# Preservação de memória, o qbit e a criptografia quântica

*Memory preservation, the qubit and the quantum cryptohgrahy*

**Alvaro Caetano Pimentel Sobrinho**
Doutor em Ciência da Informação pela Universidade Federal do Rio de Janeiro – UFRJ convênio com Instituto Brasileiro de Informação em Ciência e Tecnologia – IBICT.
E-mail: alvaro_pimentel@uol.com.br

## Resumo

Este artigo apresenta uma análise sobre a preservação da memória com a utilização dos dispositivos tecnológicos e com a introdução do conceito do bit quântico (q-bit). A proposta considera a possibilidade de transmitir e preservar a memória utilizando conceitos da física quântica, estudos sobre a mediologia e a angelética e as possibilidades de armazenamento com o uso dos meios magnéticos atuais. Há, ainda, uma breve explanação sobre as possibilidades de segurança da preservação de memória com a utilização de criptografia quântica.

**Palavras chave**: Memória. Bit. Qbit. Armazenamento. Criptografia.

## Abstract

This paper describes an analysis of the memory preservation within use of technological devices and the introduction of quantum bit (qubit) concept. The proposal considers the possibility to transmit and preserve the memory using quantum physics concepts, mediology and angeletics studies and storage possibilities using the current magnetic media. There is also a brief explanation of the memory preserving the security possibilities using quantum cryptography.

**Keywords**: Memory. Bit. Qubit. Storage. Cryptography.



DOI: 10.11606/issn.2178-2075.v9i2p71-88

## 1. Introdução

A preservação de memória, quer seja através de objetos, documentos impressos ou por meios eletrônicos, é um desafio que impõe ao ser humano um número sem fim de possibilidades para manter a história do que somos e fomos. As oportunidades e a evolução tecnológica atuais permitem manter em bases de dados até mesmo o que se julgava ser impensável há algum tempo: armazenamento de objetos físicos em um ambiente virtual. Cabe esclarecer que está se falando de uma visão imagética, uma vez que o produto matriz é que mantém e contém em si sua originalidade, sua natureza própria. Porém, poder copiá-lo e reproduzi-lo, detalhadamente, ainda que não tenha o cheiro e o sabor de sua história, permite admitir ser possível preservá-lo por muito mais tempo e distribuí-lo por diversos lugares.

No entanto, apesar das conquistas computacionais conseguidas, ainda há a busca incansável pelo armazenamento, tratamento e segurança das informações. Assim, tendo em vista a grande massa de dados e a tentativa de compreender e mapear sua estrutura, é possível pensar que volume, velocidade, variedade, veracidade e valor serão também elementos necessários para nortear o que merece ser tratado e armazenado em bases de dados e disponíveis para acesso.

Enquanto tratamento e segurança da informação podem ser tratadas no plano empírico, mesmo com a utilização de ferramentas *Computer Aided Software Engineer* (CASE), é no plano físico que se vê os erros, os acertos e ajustes necessários para buscar as informações. Armazenar é um dos principais fatores de preocupação de administradores de dados por estar fora do plano abstrato de uma análise de dados. As capacidades de discos são sempre consideradas, mas é após a construção de uma base de dados ser concluída que se verifica se o plano imaginado terá a capacidade atender às necessidades previstas e se será suportado pelo *hardware*. Ainda que haja novos artefatos que permitem guardar volumes de dados gigantescos, os avanços são proporcionalmente menores que a quantidade de informações circulantes e construídas por todas as redes de comunicação, quer seja pela Internet ou não.

## 2. O conceito do bit quântico

Estudiosos de diversas áreas têm se esmerado em solucionar a segurança, a velocidade, a capacidade de armazenamento e os tamanhos dos componentes eletrônicos e mecânicos de tal maneira que haja melhores formas de acesso e transporte de dados e computadores. É tudo muito micro... é tudo muito nano...

Um recente desenvolvimento da Mecânica Quântica (MQ) abre a perspectiva do emprego da indeterminação quântica e da superposição de estados na computação, para aumentar os "poderes" operacionais dos computadores. Com isso, Eldred (2009, p. 95) acredita que "quando o computador quântico for construído, vai-se obter uma significativa redução do tempo de computação requerido para tarefas computacionais". Certamente o usuário comum não perceberá se a "caixa" processadora de sistemas está sob conceito da Física Newtoniana ou da Física Quântica, mas a quebra de paradigma já foi iniciada, e as tentativas de projetar uma máquina quântica estão nas cabeças dos cientistas, pesquisadores e empresas.

Para iniciar, é preciso compreender o que é um bit quântico e no que ele difere de um bit convencional. Esta compreensão será fundamental para descortinar as possibilidades inimagináveis oferecidas pelos avanços conceituais e físicos da MQ.

Mas o que é um q-bit? A priori, pode-se definir um q-bit como um objeto matemático dono de certas propriedades específicas e, apesar de ser fisicamente intangível, ele existe. Nielsen e Chuang (2000, p. 13) descrevem que "a beleza de tratar q-bits como entidades abstratas é que [...] dá a liberdade de construir uma teoria geral da computação e informação quântica, que não depende de um sistema específico para sua realização".

