primeira da mãe com a criança e do treinamento esfínteriano precoce –

¹⁰ “A palavra é derivada do latim *secretu*: um lugar à parte, pensamento ou acontecimento que não deve ser revelado, mistérios (de um culto religioso). *Secretus*, o adjetivo, significa solitário, separado, isolado, recluso, dissimulado e raro. O próprio verbo *se-cernere*, na origem desta palavra, é constituído do prefixo SE – marcando a separação e de CERNERE: selecionar, passar no crivo; de que lugar distinguir, discernir ver, escolher, decidir (krinein em grego – krypto: esconder; cripta). Primeiros usos em francês: saber reservado a algumas pessoas, troca de conhecimentos reservados dados a título de conselho, um aviso dentro de um contexto político (secretário). Elementos da vida privada que não devem ser do conhecimento de todos. ‘Sob a chancela (real) do segredo’: expressão originalmente política, tornou-se metáfora da confiança com a promessa de nada revelar. ‘Em segredo’, em voz baixa (sussurro baixo). Destinada a designar por eufemismo certas coisas ou atividades: as partes sexuais (os segredos), as necessidades naturais (o segredo); “laisser un secret” (soltar um segredo) dizia-se divertidamente no século XVII para se dizer ter soltado um peido discreto. Um outro uso ainda: meio, processo, método, arte ou técnica que devem se tornar objeto de um ensinamento particular, de maneira iniciática: segredos de fabricação, segredo industrial”. (FLORENCE, 1999, p. 163)

a criança é como se fosse agida por sua mãe (l'enfant est comme agi par sa mère) – estatuto de feto?” (Florence, 1999, p. 163)

Neste sentido, o segredo é algo que efetivamente não tem existência física. Ao internalizar uma ideia que não possui traço relacional, o segredo não possui forma ou estrutura, a não ser para quem o detém e que sabe a relevância ou não daquilo que guarda e esconde do mundo. É a partir desta internalização sem contrapontos ou dialética que o segredo se torna fonte de construção de certa individualidade. Dessa forma, o segredo só existe quando ele foge deste estado psicológico e se materializa de alguma forma, digitalmente ou não. La Rochefoucauld direciona o segredo nesta moldura:

“Todo mundo concorda que o segredo deve ser inviolável, mas nem sempre concorda que a natureza e a importância do segredo: na maioria das vezes, consultamos apenas a nós mesmos sobre o que devemos dizer e o que devemos calar; existem poucos segredos eternos, e o escrúpulo em revelá-los não dura para sempre” (*apud* PROST, 2009, p. 163)

É desta moldura de segredo, internalizado na psique e alma humana, que se engendrou uma série de conhecimentos, saberes disciplinares e poderes para se materializar o segredo inserto no consciente e inconsciente. O homem torna-se portador de saberes e segredos que devem ser desvendados e produzidos. Positivamente, produzir-se-ia o segredo e arrancá-lo¹¹.

É neste duplo aspecto de se reconhecer a existência de segredos inerentes ao corpo e ao indivíduo, bem como a necessidade de que eles sejam extraídos e revelados, que surgem inúmeras normas de segredos profissionais, além daqueles que já existiam no confessionário católico e no consultório médico, que seriam um *locus* da confiança, do falar abertamente, sem medo. Nessa normalização jurídica da materialização do segredo que se produz ciência, suas divisões, os seus campos altamente especializados, interconectados, enfim, sujeita-se indivíduos.

O segredo, na sua perspectiva jurídica, é revelação do motivo por trás de algo, alguém. O direito não se encontra somente na dupla chave, normalizado e

¹¹ Ao se conceituar o segredo como inerente ao ser humano e sua individualidade, afastamos a definição de Norberto Bobbio de que o segredo seja algo relacionado ou possa exprimir as práticas de Estado (2015). O entendimento esposado nesta tese impõe uma análise mais estrita do que seja segredo, a fim de evitar uma confusão em relação ao conceito de sigilo. Bobbio amplia o conceito de segredo e abarca a ideia de sigilo para defender que o Estado democrático seja um poder visível e sem recônditos obscuros. Como o Estado democrático de direito por definição tem que ser transparente, o segredo, como prática, é um vazio jurídico. Não há permissão para a existência do segredo dentro do Estado de direito. Contudo, é permitido sim ao Estado o sigilo como parte de suas atividades governamentais, sendo uma ferramenta jurídica a ser regulada por leis e controlada pelo Poder Judiciário. O Estado de Direito não pode ser titular de um segredo.

normalizador¹², existe um aspecto psicológico que se refere ao processo decisório, confirmador ou desconfirmador da norma jurídica. Em várias normas, esta tomada de decisão é presumida positiva ou negativamente. Presume-se que o agressor quis matar alguém porque puxou o gatilho. O motivo psicológico¹³, que se subsume ao crime de matar alguém, está inserido no ato de puxar o gatilho. Somente no decurso do processo que este motivo psicológico, inferido nas hipóteses previstas nas leis, levará ou não aquele que apertou o gatilho a ser condenado. É neste momento processual que o direito busca extrair o segredo do agressor, da vítima e daquela relação existente. Com o segredo revelado nos autos que se produz, além dos aspectos materiais envolvidos, atenuantes (forte emoção, ameaça, injusta agressão etc.) e as agravantes (futilidade, torpeza, egoísmo etc.), que visam demonstrar os segredos escondidos na consecução dos atos criminosos. No procedimento criminal é muito mais evidente, como exemplo, mas que não é único, de se enxergar a busca de um motivo psicológico do segredo de determinadas práticas sociais e jurídicas. Ao incentivar a todo momento a produção e materialização do segredo, a fim de normalizar o desviado e sujeitá-lo a uma expectativa, espalhando-se este comportamento pelo ordenamento jurídico, transforma esta prática numa necessidade axiológica do direito moderno.

Este fator psicológico que embalsama o segredo e que está fora do poder estatal e dos mecanismos de controle, será deslocado para a regulação das tecnologias de informação e comunicação, mais especificamente para as técnicas de criptografia. O segredo, como característica humana e atrelada à dignidade, pode ser objeto de controle do Estado e de empresas quando ele é ampliado para sistemas de informação? Diante da perspectiva do conceito trazido, o segredo pode ser ampliado para além do binômio consciência e inconsciência do ser humano em seu aspecto biológico? Mais especificamente, existe uma consciência digital do sujeito? Se começar a responder sim para todas estas perguntas, somente para não as deixar sem enfrentamento, mas que serão objetos de discussão mais à frente, estaríamos reconhecendo definitivamente a ideia de um sujeito digital, extensivo ao biológico. Fazer este movimento é necessário?

¹² Ver Márcio Alves da Fonseca, Michel Foucault e o Direito.

¹³ A motivação psicológica, tal como propomos nesta tese, é: “A motivação é encarada como uma espécie de força interna que emerge, regula e sustenta todas as nossas ações mais importantes. Contudo, é evidente que motivação é uma experiência interna que não pode ser estudada diretamente” (Vernon *apud* Todorov *et* Moreira, 2005). E na motivação psicológica existem dois aspectos a serem definidos: “Diz-se frequentemente que há duas concepções, mais ou menos incompatíveis, da natureza humana. Uma delas sustenta que o homem é um ser essencialmente racional, seletivo, dotado de vontade, que conhece as fontes de sua conduta ou que está cômico das razões para a sua conduta e é, portanto, responsável por ela. O outro ponto de vista afirma por vezes que o homem, por natureza, é irracional, e que seus impulsos e desejos devem ser controlados pela força das sanções da sociedade” (Cofer *apud* TODOROV *et* MOREIRA, 2005). O direito tem como escopo sancionar este irracional que gera a desconformidade.

