



Informação e teoria quântica

Olival FREIRE JUNIOR & Ileana Maria GRECA



RESUMO

A pesquisa em informação quântica sugere uma íntima conexão entre o conceito de informação e a teoria quântica, mas essa conexão envolve nuances cuja análise é o objeto deste trabalho. A sabedoria comum nesse campo divide-se em duas grandes áreas, não excludentes entre si. Há os que são movidos pela possibilidade de uso da teoria quântica em um novo campo, o da computação, independentemente do esclarecimento de seus fundamentos, aqui incluído o conceito de “informação”. Alguns consideram que estamos diante de um grande problema conceitual sem resposta satisfatória no momento, enquanto que outros, dentre os que reconhecem a magnitude do problema, têm proposto formulações com a pretensão de solução do problema. Este artigo tem pretensões modestas. Não pretendemos aportar novas soluções ao problema, nem apoiar uma das soluções existentes. Temos a expectativa de através da análise histórico-conceitual do problema mapear as diversas possibilidades, apontando o que nos parecem ser aspectos fortes e fracos nessas possibilidades.

PALAVRAS-CHAVE • Teoria quântica. Informação quântica. Informação. Entropia. Conferências de Oviedo. Emaranhamento. Teleportação.

INTRODUÇÃO

A pujança do campo de pesquisa, quiçá uma disciplina, denominado de “informação quântica” sugere uma íntima conexão entre o conceito de “informação” e a teoria quântica. Essa conexão, contudo, envolve nuances cuja análise é o objeto do presente artigo. De fato, veremos que uma delas é a possibilidade de exploração de propriedades estritamente quânticas, em especial o emaranhamento, para fins de computação, seja para criptografia seja para processamento bem mais veloz que os que podem ser concebidos na computação usual. Nessa nuance, certamente a dominante na informação quântica, o conceito de “informação” deve ser compreendido como associado ao procedimento de cálculo do conteúdo informacional dos estados quânticos, de onde a expressão “*qubit*” por analogia à conhecida expressão “*bit*”. Enquanto um *bit* carrega uma unidade de informação através de um circuito que está ligado ou desligado, um *qubit* carrega uma unidade de informação no estado quanto-mecânico de dois níveis, a exemplo daquele associado à polarização de um fóton, com o estado descrito pela superposição de auto-estados associados às polarizações vertical e horizontal. Nessa linha,

os pesquisadores da informação quântica usam tipicamente a teoria da informação de Shannon com a mesma propriedade com a qual a ciência da informação e a engenharia de telecomunicações usam essa mesma teoria para analisar os atuais dispositivos de processamento, armazenamento e transmissão de informações. Uma segunda nuance sugere, contudo, que a informação seria o próprio objeto da teoria quântica. Nessa direção, por tratar-se da interpretação do formalismo da teoria quântica, bem como da definição de seu objeto, estamos lidando com o campo de fundamentos da teoria quântica. Nesse sentido, a discussão sobre o significado da informação no campo da informação quântica não é independente dos debates sobre a interpretação da própria teoria quântica. Ademais, como argumentado por Anton Zeilinger, um dos físicos que tem trabalhado na segunda direção, a teoria da informação de Shannon revelar-se-ia inadequada ao objetivo de compreender a quântica como uma teoria cujo objeto seria a informação.