Na teoria da informação quântica, o q-bit – quantum bit ou bit quântico – equivale ao bit dos computadores digitais e é utilizado como forma de medida para os computadores quânticos. Entretanto, o q-bit não se apresenta em apenas dois estados (0 ou 1), mas sob uma possibilidade infinita de estados superpostos e que não podem ser observados em objetos macroscópicos ou clássicos. Em outras palavras, significa que essa unidade de informação quântica é um vetor de estado em um sistema de MQ de dois níveis, normalmente, equivalente a um vetor de espaço bidimensional sobre os números complexos.

Nesse sistema, a forma de transmissão da informação (aqui com sentido de memória)

dá-se através de fótons excitados em um feixe de luz e movimentados para um material qualquer. Não se está considerando a longevidade, ou durabilidade, ou resistência do material, até porque a questão é ver as possibilidades de armazenar informações a nível molecular.

O fato de a computação quântica permitir uma instantaneidade dos dados faz com que os avanços conquistados continuem estimulando os especialistas e seja objeto de estudo de diversos institutos de pesquisas no mundo inteiro. No entanto, algumas incertezas persistem devido a obstáculos conceituais que se manifestam quando da aplicação prática da teoria.

A grande questão é que, para os físicos, ao se buscar uma informação, é necessário que haja uma medição do estado do q-bit. Isso feito, evidencia-se uma alteração de um estado, por conta da interferência direta no objeto medido, o que pode se tornar uma desinformação no estado alterado, e que, em tese, não afetaria a gravação original. As possibilidades de armazenamento, considerando o conceito da informação quântica, são imensuráveis, e esses questionamentos suscitam hipóteses para a sociedade da informação e o problema de recuperação, armazenamento, segurança e disseminação da informação sob esta nova visão: a computação quântica.

O que se evidencia com essa possibilidade que os princípios da MQ oferecem é que a memória, mais que ser preservada, poderá oferecer uma possibilidade bastante grande de armazenamentos em um estado magnético. Não se pode atestar, apesar de alguns experimentos bem sucedidos, que a preservação acontecerá de fato, mas não há como negar a exequibilidade que os avanços atuais podem permitir. Decerto que a preservação das memórias, diante dessas possibilidades, é bem ampla. Certamente, novos paradigmas serão discutidos, a partir do que a MQ poderá oferecer em termos de armazenamento, assim como a velocidade de transmissão e processamentos das imagens e sons. Vale ressaltar que as imagens e os sons são apenas um braço do oceano filosófico da representação do que é uma memória, mas será possível, com muita certeza, reproduzir-se, a partir do que estiver armazenado nos confins da quântica, um modelo que represente o estado e, por que não, o hábito e o sentimento de um ser humano em um determinado lugar do planeta.

## 3. O bit e o bit quântico

É relevante compreender que um computador clássico pode ser definido, de maneira bem superficial, como um equipamento capaz de "ler" um conjunto de dados codificados sob o sistema binário (0 e 1). Ou seja, é um dispositivo que recebe dados, processa, executa cálculos e dá, como resultado, uma saída também codificada em zeros e uns representados em bits. As operações desses bits são executadas por portas lógicas implementadas, fisicamente, por transistores, diodos e outros componentes eletrônicos. A excitação desse circuito, representado pelas portas encapsuladas em chips ou similares, é dada pela energia fornecida por uma corrente qualquer. Não é relevante especificar o tipo de corrente, mas a mecânica que envolve um computador é dependente da presença de bits e da eletricidade, para conservar o sistema de informações acumuladas.

O conceito de um bit pode ser traduzido como a magnetização de um anel de ferrite por uma corrente elétrica, isto é, o "0" representa um anel desmagnetizado ou estado de baixo potencial elétrico; o "1" é o anel magnetizado, ou estado com alto potencial elétrico. A ausência de corrente elétrica indica a impossibilidade de anéis magnetizados e, portanto, não há bits. Em outras palavras, o bit é uma manifestação física dependente da presença de um estímulo externo o qual, obrigatoriamente, é proveniente de uma fonte de energia que não pode ser interrompida. Ainda que esteja sob a forma de semicondutores, a simulação dos bits será sempre de dois estados: "baixo" (0) ou "alto" (1), inseridos em uma superfície magnetizável por meio de um pulso elétrico. Dessa maneira, a ausência da eletricidade identifica o não-bit e faz com que todos os dados armazenados sob esse modelo binário sejam apagados. Essa volatilidade aponta a necessidade de armazenamento das informações em dispositivos auxiliares como discos removíveis ou memórias. Isso exige a presença de um sistema de informações para efetuar a transcrição dos dados para os dispositivos móveis.

O fato é que os obstáculos que surgem com as novas teorias fazem com que as pesquisas sejam mais aprofundadas. Os novos estudos, mesmo possibilitando uma menor intervenção humana para a obtenção de um estado do q-bit, ainda mostra a incerteza na "leitura" de um dado inserido em um q-bit. As alternativas continuam surgindo para apresentar soluções quânticas e, de acordo com Piveta (2012), apesar de alguns estudiosos como Frederico Brito, do IFSCAR-USP, apontarem a possibilidade de criação de um chip quântico a partir de 128 anéis supercondutores mantidos a uma temperatura de 30 milikelvin,

o anel de ferrite continua sendo o mesmo princípio utilizado nos computadores clássicos.