3. Privacidade: reação às disciplinas e saberes

Percebe-se no estudo dos conceitos de sigilo, segredo e privacidade, que, não raro, eles são misturados e utilizados sem quaisquer contextualizações ou delineamentos. A intenção deste artigo é construir uma genealogia destes conceitos, destituindo-se do seu teor teleológico que, porventura, venha inundar os sentidos que lhe são atribuídos. Ao se realizar a investigação crítica, nota-se o deslocamento das práticas sociais, históricas, econômicas e culturais nos atos de esconder, colocar fora de alcance, ocultar algo ou alguém de outrem.

Com o sigilo, o que era ocultado torna-se pertinente na alçada externa do indivíduo. Estabelecia-se uma relação sigilosa, com os seus códigos e ferramentas, a fim de que só algumas pessoas tivessem acesso ou entendimento sobre uma determinada informação, dado ou coisa. O sigilo, por sua concepção estrutural, possui algo de mágico, em que poucos possuem ou simplesmente desconhecem o entendimento do todo, mas conseguem enxergar os resultados obtidos sem entender os meandros.

O segredo é de outra natureza, que pode se entender complementar ao sigilo, mas que não se reduz a ele e tem como consequência uma ampliação ainda mais abrangente da ideia de esconder algo ou alguém de outrem. O segredo é de ordem interna, não palpável, não existente. É uma não informação que só se realiza, tornando-se segredo a partir do momento que algo ou alguém consegue produzi-la fora do eu. O segredo não necessariamente é conhecido pelo seu detentor, no que pode estar escondido de seu consciente ou escamoteado pelo seu inconsciente. Engendra-se o segredo no contexto de uma sociedade disciplinar que constrói outro tipo de sujeito, outros conhecimentos, outras verdades. Isto não significa que o sigilo tenha se tornado obsoleto. Eles convivem e se retroalimentam a partir do momento que o segredo se materializa numa arquitetura moldada pelo sigilo.

A privacidade desloca e moldura um conjunto de práticas ampliadas acerca da necessidade humana de se esconder ou de ocultar coisas e informações, que, primeiramente, surge de uma reação jurídica, normalizadora em face a esta sociedade de massas, disciplinar. É neste sentido que a privacidade como conceito, prática social e jurídica questiona a posição do sigilo e do segredo, os quais são insuficientes como ferramenta de isolamento numa sociedade disciplinar e panóptica, que ilumina a tudo e a todos. Os mecanismos do sigilo e do segredo, mesmo que entronizados em legislações nacionais, são precários para deter este avanço da produção de saberes e poderes, da transparência.

Em face deste reconhecimento, timidamente, no fim do séc. XIX, Louis Brandeiss desenhou um direito de ser deixado em paz (“right to be alone”). Desta forma, a privacidade, conectada com a dignidade humana, estaria condicionada a dois critérios: solidão como condição de liberdade e a não interferência de outrem sobre assuntos que não seriam mais de interesse público. O deslocamento da privacidade em relação ao segredo e ao sigilo é um duplo reconhecimento: de que há um Estado de vigilância espreado por toda a sociedade¹⁴; e que há uma sociedade de massas que alcança todos os aspectos da vida do indivíduo. A opressão e dominação do Estado e da sociedade de massas impingem ao indivíduo uma vigilância constante e presente e, ao mesmo tempo, uma produção cada vez mais incessante de informações *per si*, de si e para si. É neste ponto que o direito de estar só reage a este olhar panóptico e difuso que nunca cessa.

São insuficientes os subterfúgios do sigilo e do segredo para se viver anonimamente e impedir este acúmulo de informações e dados sobre si que a privacidade, como um valor, constitui-se de uma ferramenta de luta e oposição à transparência total. A privacidade é uma estratégia de outra ordem do segredo e do sigilo. Ela combate o etéreo e difuso do estado de vigilância, das redes disciplinares que opõem e obstaculizam o direito do indivíduo se afastar e se esconder e das redes que extraem cada vez mais informações e dados do sujeito.

Ensimesmar-se é cada vez mais uma não opção a partir do esquadrinhamento de sujeitos emoldurados, previsíveis e controlados. A partir do séc. XIX, as tecnologias foram iluminando ao que era obscuro e não conhecido. Os saberes desenvolvidos pela racionalização científica em áreas médicas, biológicas, de engenharias e arquiteturas, produziram tecnologias labirínticas, impossíveis de se alcançar o sentido e o objetivo delas e do que significa a vida. As casas burguesas ficaram menores e com espaços cada vez mais divididos e definidos e na forma de como a família se comportavam. As cidades planejaram-se em estruturas mais abertas, amplas e gigantes e, ao mesmo tempo, mais esquadrinhadas e controladas para atender a exigência da sociedade disciplinar. As ciências começaram a produzir tecnologias de vigilância e de controle, i.e. fotografia e cinema, de transportes e de produção exponenciais. Enfim, pode-se elencar muitas das transformações trazidas pelas disciplinas e suas tecnologias, contudo, há que se retratar que a privacidade surge como reação e enfrentamento a esta racionalização científica e de práticas sociais que sujeitam e dominam o indivíduo. E a forma jurídica para isto é o reconhecimento da privacidade como um direito, um

¹⁴ Ver Vigiar e Punir de Michel Foucault.

direito fundamental que se une e dá sentido ao sigilo e ao segredo, mas não se funde a eles. É do direito fundamental à privacidade que se englobam e surgem outros aspectos e direitos conexos, tal como o direito à vida privada, intimidade, inviolabilidade do domicílio e da correspondência ou contra o arbítrio estatal¹⁵.

Com o avanço e desenvolvimento das tecnologias e das ciências, o direito à privacidade encaminhou-se para uma moldura ainda mais específica e diferenciada: como a um direito de obstaculizar a vigilância. Eric Hughes, no Manifesto Cyberpunk, apontou este deslocamento da privacidade como um direito de mostrar-se seletivamente em face do excesso de transparência:

“Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world”¹⁶.

Encaminhou-se a moldura da privacidade para um direito de não ser monitorado, não ser registrado e de não ser reconhecido¹⁷. Rainer Kuhlen direciona a privacidade como "autonomia informacional" (Informationelle Selbstbestimmung), ou seja, a capacidade de escolher e utilizar o conhecimento e a informação autonomamente, em um ambiente eletrônico, e de determinar quais atributos de si serão usados por outros (*apud* CAPURRO, 2013)¹⁸.

E é neste recorte de privacidade, como o direito de não ser monitorado, registrado ou reconhecido, que se verifica os contornos que o diferenciam do segredo e do sigilo. E com este olhar, reconhece-se que os deslocamentos são *pari passu* os das estruturas sociais, históricas, econômicas e tecnológicas existentes. Sigilo, segredo e

¹⁵ E assim é o que determina o art. 12 da Declaração Universal dos Direitos Humanos adotada pela Assembleia Geral das Nações Unidas estabelece que o direito à vida privada é um direito humano: "Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências ou ataques.". O artigo 17 do "Pacto Internacional dos Direitos Civis e Políticos" adotado pela Assembleia Geral das Nações Unidas, consagra o seguinte: 1. "Ninguém será objeto de ingerências arbitrárias ou ilegais em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques ilegais a sua honra e reputação. 2. Toda pessoa tem direito à proteção da lei contra essas ingerências ou esses ataques."

¹⁶ Tradução livre: “Privacidade é necessária para uma sociedade aberta na era eletrônica. Privacidade não é segredo. Um assunto privado é algo que ninguém quer que o mundo inteiro saiba, mas um assunto secreto é algo que ninguém quer que ninguém saiba. Privacidade é o poder de seletivamente revelar-se para o mundo”. <<https://www.activism.net/cypherpunk/manifesto.html>>, acessado no dia 10.04.2019, às 11h53min.