A possibilidade de conexão entre a informação e o objeto da teoria quântica não é nova, remontando aos debates, especialmente entre Einstein e Bohr, que se seguiram à criação da teoria no final da década de 1920. Aqueles familiarizados com os debates sobre a interpretação da teoria quântica reconhecerão nas expressões “interpretação epistêmica” e “interpretação ontológica” o prenúncio dos problemas atuais. Contudo, foi a criação do campo da informação quântica em meados da década de 1990 que alterou dramaticamente os termos do debates sobre essa conexão. Curioso notar que o próprio campo da informação quântica emergiu como uma mescla entre cientistas e engenheiros ligados à ciência da informação e a problemas dessa área, de um lado, e cientistas ligados ao campo dos fundamentos da teoria quântica, de outro. Essa mescla aparece tanto na lista dos principais resultados que constituíram o campo como na configuração dos espaços institucionais, eventos e revistas, nos quais ele se desenvolveu. A sabedoria comum nesse campo, no que diz respeito ao estatuto da informação, divide-se em duas grandes áreas, não excludentes entre si. Há os que são movidos pela possibilidade de uso da teoria quântica em um novo campo, o da computação, independentemente do esclarecimento de seus fundamentos, incluindo-se nisso o conceito de “informação”. Esses autores assemelham-se a boa parte da geração que sucedeu os criadores da teoria quântica, a qual se lançou na aventura das aplicações da nova teoria científica, sem maiores preocupações com o bom fundamento de suas bases. Alguns autores consideram que estamos diante de um grande problema conceitual sem resposta satisfatória no momento, enquanto outros, dentre os que reconhecem a magnitude do problema, têm proposto formulações com certa pretensão de tê-lo solucionado. Mais recentemente, novos desenvolvimentos no campo de fundamentos da teoria quântica, como o teorema PBR, publicado em 2012, têm reaquecido tanto o debate sobre as interpretações da teoria quântica quanto o estatuto do conceito de “informa-

ção” no âmbito dessa teoria. Esse último problema, que é o foco de interesse deste artigo, revela-se central em uma fronteira do conhecimento que mobiliza tanto desenvolvimentos científicos teóricos e experimentais, incluindo potencialidades tecnológicas, quanto aspectos conceituais e filosóficos, renovando aquilo que o físico e filósofo Abner Shimony uma vez denominou de “metafísica experimental”.

Este artigo está organizado como segue. Na primeira seção, faremos uma breve resenha histórica de como o conceito de “informação” apareceu nos debates sobre a interpretação da teoria quântica. Na segunda seção, faremos um resumo dos principais marcos que levaram à configuração do campo da informação quântica. Na terceira, analisaremos a mescla do campo de fundamentos com o emergente tema da informação quântica através da análise de um ambiente institucional específico, o das conferências de Oviedo, realizadas em 1993, 1996 e 2003, naquela cidade da Espanha. Na quarta seção, apresentaremos algumas das posições recentes influentes no debate sobre a relação entre a informação e a teoria quântica, em particular, as posições de Anton Zeilinger, John Archibald Wheeler, Christopher Fuchs e Wojciech Zurek. Por fim, concluiremos avaliando a extensão da centralidade do conceito de informação na teoria quântica.

1 A INFORMAÇÃO NOS DEBATES INICIAIS SOBRE A TEORIA QUÂNTICA

Desde os primeiros debates sobre a interpretação física do formalismo matemático da teoria quântica estavam presentes referências ao conceito de “informação”, embora esse conceito não estivesse no centro das controvérsias. Muito do debate deve ser referido à disputa entre Albert Einstein e Niels Bohr sobre a consistência e a completude da nova teoria física.¹ A incompletude da teoria, sustentada por Einstein, implicava que a teoria trazia uma informação incompleta sobre os sistemas físicos por ela descritos. Em uma comparação que se tornou padrão, Einstein lembrava do exemplo da mecânica estatística, a qual descreve um agregado de um grande número de sistemas, enquanto os sistemas são descritos individualmente pela mecânica clássica. Desse modo, as médias estatísticas que comparecem na mecânica estatística refletem um conhecimento insuficiente do número muito grande de sistemas individuais, os quais, entretanto, são descritos de forma determinista pela mecânica clássica. Conforme Einstein,

¹ A literatura sobre os debates entre Einstein e Bohr é extensa. Para uma introdução básica, embora já um pouco desatualizada em face de novas publicações, cf. Jammer, 1974.

Eu estou, de fato, firmemente convencido que o caráter essencialmente estatístico da teoria quântica contemporânea deve ser atribuído exclusivamente ao fato que esta teoria opera com uma descrição incompleta dos sistemas físicos (Einstein, 1982, p. 666).