Em tese, este chip quântico tornou-se possível por conta da simulação do *spin* para cima (|0>) [1] com o fluxo de corrente em um sentido e do *spin* para baixo (|1>), através da inversão da corrente. Ainda assim, permanece clara a dependência da energia elétrica para a manutenção deste sistema.

Em contrapartida, os q-bits armazenam as informações sem, necessariamente, haver um sistema computacional associado. É importante esclarecer que a computação aqui apontada não se refere aos procedimentos lógicos identificados em uma linguagem de programação, mas aos computadores ou dispositivos midiáticos munidos de processadores, os quais dispõem de um sistema operacional instalado capaz de renderizar sons, imagens ou telas para entrada de dados. Em outras palavras, o q-bit existe independentemente de haver alguma excitação externa, ao contrário do bit convencional que o explica como memória de conteúdo volátil. Por essa característica, é possível afirmar que o q-bit está mais próximo de ser um poderoso meio de armazenamento e processamento de dezenas de milhares de bits do que apenas um modelo representativo de entrada de dados.

Apesar de o q-bit poder existir em uma infinidade de estados, o resultado de uma medida do estado deste q-bit pode ser somente “0” ou “1”. Como um único número pode guardar uma infinidade de informações, seria possível guardar em q (orientação do q-bit) um ou uma coleção de livros. Essa possibilidade de armazenar de uma letra a milhares de textos permite afirmar de o q-bit poder ser considerado como um metabit[2] dos bits clássicos.

No entanto, ao medir o estado do q-bit pode-se obter somente “0” ou “1”, com uma determinada probabilidade. Ao realizar uma única medida, um observador poderá observar somente um dos estados “0” ou “1”, com sua respectiva probabilidade. Entretanto, se várias medidas forem feitas, após a primeira e no mesmo q-bit, o resultado das medidas posteriores serão sempre iguais ao resultado da primeira medida.

O problema desses processos de medições é que os estados são perturbados, leia-se

[1] *Spin* é, resumidamente, o movimento angular de elétrons quando envolvidos em um campo magnético. Na MQ a orientação dos spins são dadas pelas notações KET |n> e BRA <n|.
[2] O termo ***metabit*** dá significado ao *q-bit* capaz de definir outros bits de acordo com as mesmas propriedades de outros conceitos "meta”. Como um *metabit* é capaz de conter uma informação que pode definir outra informação, a propriedade deste *metabit* não poderá ser desvinculada do termo **metainformação.**

alterados, de forma irreversível, influenciando diretamente na informação armazenada possibilitando a esta, neste caso, ser tomada como uma **desinformação**. Por conta desse fato, Portugal (2010, p. 10) alerta que "não há como recuperar ou conhecer o estado antes da execução da medida. Se o estado não foi perturbado, então não foi possível obter qualquer informação sobre ele". A resposta a esse impasse está em um no Postulado da Medida da MQ o qual define que a probabilidade de se encontrar um valor “a” de um observável “A”, é dada após a realização de uma medida que pode ser entendida como uma interação que obriga uma partícula a assumir um determinado valor de alguma grandeza física.

Para explicar quanto de informação pode ser representada por um q-bit, Nielsen e Chuang (2000, p. 15) afirmam haver uma infinidade de pontos em uma esfera e somente isso seria suficiente para guardar textos imensos através da expansão binária infinita do ângulo $\theta$. Porém, como os autores alertam, "esta conclusão pode vir a ser enganosa por causa do comportamento de um q-bit quando observado" em um processo de medição.

## 4. Emaranhamento e superposição de estados

Para explicar medição, emaranhamento e superposição de estados, serão abordados conceitos físicos em nível macroscópico para o entendimento de seus significados. Considere-se o uso de dois objetos clássicos, como por exemplo, duas bolas, uma branca e a outra preta, que pertencem a dois personagens fictícios Alice e Bob.

Ao se colocar cada uma das bolas em uma caixa e lacrá-las sem identificar a cor no conteúdo delas, Bob pode pegar, aleatoriamente, uma caixa, enquanto a outra vai para Alice. Considere-se que os personagens se encontram distantes um do outro e não podem trocar nenhuma informação. Muito embora saibam de antemão a cor de cada bola, sem que as caixas sejam abertas ambos desconhecem a cor que está com cada um.

O ato de Bob abrir a sua caixa e verificar que está com a bola preta, imediatamente, se conclui que Alice está com a branca. Ou seja, Bob conhece o estado da partícula que está com Alice, realizando uma medida sobre a sua partícula, sem que haja comunicação entre eles. No entanto, Alice pode ainda desconhecer a cor da sua bola, ou seja, o estado da sua partícula, se não tiver aberto a sua caixa; mas tão logo o faça, saberá a cor (partícula) que está com Bob.

De forma semelhante, dois efeitos quânticos correlatos, a superposição de estados e o

emaranhamento, podem ser descritos como a representação dos mesmos personagens Alice e Bob. Cada um deles possui uma caixa fechada que contém uma bola, que pode ser branca ou preta sem ambos saberem anteriormente as cores das bolas. Antes de as caixas serem abertas, as bolas não têm cor definida, estando em uma 'superposição' de preto com branco, como se tivessem as duas cores ao mesmo tempo, e a cor de cada bola só se definirá no momento em que a caixa for aberta.