¹⁷ VIANNA, 20007.

¹⁸ “The information scientist Rainer Kuhlen conceives the concept of "privacy" (*Privatheit*) not primarily in the sense of data protection or of ‘the right to be let alone’, but of what we call in Germany “informational autonomy” (*informationelle Selbstbestimmung*) that Kuhlen understands as the capacity to choose and use autonomously knowledge and information in an electronic environment”.

privacidade são construções de tempos e espaços que não se anulam, mas se acumulam e se imbricam. Por isto que há tanta polissemia de sentidos entre estes conceitos que possuem genealogia distinta e muito bem localizada.

A privacidade como um direito fundamental a não ser monitorado, registrado e reconhecido, na perspectiva deste trabalho, em que a maioria dos aspectos da vida são virtualizados ou digitais, é um direito que se pauta pela não memória ou, pelo menos, a uma restrição à memória total e absoluta sobre o indivíduo. Na articulação destes direitos, em relação às tecnologias de informação e comunicação, verifica-se que a privacidade funcionaria, em consequência, como um direito ao esquecimento. Não haverá memória sobre determinados aspectos da vida privada e da intimidade e isto será determinado e controlado pelo sujeito digital, que teria o gerenciamento destes dados e da verdade sobre eles.

Entretanto, na prática social, econômica e tecnológica, os indivíduos estão apartados das ferramentas para verificar se os seus dados estão sendo ou não guardados em reconhecimento um direito à privacidade de não ser monitorado, registrado ou reconhecido. Diferentemente do sigilo, em que o indivíduo, de maneira incerta, possui um controle sobre o tráfego da informação ou da coisa, no direito à privacidade as ferramentas jurídicas e tecnológicas estão fora de seu alcance. É um direito equidistante e difuso que depende de uma série complexa de atores cooperando conjuntamente, sem quaisquer desvios ou conflitos, num concerto de tecnologias e requerimentos jurídicos, em que a complexidade dos aparatos inviabiliza a apreensão do direito em sua potência. A solução em parte seria atribuir aos indivíduos a se tornarem efetivamente sujeitos de direitos dentro da perspectiva cidadãos digitais.

Contudo, a questão posta aqui neste momento não se refere ao empoderamento de direitos e tecnologias em decorrência do direito à privacidade. Há que se indagar sobre os abismos entre o direito à privacidade, como uma memória seletiva e selecionável, com os esquecimentos que deveria produzir, e que de fato não produz, e as verdades multifacetadas que sujeitam os indivíduos, que deveriam ser os titulares deste direito, mas que estão alheios das condições de se empoderarem dele, física e virtualmente.

As tecnologias da informação e comunicação criam um paradoxo em que, ao aproximarem os indivíduos pelas redes, incentivam, de forma constante e profícua, uma produção de dados gigantesca sobre e entre si para os detentores destes sistemas e que, ao mesmo tempo, estes dados não mais lhes pertencem, a não ser por uma ficção jurídica, e não mais possam ser recuperados ou excluídos, se assim o desejarem. É um paradoxo do não lugar

virtual, que não mais nos pertencem, e de uma sujeição que deslocaliza a humanidade, sublimando-a.

A partir da quebra disruptiva provocada pelas tecnologias de informação e comunicação, a privacidade, o sigilo e o segredo são puramente conceitos sem aderência à realidade, pois a virtualização do homem desloca para outro lugar e tempo a produção de verdades. Os dados pessoais são corporativos e não estão mais ao alcance de uma ideia de privacidade. Nada mais é do que um indivíduo despertencido de suas memórias, puro esquecimento de uma humanidade. Neste paradoxo, a verdade torna-se uma coisa inumana, puramente tecnológica e abstrata, em que a racionalidade subtrai o homem e produz a autopoiese informática, que tem como finalidade a legitimação da inteligência artificial.

A fim de se enfrentar a projeção deste futuro tecnológico, que o processo de consumação de uma ideia de humanidade e de sujeitos deve ser reconstruída paulatinamente com vistas ao empoderamento total do sujeito digital, que é o fim e não o meio. O enfrentamento desta projeção deve perpassar um percurso que envolve a adoção de processos positivos e negativos de apreensão de como se realiza o fluxo da memória, do esquecimento e da verdade nas redes e sistemas de informação e comunicação e para além deles. Nesse passo, a abordagem flui necessariamente por um entendimento e apreensão da criptografia como um processo tecnológico e jurídico de um duplo conceitual: como uma tecnologia que permite transformar o fluxo informacional transparente em uma condição de segurança, confiabilidade, integridade e autenticidade; e, em outro aspecto, mais relacionado ao sigilo, segredo e privacidade, a criptografia permite a efetividade da memória selecionável, da retomada do controle sobre os dados e de evitar a acumulação indevida de dados e informações sobre si numa retomada do que seria uma ideia de cidadania e humanidade digital.

A estes dois caminhos que existem e podem aparentemente ser contraditórios, ou seja, a transparência em face ao sigilo, segredo e privacidade, deve-se caminhar para a compreensão desta realidade que produz informações e dados e sublima valores e necessidades. Nesta análise, em direção a uma maximização da potência dos conceitos e dos direitos aqui trazidos, cabe indagar da possibilidade de convivência e de práticas de se utilizar a criptografia como prática social, histórica, econômica, jurídica e tecnológica de combate a um destino robotizado, artificial, e de como esta tecnologia pode ser a chave de um entendimento de fenômenos complexos e polissêmicos, que inclui também a possibilidade de se admitir a inevitabilidade de um processo de futuro totalmente digitalizado.

Entender as repercussões do sigilo, segredo e privacidade com os temas até aqui tratados na tese com a aplicação da criptografia tem como objetivo compreender

como funcionariam as seguintes perguntas, mas não limitadas a elas, na construção significativa de memória, esquecimento e verdade: como acessar uma base pública ou particular se ela estiver sob o sigilo criptográfico? Em caminho oposto, a criptografia pode auxiliar também no desenvolvimento de bases públicas e no acesso à informação? Em que sentido? A criptografia afastaria efetivamente uma vigilância estatal? O Estado tem direito de ter acesso universal às chaves criptográficas? E o campo da História, como um lugar de memória, como ficaria impactado pela adoção da criptografia? Existe um direito ligado à criptografia? Delimitar as diferenças e apontar as complementariedades visa trazer a potência do funcionamento da criptografia como objeto para a construção do empoderamento do sujeito digital¹⁹.

4. Direito à Criptografia como Direito Fundamental?

A intenção deste trabalho não é fazer um estudo exaustivo sobre sigilo, segredo e privacidade. Nem muito menos demonstrar como eles são intensamente aprofundados no direito. Acredito que existe uma parte do que é segredo, sigilo e privacidade que não é sequer discutida no campo do direito. E é esta perspectiva que foi trazida acima, qual seja, do sigilo, do segredo e da privacidade, em todos os seus aspectos materiais e imateriais, como instrumentos utilizados para uma reação e de combate à práticas e tecnologias disciplinares e de controles, estatais ou não.

As estratégias de luta envolvem diferentes campos de saber e de poderes, contudo, os deslocamentos são contínuos. A adoção da tecnologia como auxiliar neste processo não é nova nem disruptiva. Ela surge como uma resposta às mudanças sociais, históricas e econômicas. A criptografia já é conhecida desde o séc. XVII, no processo de Mary Stuart, e alcançou na década de 1970 o seu apogeu matemático e tecnológico com a adoção das chaves assimétricas (SINGH, 2014).