Na analogia feita por Einstein, e tornada clássica entre muitos críticos da teoria quântica, a mecânica estatística correspondia à teoria quântica, restando por ser formulada uma teoria mais básica que servisse de fundamento à teoria quântica tal como a mecânica clássica serviria de fundamento à mecânica estatística. Nessa linha de raciocínio, portanto, a interpretação probabilística para os estados quânticos (as funções de onda), sugerida por Max Born, seria uma interpretação estatística, expressando a insuficiência da informação sobre os sistemas incorporados nos estados da teoria quântica.

Para Niels Bohr, o problema da completude da teoria quântica era um falso problema, pois ele interpretava a teoria como sendo a descrição adequada e necessária dos fenômenos que podiam ser seu objeto. Isso não significava que a teoria quântica fosse uma teoria final, e o próprio Bohr, mais de uma vez, proclamou a iminência de novas revoluções na física, ao lidar com fenômenos como as novas partículas subnucleares que começaram a ser sugeridas ou descobertas a partir da década de 1930. Para Bohr, contudo, os fenômenos relacionados à radiação e sua interação com a matéria, o que ele denominava de “física atômica”, eram adequadamente descritos pela teoria quântica, mas em uma abordagem radicalmente distinta daquela que tinha sido subjacente à descrição física até então (cf. Freire Jr., 1999, p. 35). Ele batizou essa abordagem de “princípio da complementaridade”. Embora a abordagem tenha sobrevivido no senso comum da física em uma forma excessivamente simplificada, a da dualidade onda-partícula, Bohr reportava-a a uma complementaridade entre tipos de informação que podíamos obter sobre os sistemas físicos. Para o físico dinamarquês,

a informação referente ao comportamento de um objeto atômico obtida sob condições experimentais definidas pode (...) ser adequadamente caracterizada como complementar a qualquer informação sobre o mesmo objeto obtida por algum outro arranjo experimental excluindo os requisitos das primeiras condições. Embora tais tipos de informação não possam ser combinadas em uma única representação por meio de conceitos ordinários, efetivamente elas representam aspectos igualmente essenciais de qualquer conhecimento do objeto em questão que possa ser obtido nesse domínio (Bohr, 1987, p. 26).

No que pese as indicações acima sugerirem que tanto no pensamento de Einstein quanto no de Bohr a noção de “informação” tinha significados, ainda que distintos, relevantes, esse tema não foi motivo de reflexões mais aprofundadas, porque era o tema da completude da teoria quântica que dominava as atenções. O cenário não se alteraria substancialmente mesmo na década de 1950, quando o interesse nos fundamentos da teoria quântica foi reavivado a partir do trabalho de David Bohm, que sugeriu uma interpretação causal e, portanto, uma interpretação alternativa à da complementaridade, para essa teoria. O pouco interesse no tema pode estar associado ao fato de que maioria dos físicos, que passou a trabalhar no campo dos fundamentos até fins da década de 1970, professava uma perspectiva realista a propósito da teoria quântica. Por outro lado, também deve ser notado que foi apenas a partir do final da década de 1940, com os trabalhos de Claude Shannon, que uma teoria da informação tornou-se disponível.² Isso pode ter dificultado o desenvolvimento de uma reflexão sobre o estatuto da informação na teoria quântica pelo próprio fato de que as abordagens realistas dessa teoria têm naturalmente muita dificuldade em atribuir uma centralidade ao conceito de “informação”. Afinal, tradicionalmente, a informação que obtemos de um sistema físico deveria ser apenas um reflexo ou representação de sistemas e propriedades existentes independentes dos meios utilizados para interagirmos com os sistemas. Não é por acaso que adquiriu tanta popularidade a pergunta de Einstein: “a Lua não está lá quando não a estamos observando?” O cenário mudaria ao longo da década de 1980 e, especialmente, a de 1990, tanto pela atividade de físicos como Wheeler, com a sua afirmativa - “*it from bit*” - que colocou o problema em novos termos.