O entendimento de emaranhamento pode ser descrito em um fenômeno mais simples: imaginando-se, por exemplo, em uma margem de um rio, a existência de um bastão identificado como "1" e, na margem oposta, outro bastão representando o "0". Supondo-se a presença de uma onda em uma direção A-B perpendicular à margem tocando, simultaneamente, os bastões das duas margens, pode-se afirmar que a onda possui ambos os estados "0" e "1", por não haver a possibilidade de dissociação dos estados da onda. Em outras palavras, a onda possui estados superpostos.

Da mesma forma, presumindo-se agora o rio com outra onda na direção contrária da primeira, e que esta segunda onda toque os mesmos bastões fixados nas margens junto com a primeira, antes do efeito destrutivo das ondas, ambas estarão com os estados "0" e "1". Ou seja, as ondas estarão, por um pequeno instante, emaranhadas com estados superpostos pela impossibilidade de se saber a qual delas cada estado pertence. Esta representação também pode ser observada em um copo de café com leite ou, geneticamente, como o DNA dos pais em um filho onde a separação dos "observáveis" é algo complexo de ser efetuado. No entanto, na Física, a fragilidade do emaranhamento é uma das questões desafiadoras por conta da necessidade de isolamento térmico e eletromagnético para a manutenção do sistema.

## 5. A memória como processo de armazenamento no conceito do bit quântico

A memória pode assumir diversas definições, portanto serão consideradas, dentre todas as oferecidas, apenas as relevantes para a análise deste estudo (principalmente as voltadas para o campo semântico da Informática).

A informática teve inúmeras tentativas de preservação dos dados, sem ter que remeter à Máquina de Turing, quando, na década de 50, foram utilizadas as fitas magnéticas como um dos mais eficazes meios de retenção de dados. Essa tecnologia até hoje é utilizada largamente (principalmente em *mainframes*) por sua praticidade de manuseio. Foram muitos modelos em sua escala evolucionária, chegando ao cartucho, seu formato atual, com capacidade de armazenar até 40Gb.

Os dados armazenados em uma fita são lidos sempre sequencialmente por conta de seu formato tecnológico em que uma cabeça fixa lê ou grava os dados na trilha magnética a qual está em contato permanente com ela. Esse método, para as necessidades de seus usuários, era o responsável, em muitos casos, pelo aumento do tempo de processamento de uma informação. Ou seja, a linearidade para recuperar dados era custosa e demorada para a construção de uma informação e inviabilizava, economicamente, um processo.

Com o advento das cabeças móveis aplicadas aos discos rígidos, a leitura e a gravação de dados passaram a seguir uma metodologia diferente, mais rápida e eficaz. Os discos magnéticos surgiram com o conceito de divisão de trilhas e setores, gerenciados por uma trilha índice (trilha zero), para aperfeiçoar a forma de busca e armazenamento dos dados.

Este processo mostra uma não linearidade de captura de dados basicamente similar ao representado pelo raciocínio humano, uma vez que o cérebro é, também, dividido em áreas de atuação. As redes neurais atuais, também utilizadas nas tecnologias de armazenamento dos dados, estarão mais próximas do que pode ser a representação de memória humana, tratando-se de um estudo que não será edificado neste trabalho, por não ser um de seus focos. O fato é que as memórias humanas não parecem ser lineares para a construção do conhecimento. É necessário criar o conceito ou a impressão de um objeto "in-formação", como afirmou Boss (1975[3] apud CAPURRO, 2003), e ocorre dentro dos preceitos de construção lógica. A

[3] BOSS, M. Grundriss der Medizin und der Psychologie. Bern. 1975.

dificuldade está em representar esta forma não linear de pensamento, talvez randômico ou aleatório, que obedeça a outro padrão sequencial.

Deixar perpetuadas suas experiências levou o homem a buscar tentativas de memorizar coisas, desde o alvorecer das civilizações humanas, através de diversos objetos. Porém "foram os romanos que fizeram as primeiras publicações e criaram também bibliotecas parcialmente públicas, responsáveis pela disseminação do conhecimento grego em suas conquistas no período Helenista"[4]. Consequentemente, pode-se inferir que, na documentação das bibliotecas romanas, havia, então, uma padronização de armazenamento de dados, uma vez que o conhecimento grego, lá disponibilizado, podia ser encontrado separados de outros conhecimentos e de outras culturas.

No entanto a revolução de armazenamento de dados como uma biblioteca surgiu com Otlet (1937), a partir da idealização de uma central em que pudesse armazenar todos os documentos, concentrada em um Repertório Bibliográfico Universal (RBU), sob qualquer forma. Percebe-se nele o conceito de memória que, em resumo, é a "capacidade de adquirir (aquisição), armazenar (consolidação) e recuperar (evocar) informações [ou dados] disponíveis, seja internamente, no cérebro (memória biológica), seja externamente, em diversos dispositivos artificiais (memória artificial)"[5].