Ao se alcançar o desenvolvimento matemático com as tecnologias de informação e comunicação há um redirecionamento das questões de transparência e opacidade do Estado, que são realocadas e ressignificadas para um contexto ainda não vislumbrado e, talvez, ainda incipiente. Aí, surge uma outra possibilidade de entender estes deslocamentos e de construir caminhos para um tipo de sujeito, que deve ser entendido e redefinido em seus aspectos valorativos. Parte deste processo de constituição de um sujeito, dentro de uma perspectiva jurídica, é entender se as respostas, ou uma delas, sejam direcionadas

¹⁹ Alguns doutrinadores vêm defendendo a criptografia como direito: Juliano Maranhão (2016),

a molduras dadas pela ciência e pela tecnologia. Ou seja, o sigilo, o segredo e a privacidade, como práticas de memória, esquecimento e verdade, devem se direcionar, quiçá se restringir, como enfrentamento, aos campos da ciência e da tecnologia? Há possibilidade de se atribuir valores às tecnologias? Se sim, é a criptografia, por estes usos e apropriações, um direito fundamental? Seria um direito reativo a determinadas práticas complexas que sujeitam determinados seres humanos?

Antes de enfrentar estas perguntas, há que se compreender os dois aspectos inerentes à criptografia: ser um cálculo matemático que viabiliza a transparência e a integridade da memória produzida nos arquivos digitais; e como forma de se esconder ou seleccionar a memória visível, tanto do Estado quanto de empresas e indivíduos. A partir destas análises, enfrenta-se, principalmente, a questão de a criptografia ser ou não um direito fundamental.

4.1. Integridade, Autenticidade e Confiabilidade: A Criptografia como Tecnologia da Transparência

Os primeiros combates que devem ser realizados em análises, conjecturas e críticas são aqueles direcionados ao senso comum e ao pensamento harmonizante, muito comum na doutrina jurídica brasileira. A tendência do pensamento harmonizante é traçar uma memória linear do semelhante, esquecer as diferenças e produzir uma verdade totalmente dissonante de uma realidade, a qual poderia ser possível de se apreender e traduzir, porém, ignorada por esta estrutura. O pensamento harmonizante necessita do consenso e do apoio de uma rede de pessoas e escritos para ser reconhecido e reconhecê-los, tal como um círculo de assunções e de inferências, na sua grande maioria autorreferentes, que não deslocam problemas e questionamentos. São reificações perenes de ideias já formuladas e estabelecidas. Não há o novo. É o mesmo terreno já percorrido com construções diferentes.

A dissociação do algo a se conhecer com o conhecimento afasta as possibilidades de transformação e remodelação. No fundo, somos capturados pela análise teleológica que mistura todos os conceitos e ideias para outros significados e sentidos, que já não são polissêmicos. É o outro. Um estado diferente da ontologia que se desconectou. A sensação de despertencimento do que é humano, do objeto ou dos dois atinge profundamente a relação entre as palavras e as coisas e sua condição de veracidade. O resgate das condições de significação, ou seja, trazer sentido aos signos, que foi feito acima, visa não conservar as palavras aos significantes originários, mas aflorar todas as possibilidades que os conceitos

foram desenvolvidos anteriormente e confrontá-los com as demandas de outros sujeitos e conhecimentos. Neste processo específico, sigilo, segredo e privacidade são desafiados a se ampliar até os seus limites gnosiológicos, para se constatar as condições de validade e de existência de como utilizá-los como designantes de um outro tipo de fenômeno.

Neste caminho, e é impossível enxergar o processo como um todo quando se está nele envolvido, as condições de ruptura conceitual e fenomenológica estão postas. Se já não foram realizadas, elas estão prestes ou na iminência de ocorrerem. Esticar os conceitos para além de seus limites arrebenta as relações de veracidade necessárias para a compreensão da realidade. É de se questionar com afincos se estes termos que utilizamos neste artigo, qual seja sigilo, segredo e privacidade, em razão de tanta polissemia, tanto uso inapropriado e construções inadequadas de possíveis semelhanças tenham transformado os significados púidos e esfarelados. Logicamente que a tentativa foi a de fazer surgir a potência deles e direcioná-los cada qual dentro de sua genealogia. Contudo, tal empreitada percorre terrenos áridos e de difícil encaminhamento e fixação. Concretizado ou não este feito, está posto.

A esta constatação ontológica dos conceitos desgastados, há que se direcionar a análise para a utilização do conceito de criptografia em seus aspectos tecnológicos e valorativos. A criptografia passou de uma técnica manual e trabalhosa de embaralhar signos para um sistema tecnológico complexo e multifacetado de esconder informações e dados dos mais variados. Neste processo de construção da criptografia como a técnica de se esconder signos houve 3 saltos importantes em termos tecnológicos.

Ao se considerar que o grande problema histórico da criptografia sempre foi a chave de decodificação da mensagem, que deveria ser de conhecimento do emissor quanto do receptor, e que tal chave poderia ser interceptada e a criptografia decodificada, percebeu-se a insuficiência conceitual e técnica desta forma de se esconder mensagens. O processo de deciptação de mensagens era sempre superior e vitorioso em relação a criptografia. Não existia segredo a ser escondido ou privacidade a ser preservada. A transparência, mesmo que de forma indireta, era regra das comunicações. Vivia-se o tempo da criptografia de chaves simétricas²⁰. Neste ponto, a criptografia estava conectada com o conceito de sigilo, no que se

²⁰ “Do grego *kryptós gráphein* – “escrita secreta”, é a ciência de reescrever um texto de forma a esconder o seu significado. Também em computação refere-se ao uso de técnicas que permitem escrever em cifras ou códigos, tornando uma mensagem incompreensível. Quando substituímos palavras de uma mensagem por outras definidas em um código, o processo denomina-se codificação. Quando utilizamos um método matemático para alterar a mensagem, o processo é conhecido como cifração. O processo de cifração é baseado em uma regra matemática de substituição das letras da mensagem e um número que altera o comportamento desta regra, de maneira que, ao se cifrar a mensagem com números diferentes, diferentes resultados serão obtidos. Este número é chamado de

manteve por muitos séculos. O primeiro salto importante da criptografia, ainda em chaves simétricas, foi dado pela introdução de uma técnica desenvolvida pela máquina alemã Enigma, criada pelo Dr. Arthur Scherbius, em que se combinavam sistemas elétricos e mecânicos para a decodificação das mensagens enviadas. Foi utilizado largamente na Segunda Guerra Mundial, principalmente pelo exército nazista alemão. Entretanto, o problema do envio das chaves ainda se mantinha, pois, mesmo que se aplicasse a melhor técnica, existiam inúmeros meios de se descobrir a chave utilizada para decryptografar a mensagem. O exército britânico utilizou-se de várias técnicas e tecnologias para desvendar e decryptografar as mensagens alemãs, no que desembocou numa aceleração da vitória aliada na guerra²¹.

Em pleno séc. XX, em termos de criptografia, ainda estávamos na era do sigilo. O problema da chave simétrica era indissolúvel e, somente em 1978, que foi resolvido o obstáculo do envio das chaves com máxima segurança e/ou sem risco de vazamentos. Ron Rivest, Adi Shamir e Leonard Adleman criaram o sistema de envio de chaves de forma assimétrica²², no que denominaram RSA, padrão ainda utilizado atualmente. A partir deste momento, com a criação das chaves privadas e públicas, estas partilhadas com todos e àquelas em posse do emissor/receptor é que, efetivamente, superou-se a era do sigilo e saltou-se diretamente à privacidade, da memória seletiva e da luta contra a memória total.