2 MARCOS NA CONFIGURAÇÃO DO CAMPO DA INFORMAÇÃO QUÂNTICA

Quando se procura o que se entende como “informação quântica” e “computação quântica” encontramos, invariavelmente, que são definidas como o estudo das tarefas de processamento da informação que podem ser desenvolvidas usando sistemas quântomecânicos. Embora óbvia, essa definição permite que delineemos os três campos principais que têm contribuído para sua emergência como disciplina autônoma a partir de meados dos anos 80. Esse delineamento que toma como ponto de partida a década de 1980 é, contudo, um mapeamento que busca pelas raízes conceituais do novo campo. A emergência com uma identidade própria, número expressivo de novos pesquisado-

² Dentre os poucos trabalhos dedicados ao tema da informação no período, cf. Wigner & Yanase, 1963, e as referências ali indicadas. Sobre o realismo entre os físicos que trabalham nos fundamentos da teoria quântica, cf. Freire Júnior, 2009, p. 288.

res e instituições, e crescimento significativo de financiamento ocorreria apenas a partir de meados da década de 1990.

Na linha histórica, o primeiro campo é a teoria quântica e, sobretudo, as discussões conceituais e os desenvolvimentos experimentais relacionados com o experimento de pensamento sugerido por Einstein, Podolsky e Rosen (EPR) em 1935 e o Teorema de Bell de 1964, que contrapôs a teoria quântica às premissas do realismo local. Emerge dessa vertente o primeiro grande resultado, o da não clonagem dos sistemas quânticos, ou seja, os estados quânticos não podem ser copiados com perfeita fidelidade. Esse resultado foi obtido de forma independente, em 1982, por Wootters e Zurek (1982) e por Dieks (1982). A demonstração, embasada na linearidade da mecânica quântica, bastante simples,³ e que poderia ter sido desenvolvida muito antes, somente se deu no contexto dos debates sobre situações tipo EPR. Nick Herbert (1982)⁴ tinha feito circular um trabalho, escrito em 1980, em que propunha um mecanismo para enviar sinais superluminais usando o emaranhamento dos estados EPR (cf. Kaiser, 2011). Os trabalhos de Wootters e Zurek, e de Dieks eram respostas ao desafio lançado por Herbert. A clonagem poderia permitir a determinação do estado de um sistema a partir de medições em uma coleção de cópias suas (portanto, sem interferir no estado original), mas isso abriria a possibilidade de sinais superluminais em estados emaranhados. Assim, poderíamos ser capazes de distinguir entre diferentes preparações da mesma matriz densidade e, por tanto, determinar superluminalmente qual foi a medição realizada na outra metade do par EPR. É interessante também notar que, inicialmente, Wootters e Zurek tinham pensado enviar o artigo a uma revista de baixo impacto, possivelmente pela simplicidade de sua dedução assim como pelo baixo apelo que as questões sobre os fundamentos tinham entre os físicos naquela época. Foi Wheeler quem, além de dar-lhes o título,⁵ incentivou-os a enviá-lo ao periódico *Nature* (cf. Kaiser, 2011).

Embora em nenhum dos dois trabalhos o teorema seja relacionado com a teoria da informação ou com a computação,⁶ esse teorema da impossibilidade de clonagem estabelece uma das distinções essenciais entre a informação clássica e a quântica e

³ Uma forma simples de compreender o teorema da não clonagem é pensá-lo na sua relação com o princípio de incerteza. Se fosse possível clonar um estado desconhecido, então se poderia fazer tantas cópias quantas se desejasse e medir, em cada uma delas, cada variável com precisão arbitrária, violando, dessa forma, o princípio de incerteza.