Entretanto, a preservação conduz ao armazenamento que leva em consideração as possibilidades e necessidades de espaços físicos cada vez maiores, dada a quantidade de dados, objetos e documentos a serem guardados. Isso nem sempre é possível porque alguns objetos, em seu estado físico natural, são impossíveis de serem movidos. Com esse enorme desafio, para haver a preservação, é necessário buscar alternativas (como imagens que possam reproduzir os objetos originais em equipamentos que imprimam em três dimensões) para proteger o que compõe a memória de nossa sociedade.

A saída encontrada para resolver parte do problema é a utilização dos meios magnéticos que, no que diz respeito à preservação de dados, tiveram uma evolução bastante acentuada, se for considerada a capacidade de armazenamento dos dispositivos midiáticos que fazem uso dessa tecnologia. Dentre esses equipamentos destacam-se, os *hard disk* (HD), hoje

[4] Disponível em: <http://nokhooja.files.wordpress.com/2010/08/tradicao-perene.pdf>. Acesso em: 23 maio 2012.

com capacidades superiores a 16TB (16 trilhões de bytes); os *compact disk* (CD), *digital vídeo disk* (DVD) com quatro camadas *(double dual layer*) atingindo 8,5Gb; as *pen drives* chegando à casa dos 256Gb e as placas holográficas capazes de reproduzir imagem em três dimensões.

Além das opções de *hardware* e *software* convencionais, as capacidades em volume de armazenamento tendem a aumentar, na medida em que novas possibilidades advindas dos avanços da Física permitem a utilização de novos componentes. Assim sendo, é possível armazenar filmes, músicas, imagens e toda a sorte de componentes que possam ser transformados em uma forma magnética que os represente. Desta maneira, os limites para armazenar fisicamente os dispositivos midiáticos são infinitamente maiores do que o local em que se podem guardar os documentos originais. Se for considerado que as imagens têm a possibilidade de ser arquivadas com base no conceito de *cloud computing*, ter-se-á a certeza de que não há mais limites para guardar e tampouco difundir e/ou divulgar informações.

Os dispositivos magnéticos, também citados, sugerem uma forma de representação, quando uma informação é armazenada e, por se tratar de meios magnéticos, os cuidados para manter a integridade física destes dispositivos são menos preocupantes: a tecnologia atual é uma fiel aliada da manutenção dos dados. Ao contrário do objeto real, o qual necessita de cuidados mais elaborados que vão da refrigeração à incidência de luz e do tratamento de fungos a tinta, o objeto virtual pode ser copiado, de um dispositivo a outro, tantas vezes quantas se desejar sem que haja a perda da integridade, qualidade e/ou significado do que está gravado. Além disso, é sempre possível que um usuário tenha o desejo de ter consigo, em seu computador pessoal, uma cópia da informação que considere relevante para sua vida profissional ou social. Isso significa que uma informação está sempre sendo preservada automaticamente em alguma esfera, em algum lugar e por alguém desconhecido. Sob este olhar, Zook observa uma

> manifestação óbvia da diminuição da importância da co-presença física e a emergência das comunidades virtuais, (cujo) [...] conceito é baseado na ideia de comunidades e grupos que coexistem e se comunicam, não através de uma proximidade física, mas por meio de uma grande variedade de Tecnologias de Informação. (ZOOK, 2006, p.61)

Evidentemente, a portabilidade e manuseabilidade desses materiais são bem mais

[5] Disponível em: <http://houaiss.uol.com.br/busca.jhtm?verbete=pragm%E1tica&stype=k>. Acesso em: 13 dez. 2012.

seguras e garantem a integridade do objeto que o originou. É clara a necessidade de se levar em consideração a segurança do que pode ou não ser sigiloso, disponibilizado ou divulgado, mas isso, em qualquer nível de análise, é sempre uma discussão a ser aprofundada em outras esferas. Até porque, há informações sigilosas e que não podem ser divulgadas livremente.

Capurro (2006), por causa das crescentes polidefinições de uma mesma imagem, apresenta a instigante ciência das mensagens, que chama de "angelética" (do grego "angelia" = mensagem), e o problema da transmissão e da permanência de mensagens da memória cultural, baseadas nas estruturas materiais (meios) e organizacionais denominada de "mediologia". Vê-se que, em qualquer nível de estudos, armazenar informação é um dos grandes problemas a serem resolvidos.

A preservação de memória e a tomada de decisões está em nossa sociedade atual bem representada pela grande rede – Internet – talvez até mais pontualmente pelo Google. Como um grande oráculo, sempre há uma resposta para qualquer questão dada por seres virtuais-reais situados em um lugar físico-geográfico não localizável, muitas vezes sem face, mas com uma resposta respaldada por outros que corroboram e ratificam suas afirmações.

A continuidade de nossa sociedade, atualmente, considerando a não extinção do planeta, está preservada, e o fato é que o que está em circulação precisa ser repensado como memória e, para isso, deve-se rever o verdadeiro significado do que é a representação desta memória.

A impressão que se tem, atualmente, é de que há uma vetorização de hipertextos em combinação com objetos imagéticos que conduzem a um não menos volumoso conjunto de informações (muitas sem sentido, nexo ou veracidade). Não se pode ter a certeza de que os oráculos dizem a verdade porque as respostas vêm através de um metadado que conduz a um endereço que pode desaparecer da mesma forma e com a mesma velocidade com que surgiu.