O terceiro salto da criptografia foi com a tecnologia do *blockchain*, que alterou a perspectiva e a ideia de como a criptografia poderia ser implementada. A esta ampliação da ideia do que poderia ser criptografado e como seria redistribuída a informação e os dados. Michael Crosby (*apud* DE LUCCA *et* NAJJARIAN, 2018, p 775) define o que é *blockchain*:

“*Blockchain* é essencialmente um banco de dados de registros distribuídos ou um livro-razão público de todas as transações ou eventos digitais que foram executados e compartilhados entre os participantes. Cada transação no livro-razão é verificada pelo consenso formado pela maioria dos participantes do sistema. E, uma vez convalidadas, as informações não mais podem ser apagadas. A *blockchain* possui um registro certo e verificável de cada transação realizada. Usando uma analogia básica, é mais fácil furtar um biscoito de um pacote mantido em local isolado do que furtar um biscoito de um pacote mantido em um mercado, onde se estará sendo observado por milhares de pessoas”.

chave, e quanto maior for, mais segura será a cifragem. Este processo visa a assegurar que apenas o destinatário consiga ler uma mensagem eletrônica, realizando o processo inverso, a decifragem. Quando cifragem e decifragem são realizadas com a utilização de uma senha ou chave única, denominamos o processo de criptografia simétrica” (NOBRE, 2007, p. 417).

²¹ Ver SINGH, 2014.

²² “A criptografia assimétrica permite trafegar dados confidenciais na internet de forma segura e flexível. Para a realização de acesso seguro, garantindo confidencialidade e sigilo na transferência dos dados, sejam eles de uma transação bancária ou de um paciente, a utilização de criptografia é realizada através de um protocolo denominado SSL/TLS (*secure socket layer*). (NOBRE, 2007, p. 417)

Na forma como é posta a tecnologia de *blockchain*, numa estrutura em que todas as partes podem, de forma segura e verificável, constatar a validade de documentos e transações:

“Assim, pode-se dizer que os princípios sobre os quais a tecnologia *blockchain* se fundamenta são: (i) criptografia, que permite a preservação da integridade dos registros e os protege contra possíveis violações; (ii) rede descentralizada *peer-to-peer*, à qual todos os participantes têm acesso; (iii) mecanismos de consenso, por meio de algoritmos que determinam a ordem das transações; (iv) registro de transações (*ledger*) em blocos ligados por meio de criptografia; e (v) regras de validação, que determinam como validar e atualizar os registros de transação”. (SILVA *et* SILVA, 2018, p. 702).

Assim, num deslocamento tecnológico, a criptografia adquiriu uma outra característica, mais ampla, relacional e transparente. A criptografia, cujo nascimento serviu para atribuir a cada um a capacidade de construir memórias seletivas e não acessíveis, transformou-se numa técnica de certificar a autenticidade, a integridade e validade de documentos digitais. Não somente isto, a tecnologia do *blockchain* permite a todos que estão inseridos naquele bloco, a possibilidade de verificar quem inseriu aquele documento, como ele foi alterado, distribuído e/ou excluído. O *blockchain* tornou-se uma possibilidade de se registrar a vida e morte de um documento digital.

Em razão destas características do *blockchain*, ou seja, da criptografia em estrutura de redes, desenvolve-se a possibilidade da certificação da memória, bem como o reconhecimento de todos os participantes da rede da existência e confiabilidade daquele documento digital. Mas a transparência do documento digital é referente a estrutura tecnológica do documento, ou seja, a sequência de *bits* blindada pela criptografia, no que possibilita o reconhecimento de sua alteração, caso ocorra, pela alteração da chave criptográfica original. Há que se ressaltar que a transparência permitida pelo *blockchain* não alcança o seu conteúdo humanamente reconhecível da mediação dos *bits*. Em razão das inúmeras mediações tecnológicas da experiência referente ao conteúdo documento digital, no que impossibilita o entendimento do que está inserido nele, que existe uma dificuldade em relação ao funcionamento da tecnologia e do que ela proporciona como benefício.

Desta forma, são destituídos os sujeitos das condições de compreender o fenômeno, o que pode gerar excessiva euforia ou extremo pessimismo. A tecnologia do *blockchain* é importante no desenvolvimento para além do que foi imaginada a criptografia, mas, como toda tecnologia, possui inúmeros problemas que são inerentes ao fator humano e ao que se considera estado da arte. Questões outras são levantadas na utilização desta tecnologia e que estão fora de como funciona a criptografia, mas como são desenvolvidos os

blockchains. Como o *blockchain* é mais utilizado ainda em seus aspectos financeiros e no seu valor simbólico de troca, em face desta estrutura de redes, que muitos problemas são verificados no seu uso. Geralmente são problemas relacionados com a segurança de informação dos usuários²³, dos detentores das moedas digitais²⁴ e no que tange mesmo à segurança do *blockchain* como tecnologia confiável para tudo que pode ser feito ou que consideram que possa ser realizado²⁵.

Independentemente dos problemas existentes e se eles serão ou não solucionados, as possibilidades do *blockchain* e da criptografia, como conceitos e práticas, estão ampliados e ressignificados. A criptografia poder ser uma ferramenta de transparência e de certificação de uma memória, e não ser só esquecimento, possibilita um reposicionamento acerca dos aspectos valorativos e como esta tecnologia pode ser utilizada em todos os aspectos da necessidade humana.

4.2. Criptografia como Direito à Memória do Esquecimento?

A criptografia, em sua construção original, foi delineada para ser a técnica de se esconder ideias, mensagens, informações, dados. Embora tenha se deslocado para ser também a tecnologia da transparência, a criptografia funciona principalmente para ser parte de uma memória seletiva e não alcançável. No mar de dados produzidos, a criptografia torna-se uma prática contra a vigilância de empresas, Estados e outras pessoas. É uma ferramenta que produz um outro tipo de sujeição, livre da influência dos metadados e daquelas outras que nos condicionam e nos submetem e que estão inseridas nos sistemas de informação, as quais não fazemos a mínima ideia.

²³ Hackers roubam US\$ 50 milhões em bitcoins usando propagandas no Google. Disponível em: <<https://www.infomoney.com.br/mercados/bitcoin/noticia/7280346/hackers-roubam-milhoes-bitcoins-usando-propagandas-google>>, acessado no dia 28.04.2019, às 14h10min.

²⁴ Dono morre com única senha e câmbio de criptomoedas perde US\$ 190 milhões. Disponível em: <<https://www.tecmundo.com.br/mercado/138413-cambio-criptomoedas-perde-us-190-milhoes-dono-morrer-senha.htm>>, acessado no dia 28.04.2019, às 14h10min.

²⁵ Esta reportagem apresenta cinco pontos problemáticos para a adoção da tecnologia blockchain em larga escala e de forma mais consistente. São estes os problemas apresentados no uso do blockchain: a falhas do software do *blockchain*; que nem sempre o *blockchain* é ideal para armazenar dados; o *blockchain* não é necessariamente seguro; escala e confidencialidade são desafios ainda não superados; e contratos inteligentes via *blockchain* são superestimados. “Cinco problemas com o Blockchain que ainda precisam ser resolvidos”. Disponível em: <<https://cio.com.br/cinco-problemas-com-o-blockchain-que-ainda-preciam-ser-resolvidos/>>, acessado no dia 28.04.2019, às 14h19min.

A criptografia, a partir dos anos 1970, é cada vez mais utilizada²⁶.