A memória, caso possa ser concebida como imagética e com cunho de informação, faz parte, agora, dos conceitos da sociedade da informação. Desta maneira, Lévy (2001, p. 34) traduz que se vive como “bits e bytes em uma descarga entrópica [que] substituem o imaginário bíblico em nome da urgência da sociedade da informação mediada pelas novas tecnologias.”

No entanto, independente de qualquer consideração, o fato é que, atualmente, o ponto

primordial para preservar a memória se dá através de dispositivos imagéticos que permitem o conceito de ubiquidade. Isso leva a pensar que Proust, segundo Brassäi (2005), em seus estudos de fotografia, talvez tivesse pressentido o fenômeno de inserção de imagens na rede. Tanto que Brassäi (2005) consegue visualizar uma relação entre memória e imagem que parece estar próximo a um breve acesso à Internet, a sites de imagens. Assim, tem-se a impressão de que a memória para Proust nada mais era do que senão uma imensa biblioteca de arquivos tão extensos que poderiam ser "um tesouro desconhecido escondido bem ao nosso alcance, porém quase inacessível" (BRASSÄI 2005, p.155-156). Como afirma Silva Filho (2010, p. 86), “propor que as imagens na rede são além de arquivos, tesouros, é passear por um mundo novo de conceitos do âmbito do audiovisual atrelado as novas tecnologias”.

Face a face com um monitor ou modernos aparelhos celulares, agora *smartphones*, *tablets* e *iPods*, o ser humano, com câmeras, tornou-se um produtor de imagem de tal maneira que pode memorizar, transmitir e distribuir pela Internet seus produtos e tudo o que lhe perpassa pela mente e pelos olhos. Vive-se um verdadeiro totalitarismo dos aparelhos em miniatura, cujo aspecto instrumental do aparelho passa a ser desprezível. O que conta, segundo Flusser (1998, p.47), e confere valor a um equipamento "são as virtualidades contidas nas regras: o *software* (...)" fazendo o poder passar do "proprietário para o programador de sistemas" na ânsia da magia imagética. É a era dos chamados bigdados!

Inevitavelmente, a leitura de uma imagem, quer seja uma foto ou uma pintura, e graças a seu código de conotação, dependerá "sempre do 'saber' do leitor como se fosse uma verdadeira língua, inteligível apenas para aqueles que aprenderam seus signos" (BARTHES,1990, p.22). Interpretar uma imagem necessita de conhecimento técnico, tal como Aumont observa:

> se a imagem contém sentido, este tem de ser lido por seu destinatário, por seu espectador: é todo o problema da interpretação da imagem(...) [As] imagens, visíveis de modo imediato e inato, nem por isso são compreendidas com facilidade, sobretudo se foram produzidas em um contexto afastado (...) no espaço ou no tempo, as imagens do passado costumam exigir mais interpretação. (AUMONT, 2002, p.250)

Em suma, isso parece ser o que os astrofísicos estão habituados a fazer ao "lerem" as imagens enviadas e fotografadas pelos telescópios espaciais e percebem a presença de uma ausência, por exemplo. A Internet tem a arte de seduzir, atrair e entender (como nunca) as imagens criadas por ela. No entanto, o fenômeno da utilização das imagens, com movimento, na rede, é relativamente recente e, consequentemente, ainda pouco estudado.

Em seus estudos, Kerckhove[6] (apud SILVA FILHO, 2010, p. 87) percebe que o homem mudou, e por causa desse bombardeio de imagens, afirma que “um novo ser humano está para nascer”, e esse sentimento parece ter no dispositivo imagético uma constatação. Sem dúvida, com base nessas evoluções que aconteceram tão rapidamente na distribuição e divulgação de imagens, pode-se afirmar que esse "novo ser humano, através de suas tecnologias, é um ser-da-memória. [Consequentemente], um novo ser humano parece nascer na rede mundial de computadores, [quase como] um homem-máquina que se pauta pela interação" (SILVA FILHO, 2010, p. 87).

Atualmente, é possível e permissível interagir com imagens, isso ajuda a resolver alguns porquês e algumas preocupações. Se se imaginar as maneiras pelas quais podem-se obter uma informação e os alcances que estas podem atingir, é igualmente possível admitir que a memória esteja cada vez mais e mais social. As imagens finais de diversos sites e páginas, a toda hora, convidam, de forma encantadora, o usuário a convergir para a memória recente ou não. Este relacionamento integrado entre a imagem e a memória, considerando o ambiente virtual, pode

> traduzir para o homem hiperconectado uma nova forma de ler o mundo. (...) A Internet não se trata mais somente de uma biblioteca de babel com o registro imagético invadindo a rede mundial de computadores, ela relaciona-se com uma nova configuração da memória. De uma memória individual para uma nova conexão com o outro. (SILVA FILHO, 2010, p. 87)

O estudioso da memória McLuhan (1964) apresenta a concepção do prolongamento da consciência não se dar apenas com o acúmulo conhecimento, “mas, principalmente, com as novas possibilidades de rearranjar tais conhecimentos, através das mídias eletrônicas” favorece a passagem de conectar a materialidade à memória (PEREIRA, 2004[7] apud SILVA FILHO, 2010, p. 87).

Por sua vez, Bergson (1999, p. 88) "não atribui ao cérebro nem a função de 'representar' ideias, nem mesmo a função de arquivar lembranças. É nesse sentido que [se pensa] a relação entre memória e as novas imagens na rede mundial de computadores". De acordo com ele, “ao mais ínfimo movimento do objeto ou dos olhos, já não haveria uma imagem, porém dez, cem, mil imagens, tantas quantas numa película cinematográfica ou

[6] KERCKHOVE, D. **A pele da cultura**. Lisboa: Relógio d'água, 1997.
[7] PEREIRA, V. A. Consciência e memória como objetos da comunicação. **Revista Famecos**, Porto Alegre, n. 24, 2004.

mais...” (BERGSON, 1999[8] apud ROSENFELD, 1988, p. 13). Esse pensamento é corroborado por Deleuze (1985, p. 315), ao afirmar que “a própria tela (...) não parece mais remeter à postura humana, como uma janela ou ainda um quadro, mas constitui antes uma mesa de informação, superfície opaca sobre a qual se inscrevem “dados””.

Ainda nesta mesma linha de raciocínio, Silva Filho (2010), aponta que Huyssen (2000, p. 33) idealiza uma “arqueologia de dados” e acredita que essas imagens contemplam um novo objeto da memória. O fato é que, se o fenômeno da desterritorialização da informação é um consenso, pode-se, então, ter a certeza absoluta de que, a qualquer momento, tem-se a oportunidade de reavivar a memória através de um vídeo ou em um dispositivo imagético. A memória passa a ter o sentido dinâmico, a partir do momento em que encontra outra imagem que represente uma memória com movimento.

Não há dúvidas de que a Internet se constitui como o novo acervo e gigantesco arquivo da memória na atualidade. O grande problema continua sendo a guarda e o armazenamento.O fato é que os computadores atuais, mesmo com as notáveis evoluções tecnológicas, aproximam-se de limitações que exigem de especialistas novas buscas por soluções que deem velocidade e segurança aos seus usuários. Daí os pensamentos tecnicistas, de empresas e pesquisadores, voltarem-se para a computação quântica a qual permite infindáveis possibilidades de processar e armazenar grandes volumes de informações.

Ao se analisar a evolução dos computadores quânticos, pode-se observar significativos avanços, tanto como ciência pura como aplicada. De acordo com Oliveira et al (2003), os computadores digitais estão chegando ao limite de suas capacidades e, por isso, é necessário pesquisar outras formas de suprir as dificuldades que estão prestes a chegar. Para isso, a solução natural foi pensar

> em um modelo de computação baseado nas leis da mecânica quântica [que] (...) resultaram na descoberta de procedimentos de cálculos quânticos capazes de realizar em minutos ou horas tarefas que levariam bilhões de anos em computadores clássicos, e fizeram eclodir uma busca febril em todo o mundo pela compreensão e manipulação da chamada “informação quântica”. (OLIVEIRA et al.; 2003, p. 22)

[8] BERGSON, H. **Matéria e memória**. São Paulo: Martins Fontes, 1999.

## 6. Criptografia quântica

Qualquer modelo de preservação de memória, quer esteja sob a tutela da computação quântica ou não, requer a segurança da informação. Existem vários tipos de criptografias que foram desenvolvidas como maneira de preservar determinados dados de possíveis predadores. Alguns seguiram modelos simétricos, outros assimétricos, mas, atualmente, a investigação tem sido pela criptografia quântica a qual tem como base o princípio de incerteza de Heisenberg. Dessa forma, é possível usar duas mensagens em uma única transmissão quântica porque o receptor poderá ler apenas uma mensagem de cada vez e nunca as duas simultaneamente. Para compreender essa definição, baseada em Heisenberg, basta imaginar que não se pode conhecer a velocidade e posição de uma partícula em uma mesma medida (como por exemplo, o caso de uma única foto em que não pode afirmar, na maioria dos casos, se o objeto está ou não em movimento). Isso significa que sempre haverá uma incerteza no mundo subatômico e é daí que a criptografia quântica se aproveita para se desenvolver utilizando pares de fótons.

Esse modelo permite que duas pessoas desconhecidas e sem contato algum criem suas próprias chaves secretas e as envie através dos fótons. Se por acaso esses fótons sofrerem qualquer tipo de interferência durante a transmissão, haverá uma alteração no estado do fóton fazendo com que as chaves enviadas não sejam percebidas pelo receptor que poderá interromper a transmissão dos dados.

No entanto, apesar de parecer ser o ideal para evitar a interceptação de mensagens, os problemas enfrentados ainda são muito complexos de serem resolvidos. Por exemplo, apesar de vários estudos, ainda não se conseguiu alcançar grandes distâncias, mesmo como uso de fibras ópticas de grande pureza. Outra limitação encontrada está na fragilidade e suscetibilidade à interferência de ruídos, provocadas pelo meio físico em que a transmissão acontece. Isso envolve tanto a transmissão via satélite quanto por cabos.