Com a produção em massa dos microcomputadores e a diminuição dos custos dos dispositivos informáticos em geral, tornou-se mais acessível a todos indistintamente a possibilidade de se utilizar a criptografia, como meio de proteção da privacidade e da memória. Em face disto, em tempos de tecnologias de informação e comunicação, professou-se a ideia de que a criptografia como um requisito inerente à defesa da privacidade, a qual não partilhamos. Se assim fosse, ignoraríamos os aspectos negativos da adoção desta tecnologia e de como eles poderiam ser manipulados sem o consentimento e o conhecimento de quem estivesse usando esta tecnologia. Exemplo desta perspectiva é o fato de que os ingleses, na II Guerra Mundial, já haviam decifrado o código do Enigma alemão no começo das batalhas. Ou seja, eles já sabiam de todos os movimentos e estratégias de guerra alemã, que acreditavam no sigilo de suas informações. Somente anos depois que os ingleses divulgaram o trabalho por eles desenvolvidos e quem os desenvolveu²⁷. A possibilidade de uma manipulação dos dados sem o conhecimento dos sujeitos afasta a interpretação ampliadora que possa ser dada à criptografia, principalmente no tocante a uma equivalência a defesa da privacidade.

Soma-se aos problemas de confiabilidade da criptografia, como instrumento de segurança da informação, outro aspecto negativo que a impede de ser atrelada à privacidade. E, neste caso, relaciona-se a mera possibilidade de os governos obrigarem às empresas de criptografia, principalmente aquelas com existência física ou jurídica no seu território, o acesso a todos as chaves decodificadoras, a fim de poderem analisar o conteúdo de todas as mensagens transmitidas. Todos os governos, sem exceção, querem ter acesso ao conteúdo criptografado. Os EUA são os mais ativos nesta atividade, mas não são os únicos. Tal como foi relatado no capítulo 2, os EUA, através da NSA e do FBI, vêm, reiteradamente,

²⁶ O sistema PGP (*pretty good privacy*, privacidade muito boa), por ser gratuita, foi importante para a difusão da criptografia, em face do padrão RSA, que é proprietário. Este sistema foi criado por Phil Zimmerman em 1991. “O PGP combina algumas das melhores características de ambos, criptografia com chave privada e criptografia com chave pública. PGP é um sistema de criptografia híbrido. Quando um usuário codifica os dados com PGP, PGP primeiro comprime os dados. Compressão de dados economiza tempo de transmissão de modem e espaço de disco e, mais ainda, fortalece a segurança da criptografia. A maioria das técnicas dos criptanalistas exploram padrões achados nos dados para quebrar a cifra. Compressão reduz estes padrões dos dados originais, assim sendo, aumenta grandemente a resistência para criptanalistas. (Arquivos que são muito pequenos para comprimir ou que não comprimem bem não são comprimidos.) PGP então cria uma sessão com chave (session key), que é gerada somente uma vez (esta chave seria a equivalente a criptografia com chave privada). Esta chave é um número randômico gerado a partir de movimentos randômicos do seu mouse e das teclas que você aperta. Esta sessão com chave privada funciona com um algoritmo de encriptação muito seguro para encriptar os dados originais; o resultado desta primeira fase são os dados encriptados (cifrados). Uma vez que os dados são encriptados, o resultado da primeira fase (dados encriptados com chave privada) passa então por uma fase de encriptação com chave pública na qual é encriptado com a chave pública do receptor. A chave gerada aleatoriamente na primeira fase (session key) é transmitida junto com os dados encriptados resultantes da segunda fase para o receptor”. (https://www.gta.ufrj.br/grad/00_1/rodrigo/fr6right.htm, acessado no dia 29.04.2019, às 11h40min).

²⁷ Ver SINGH, 2014.

utilizando-se do discurso da diminuição da privacidade em prol da segurança para terem acesso às chaves criptográficas, que lhes permitiriam analisar todos os conteúdos trafegados em suas redes domésticas. O ex-presidente Barack Obama já defendeu esta ideia abertamente:

“Se criarmos um sistema [de segurança] impenetrável, sem chaves, sem portas, como vamos prender [quem distribui] pornografia infantil, como vamos frustrar ataques terroristas? Que mecanismos temos até mesmo para garantir o recolhimento de impostos? Se não há como violar [a criptografia], se o governo não puder entrar, então todo mundo anda por aí com uma conta de banco suíço no bolso, certo? Tem de haver algum tipo de concessão.”²⁸

Contudo, esta posição é partilhada por inúmeros governos, principalmente aqueles governos com direcionamento menos democrático e mais ditatorial. O governo brasileiro e sua força policial vem se posicionando em busca da restrição dos direitos à privacidade e de outras liberdades fundamentais, em prol da vigilância de seus cidadãos com a desculpa mal posta de lutar contra a criminalidade. Este posicionamento autoritário e não garantidor dos direitos fundamentais vem sendo construído ao longo dos anos sempre a reboque de um discurso moralista e conservador. Por exemplo, a lei de pedofilia na internet, promulgada em 2008, diretamente criminaliza, potencialmente, todos os cidadãos da possibilidade de cometerem este crime. Além da definição do crime ser ampla, a lei condena o simples armazenamento, o que possibilita alguém forjar um flagrante criminoso por quem não tem conhecimento técnico para se proteger. Com a acusação genérica de alguém possuir imagens ou vídeos contendo pedofilia infantil, podem-se emitir mandados de busca e apreensão, autorizações para se invadirem computadores ou decriptografar mensagens protegidas. Todos estão suscetíveis de serem investigados. Neste mesmo passo, a atuação governamental brasileira vem desenvolvendo em relação ao Whatsapp, aplicativo de comunicação privada, que se utiliza de criptografia ponto a ponto, que impede a leitura dela sem a chave²⁹. O governo e a força policial acreditam que o acesso a estas chaves poderiam ajudar a melhorar as investigações criminais. Estes mesmos agentes não elucidam como eles protegerão, se tiverem acesso, a privacidade daqueles que não estão em sede de investigação criminal, quiçá cível.

Em face de todos estes movimentos visíveis e invisíveis sobre a criptografia, que se deve criticar a tentativa de aproximá-la ou igualá-la a uma defesa da privacidade, que é muito mais ampla e complexa. Não se está a dizer que a criptografia não tem o seu valor como ferramenta de auxílio à privacidade. Ela é importante. Contudo, os esforços para implementá-la em outras possibilidades e termos não estará jamais referenciada a uma

²⁸ Disponível em: <<https://exame.abril.com.br/tecnologia/nao-podemos-ter-visao-absolutista-sobre-criptografia-diz/>>, acessado no dia 29.04.2019, às 12h01min.

²⁹ Esta discussão foi levada ao Supremo Tribunal Federal (STF): <<http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=345369>>, acessado no dia 29.04.2019, às 12h12min.

perspectiva que a atrele diretamente à privacidade. Como foi visto acima, a criptografia, enquanto técnica e prática, engendra outra maneira de se criarem valores e necessidades, que não são atributivas e restritivas de um direito fundamental à privacidade.

Uma outra questão negativa que deve ser posta em relação à criptografia, além da possibilidade de ela ser apropriada por mecanismos de vigilância, é a de que ela tem um custo, mesmo que tenha diminuído ao longo dos anos, que inviabilizaria a sua apropriação por todos como prática anti-vigilância. Para se implementar a criptografia existe um custo alto, tanto na parte econômica como na implantação da estrutura de cultura da segurança de informação. Os dispositivos informáticos não serão os mesmos vendidos nas lojas de rua ou *e-commerce* comuns. Eles deverão ser outros que não podem ser geolocalizados e que possuam capacidade de fazerem ligações não rastreáveis e criptografadas. São dispositivos de alto valor. Poucos têm condições financeiras de comprá-los.

Por outro lado, há que se desenvolver uma cultura de segurança de informação, para que os portadores destes dispositivos os utilizem da forma correta, pois, do contrário, estarão à mercê de práticas e mecanismos de vigilância. E, neste sentido, por uma série de questões, os mais pobres são afetados para além da desigualdade econômica. Eles não têm condições de criar o ambiente favorável a se protegerem das práticas e mecanismos de segurança de informação, que funciona num movimento de dentro para fora e de fora para dentro. De dentro para fora, quando o cidadão se torna sujeito digital e consegue manusear a memória que é produzida sobre si. De fora para dentro, quando o sujeito digital entende e compreende as informações que são e podem ser produzidas sobre ele, sem que tenha controle delas.

Nestes dois movimentos, o cidadão é mais sujeito a práticas digitais de vigilância do que alguém empoderado delas. E, nestas ausências, o cidadão perde-se nos processos que são criados e desenvolvidos fora dele e de sua compreensão. É um cidadão digitalizado excluído das ferramentas de sua autodeterminação. Produz-se memórias que são relativas a ele, mas que não são suas ou que possam ser contestadas. É nesta direção que uma pesquisa estadunidense de Mary Madden nos traz:

“Our research suggests that low-income Americans, and in particular, foreign-born Hispanic adults, are disproportionately reliant on mobile devices as their primary source of internet access. While internet connectivity has become essential to these communities, it also creates privacy and security vulnerabilities that they don’t feel prepared to navigate. The survey findings illustrate a substantial demand for educational resources among low-socioeconomic-status groups, but many feel as though it would be difficult to get access to the tools and

strategies they would need to learn more about protecting their personal information online”³⁰.

Esta pesquisadora estadunidense aponta que as pessoas de baixa renda são atingidas em dois aspectos importantes: a hipervisibilidade e a invisibilidade. Elas são alvos injustos de práticas governamentais de vigilância, pois os *softwares* são desenvolvidos para somente os enxergarem. Não só as pessoas de baixa renda, mas aqueles que sejam considerados inimigos ou perniciosos para a administração governamental, as pessoas de baixa educação, os negros, os hispânicos no caso estadunidense. Todas estas práticas de vigilância devem ser espalhadas nestas comunidades sem que elas sejam reconhecidas, ou seja, devem ser invisíveis.

As práticas de hipervisibilidade e invisibilidade não são segredo nem são sigilosas. Elas são reconhecidas diariamente e são incentivadas por todos. É uma memória positiva que deve ser invisível e que tem de gerar benefícios para o cidadão. É uma suposta negociação que o poder de barganha é nulo, pois o sujeito não possui o controle de seus dados, de suas memórias e de seus esquecimentos. As verdades estão com as empresas e governos que têm o acesso a esta massa de dados que produzem a cada segundo. Uma das consequências desta estrutura é a utilização dos dados como forma de monitorar os sujeitos a se manterem nas condições socioeconômicas que estão. É um controle de dominação de corpos e mentes, a partir de uma memória sempre viva, ativa, presente e nunca de esquecimentos. Não há possibilidade de esquecimentos.

Dentro deste quadro negativo, em que a criptografia possui características de exclusão que afastam o cidadão de suas vantagens e benesses, como apresentá-la como solução igualitária e inclusiva de todos na busca contra as práticas de memória total? Alçar a criptografia como direito fundamental superaria os problemas práticos de sua implementação? A sociedade arcaria com os custos econômicos e educacionais para implantar a criptografia como direito fundamental?

O primeiro ponto que se tem de enfrentar é a questão do custo de implementação de um suposto direito fundamental à criptografia, como ferramenta de luta contra a dominação total da memória, contra a transparência. Esta é uma discussão muito bem

³⁰ Tradução livre: “Nossa pesquisa sugere que os americanos de baixa renda, e em particular, os hispânicos adultos, são desproporcionalmente dependentes de dispositivos móveis como sua fonte primária de acesso à internet. Enquanto a conectividade à internet torna-se essencial para estas comunidades, aumenta-se as vulnerabilidades relacionadas à privacidade e à segurança que eles não estão preparados ao navegarem. Os resultados da pesquisa mostram uma demanda grande em busca de recursos educacionais entre os grupos de baixa renda, mas muitos sentem dificuldade para acessar as ferramentas e estratégias que necessitam para aprender mais sobre assuntos relativos a como protegerem seus dados pessoais *online*”. Disponível em: <<https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html>>, acessado no dia 29.04.2019, às 14h50min.

desenvolvida na área da saúde, pois o Estado é obrigado a cobrir os custos dos remédios a preço acessível ou até mesmo subsidiar estes valores para os cidadãos de baixa renda³¹. No STF, em relação ao tema da saúde, mais diretamente relacionado com a decisão do Estado ter de arcar com os custos dos remédios para os cidadãos, as decisões são quase unânimes de que não se pode limitar o direito à vida. Não se é analisado as questões de uma reserva do possível para ser arcar com este direito, fatores econômicos ou custo de implementação. O Estado tem que suprir a necessidade do cidadão. Estas decisões sobre o fator do custo do direito na área da saúde são estendidas aos temas relativos ao direito à educação. Contudo, quando o assunto é intervenção federal nos Estados por não pagamento de precatórios, as decisões acabam por respeitar a reserva do possível e o custo do direito para indeferir os pedidos (WANG, 2008).

Ao se ampliar a análise das decisões do STF para estes direitos relativos à saúde, educação e aos pagamentos de precatórios, nos termos constitucionais, um suposto direito à criptografia poderia ter uma interpretação menos extensiva. Se houver um direito fundamental à criptografia, ele estaria localizado na linha interpretativa desenvolvida pelo STF nos casos relativos à intervenção federal nos Estados por não pagamento de precatórios. Avaliar-se-ia o custo do direito para a sua implementação. No caso da criptografia, isto tornaria inviável este direito de ser aplicado e espreado além das linhas da interpretação jurídica, pois, conforme mostrado acima, existe um custo imenso para aqueles de baixa renda e baixa educação. Em países com diferenças sociais e econômicas gritantes, o custo de um direito à criptografia obstaria o direcionamento do orçamento estatal para resolver as diferenças de acesso à tecnologia, a igualdade social, a liberdade de expressão, enfim, não seria algo efetivo.

E, por fim, há que se perguntar se o Estado, além de não arcar com os custos do direito, teria interesse em não mais poder usar da vigilância sobre os seus cidadãos? Neste passo, um direito à criptografia seria eficiente como uma memória seletiva contra a transparência? Existem muitas pesquisas que mostram que a criptografia não protegerá

³¹ No âmbito da OMC, foi aprovada a Declaração Sobre o Acordo Trips e a Saúde Pública, em que os países membros da OMC concordaram que a saúde pública deve ter primazia sobre os interesses comerciais, para que os países em desenvolvimento possam assegurar a todos os seus cidadãos o acesso a medicamentos com preços acessíveis. A Declaração traz os seguintes termos:

1. Nós reconhecemos a gravidade dos problemas de saúde pública que afligem muitos países em desenvolvimento e países menos desenvolvidos, especialmente aqueles que resultam do HIV/AIDS, da tuberculose, da malária e de outras epidemias.

4. Nós concordamos que o Acordo TRIPS não deve e não pode prevenir os países membros de adotar medidas para proteger a saúde pública. Consequentemente, enquanto reiteramos nosso compromisso com o Acordo TRIPS, nós afirmamos que o Acordo pode e deve ser interpretado e implementado de maneira a apoiar os membros da OMC a proteger a saúde pública e, em particular, promover o acesso a medicamentos para todos.

eficientemente os conteúdos que não devam ser acessados³². Tal situação poderia colocar em dúvida a efetividade de um direito que, atrelado à tecnologia, esteja ultrapassado nos valores que deveria defender. Deve-se gastar tintas e mais tintas para se defender um direito ineficaz?