O que seria uma limitação para o uso da criptografia quântica é a necessidade de haver entre o emissor e o receptor o mesmo tipo de equipamento (como os interferômetros) que efetuasse a leitura dos fótons para validar a comunicação, aparentemente foi resolvida. Porém, O'Brien (2007), descobriu a possibilidade de efetivar a criptografia quântica entre dispositivos móveis. Seu estudo aponta que somente um dos envolvidos na transmissão necessita de possuir o equipamento de óptica quântica como uma fonte de fótons. Significa que o emissor

cria os fótons e depois os envia através de uma fibra óptica comum para o receptor que modifica os fótons codificando-os com informações antes de devolvê-los ao emissor. Isso simplifica consideravelmente o equipamento de que o receptor precisa, permitindo o modelo caber em um dispositivo portátil.

Ainda que as soluções ainda estejam em um nível não comercial, os estudos avançam e desafiam os estudiosos. Apesar de ser ainda algo intangível, conseguir esse modelo criptográfico é a meta de vários institutos de pesquisa, por ser o melhor de todos os conhecidos e, em tese, impossível de ser descriptografado.

Assim, preservar memória em computadores quânticos utilizando a criptografia quântica são os objetivos que se deseja alcançar. Considerando se tratar de um grande conjunto de hipóteses que devem ser tratadas e estudadas com especialistas experientes nesta área, não há, de fato, muito a ser apresentado senão as possibilidades que podem ser alcançadas e conquistadas com esta pesquisa.

## Referências

AUMONT, J. **A imagem**. 7. ed. Campinas, São Paulo: Papirus, 2002.

BARTHES, R. **O óbvio e o obtuso**: ensaios críticos III. Rio de Janeiro: Nova Fronteira, 1990.

BRASSÄI, G**. Proust e a fotografia**. Rio de Janeiro: JZE, 2005.

CAPURRO, R. **Foudantions of information science**. 2003. Disponível em: <http://www.capurro.de/tampere91.htm>. Acesso em: 13 jun. 2017.

_____. Towards an ontological foundation of information ethics. **Ethics and Information Technology**, v. 8, p. 175-185, Springer 2006. Disponível em: <http://www.springerlink.com/content/f128473n7141m6m6/>. Acesso em: 19 nov. 2011.

DELEUZE, G. **A imagem-tempo.** São Paulo: Brasiliense, 1985.

ELDRED, M. **The digital cast of being**: metaphysics, mathematics, cartesianism, cybernetics, capitalism, communication. Cologne: Artefact, 2009. Disponível em: <http://www.arte-fact.org/dgtlon_e.html>. Acesso em: 26 ago. 2017.

FLUSSER, V. **Ensaio sobre a fotografia**: para uma filosofia da técnica. Lisboa: Relógio D'Água, 1998.

HUYSSEN, A. **Seduzidos pela memória**. Rio de Janeiro: Aeroplano, 2000.

LÉVY, P. **Cibercultura**. São Paulo: 34, 2001.

MCLUHAN, M. **Os meios de comunicação como extensões do homem**. São Paulo: Cultrix, 1964.

NIELSEN, M. A; CHUANG, I. I. **Quantum computation and quantum information**. London: Cambridge University Press, 2000.

O'BREIN, J. L. Optical Quantum Computing. **Science**, v. 318, p. 1567-1570, 07 dez. 2007. Disponível em: <http://science.sciencemag.org/content/318/5856/1567/tab-pdf>. Acesso em: 20 out. 2011.

OLIVEIRA, I. S. et al. Computação quântica: manipulando a informação oculta do mundo quântico. **Ciência Hoje**, Rio de Janeiro, v. 33, n. 193, p. 22-29, 2003. Disponível em: <http://www.cbpf.br/~qbitrmn/divulgacao/artigo_CH.pdf>. Acesso em: 20 dez. 2011.

OTLET, P. **Documentos e documentação**: introdução aos trabalhos do Congresso Mundial da Documentação Universal, realizado em Paris. 1937. Disponível em: <http://www.conexaorio.com/biti/otlet/index.htm>. Acesso em: 13 out. 2011.

PIVETA, M. A nova onda dos qubits. **Revista Pesquisa FAPESP**, São Paulo, ed.193, 2012. Disponível em: <http://revistapesquisa.fapesp.br/wp-content/uploads/2012/03/052-0571.pdf>. Acesso em: 03 nov. 2012.

PORTUGAL, R. **Códigos quânticos**. Petrópolis: Rio de Janeiro: Laboratório Nacional de Computação Científica, 2010. Disponível em: <http://www.lncc.br/~portugal/CodigosQuanticos.pdf>. Acesso em: 10 set. 2012.

ROSENFELD, I. **A invenção da memória**. Rio de Janeiro: Nova Fronteira, 1988

SILVA FILHO, W.O. **O youtube e a memória**: **um arquivo para além das mensagens**. Rio de Janeiro: ARTEFACTUM, 2010. Disponível em: <http://artefactum.rafrom.com.br/index.php/artefactum/article/view/83>. Acesso em: 05 jan. 2011

VEDRAL, V. **Decoding reality**: the universe as quantum information. Oxford: Oxford University Press, 2010.

ZOOK, M. The geographies of the Internet. **Annual Rewiew of Information Science and Technology**, Medford, v. 40, p. 53-78, 2006.

Artigo submetido em: 07 fev. 2017
Artigo aceito em: 06 jun. 2018