Enxergar um possível direito fundamental à criptografia é algo muito além do que é necessário para se enfrentar a hipervisibilidade e a invisibilidade. A perspectiva deve ser outra para não ser esvaziado tanto o suposto direito à criptografia como aqueles outros conexos a ele, principalmente o direito à privacidade. Negar a valoração da criptografia como um direito fundamental recoloca-a como ferramenta útil e necessária para ser utilizada como parte do processo de construção de sujeitos digitais, de emponderá-los. O relatório do Conselho de Direitos Humanos da ONU enfrentou muito bem esta questão:

Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective”.³³

Entender as miríades que envolvem a criptografia como ferramenta e os saberes poderes que a constituem, afastam as possibilidades de ela ser considerada um direito, ainda mais fundamental. No entanto, é necessário entender as engrenagens destes processos e localizar de fora para dentro das tecnologias de informação e comunicação uma renovação da discussão ou reposicionamento de como endereçar a memória, o esquecimento e a verdade.

Percebe-se a insuficiência dos conceitos para além do seu *locus* estabelecidos. Aos desafios postos e construídos, há que se construir conceitos que decifram

³² Uma reportagem sobre quebra de criptografia destaca: “Até há pouco, alegando proteção antiterrorista, os Estados Unidos restringiam a venda de *software* de segurança a estrangeiros a chaves de até 56 *bits*. ‘Um PC comum só precisa de uma semana para quebrar uma chave desse tamanho. Um bom *hacker* quebra em menos’, diz Lorenzo Ridolfi, da Pontifícia Universidade Católica do Rio de Janeiro. ‘O governo americano dispõe de supercomputadores capazes de realizar essa tarefa em segundos.’”

“Um sinal inequívoco disso é que em janeiro, Washington franqueou a exportação de programas com chaves de 128 bits. ‘Essa liberação só faz sentido se a CIA já dispuser de meios para quebrar chaves desse tamanho facilmente’, especula Ridolfi. Guerra é guerra”. O segredo da criptografia. Disponível em: <<https://super.abril.com.br/tecnologia/o-segredo-da-criptografia/>>, acessado no dia 29.04.2019, às 16h44min.

³³ Tradução livre: “A criptografia e o anonimato, e o conceito de segurança por trás deles, fornecem a privacidade e a segurança necessária para o exercício do direito à liberdade de opinião e de expressão na era digital. Tal segurança pode ser essencial para o exercício de outros direitos, incluindo direitos econômicos, privacidade, devido processo legal, liberdade de associação e reunião pacífica e o direito à vida e à integridade física. Em razão de sua importância aos direitos de liberdade de opinião e expressão, as restrições à criptografia e ao anonimato devem ser estritamente limitadas em conformidade com os princípios da legalidade, necessidade, proporcionalidade e da legitimidade”. HRC/29/32, que está disponível em: <<http://bit.ly/1FmfiAi>>, acessado no dia 29.04.2019.

estes deslocamentos e consigam resgatar, se é possível, o valor do humano nestas estruturas que nos empurram à virtualização e sublimação do eu.

5. Referências Bibliográficas

ARENDT, Hannah. A condição humana. Rio de Janeiro: Editora Forense Universitária, 2004, p. 15.

CAPURRO, Rafael. Privacy a Intercultural Perspective. <<http://www.capurro.de/privacy.html>>, acessado no dia 10.04.2019, às 11h53min.

DE LUCCA, Newton e NAJJARIAN, Ilene Patrícia de Noronha. Criptomoedas: Novos Meios de Pagamento. *in* Parentoni, Leonardo & Miranda, Bruno & Lima, Henrique. Direito, Tecnologia e Inovação - v. I (Law, Technology and Innovation). Belo Horizonte: Editora D'Plácido, 2018, p. 767-792.

EXAME – <https://exame.abril.com.br>.

FLORENCE, Jean. A Propósito do Segredo. Université Catholique de Louvain – Bélgica. Psicologia: Teoria e Pesquisa. Mai-Ago 1999, Vol. 15 n. 2, pp. 163-166.

GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO (GTA) UNIVERSIDADE FEDERAL DO RIO DE JANEIRO (UFRJ) – <https://www.gta.ufrj.br/>.

HUGHES, Eric. A Cypherpunk's Manifesto <<https://www.activism.net/cypherpunk/manifesto.html>>, acessado no dia 10.04.2019, às 11h53min.

MARANHÃO, Juliano. Ambiente virtual transforma profundamente categorias jurídicas. Revista Consultor Jurídico. Dez/2016. <<https://www.conjur.com.br/2016-dez-05/juliano-maranhao-ambiente-virtual-transforma-profundamente-direito#author>>, acessado no dia 15.04.2019, às 16h30min.

NEW YORK TIMES – <https://www.nytimes.com>.

NOBRE, Luiz Felipe *et al.* Certificação digital de exames em telerradiologia: um alerta necessário. *Radiol Bras*, São Paulo, v. 40, n. 6, p. 415-421, dez. 2007. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-39842007000600011&lng=en&nrm=iso>. Acessado no dia 26.04.2019.

ONU – Organização das Nações Unidas – <https://nacoesunidas.org/>.

PROST, Antoine e Gérard Vincent. *História da Vida Privada, 5: Da Primeira Guerra a nossos dias*. Trad. Denise Bottmann. São Paulo: Companhia das Letras, 2009.

SILVA, Alexandre Couto e SILVA, Ricardo Villela Mafra Alves da. O Blockchain como Ferramenta de Governança Corporativa para a Redução de Custos de Agência em Sociedades Anônimas. *in* Parentoni, Leonardo & Miranda, Bruno & Lima, Henrique. *Direito, Tecnologia e Inovação - v. I (Law, Technology and Innovation)*. Belo Horizonte: Editora D'Plácido, 2018, p. 697-724.

SINGH, Simon. *O Livro dos Códigos*. São Paulo: Ed. Record, 2014.

STALLINGS, William. *Criptografia e Segurança de Redes*. Trad. Daniel Vieira. Revisão Técnica Paulo Sérgio Licciardi Messeder Barreto e Rafael Misoczki. 6ª edição. São Paulo: Pearson Education do Brasil, 2015.

SUPER INTERESSANTE – <https://super.abril.com.br>.

SUPREMO TRIBUNAL FEDERAL – <http://www.stf.jus.br>.

TODOROV, João Cláudio; MOREIRA, Márcio Borges. O conceito de motivação na psicologia. *Rev. bras. ter. comport. cogn.*, São Paulo, v. 7, n. 1, p. 119-132, jun. 2005. Disponível em <http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1517-55452005000100012&lng=pt&nrm=iso>. Acessado em 22 abr. 2019.

VIANNA, Túlio. *Transparência pública, opacidade privada*. Rio de Janeiro: Ed. Renovar, 2007.

WANG, Daniel Wei Liang. Escassez de recursos, custos dos direitos e reserva do possível na jurisprudência do STF. *Rev. direito GV*, São Paulo, v. 4, n. 2, p. 539-568, dez. 2008. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1808-24322008000200009&lng=en&nrm=iso. Acessado no dia 29.04.2019. <http://dx.doi.org/10.1590/S1808-24322008000200009>.

XENOFONTE. *Memoráveis*. Trad. Ana Elias Pinheiro. Coimbra: Imprensa da Universidade de Coimbra e Annablume, 2009.

_____. *Econômico*. Trad. Anna Lia Amaral de Almeida Prado. São Paulo: Ed. Martins Fontes, 1999.