⁴ Herbert pertencia ao Fundamental Fysics Group, um grupo informal de físicos jovens que, na década de 1970, contribuíram para reavivar nos Estados Unidos os debates sobre os fundamentos da mecânica quântica. Para a história desse grupo e de seus aportes à física, cf. Kaiser, 2011.

⁵ Wheeler era conhecido por cunhar nomes de grande impacto. São dele, além de “clonagem”, e do “*It from bit*”, também “buraco negro”.

⁶ Os primeiros trabalhos a citarem o trabalho do Wootters e Zurek da não clonagem estão quase todos relacionados com os debates sobre o EPR e não com a informação ou a computação. Também, no mapa das citações, é possível observar que o número de citações desse trabalho dispara a partir de 1998: até 1997, o artigo é citado 96 vezes; desde 1997 até 2012, 1396, agora em relação direta com o novo campo da informação quântica.

implica limitações à computação quântica, sobretudo, relacionadas com as técnicas clássicas de correção de erros (criação de cópias dos arquivos originais).⁷ Cabe salientar que um pouco antes, Wootters e Zurek (1979) haviam escrito um artigo, incentivados pelo seu mentor John Archibald Wheeler, onde usavam ideias da teoria da informação clássica, em particular, a medida da perda de informação de Shannon, por ser “uma linguagem apropriada” para discutir fenômenos intermediários entre onda e partícula no experimento da dupla fenda. Nesse trabalho, eles indicam que as noções de informação já haviam sido usadas com sucesso na mecânica quântica, citando a tese de Hugh Everett, defendida em 1957, mas só publicada na íntegra em 1973.⁸

Por outra parte, o campo que hoje se denomina de informação e computação quântica não poderia ter emergido sem o desenvolvimento das novas técnicas experimentais em ótica quântica, física atômica e física da matéria condensada, as quais permitem manipular e estudar sistemas quânticos simples (cf. Nielsen & Chuang, 2010). Várias dessas técnicas têm uma estreita vinculação com a verificação experimental das desigualdades de Bell (cf. Bromberg, 2006; Freire Jr., 2006); e permitiram, de forma singular, a implementação do emaranhamento de estados quânticos, ferramenta indispensável para a computação quântica.

Outro dos campos derivou diretamente nas ciências da computação. A ciência da computação moderna tem sua origem no trabalho de Alan Turing (1936), no qual se estabelece que qualquer função computável pode ser desenvolvida por um certo procedimento universal, a chamada “máquina universal de Turing”, que captura, assim, de forma completa, o que significa desenvolver uma tarefa mediante algoritmos. E, de fato, até hoje não se descobriu nenhum cálculo algorítmico que não possa ser implementado em uma máquina de Turing. A tese de Church-Turing diz justamente que uma função é algorítmicamente computável se e somente se ela é computável em uma máquina de Turing. Ou seja, se um algoritmo pode ser realizado em qualquer peça de hardware, então existe um algoritmo equivalente para uma máquina universal de Turing que realiza exatamente a mesma tarefa que o algoritmo inicial. Isso estabelece uma equivalência entre o conceito físico da classe de algoritmos que podem ser realizados em algum dispositivo físico com o conceito matemático da máquina universal de Turing (cf. Nielsen & Chuang, 2010), equivalência que está na base dos desenvolvimentos tecnológicos relacionados com a computação digital.

Com o desenvolvimento de hardwares cada vez mais poderosos, começou uma preocupação com os problemas que o tamanho dos componentes, cada vez mais pequenos, poderiam ter ao se atingir o limite entre a física clássica e a quântica. Uma

⁷ Peter Shor (1996) e Andrew Steane (1996), contudo, desenvolveram de forma independente um código de correção de erros que pode “contornar” o teorema da não clonagem.

⁸ Sobre a distinção entre a tese original e a versão publicada em 1957, cf. Osnaghi, Freitas & Freire Júnior, 2009.

solução a esse respeito seria mover-se diretamente para um paradigma diferente de computação, usando a mecânica quântica para realizar computações em lugar da física clássica. Na conferência “Physics and computation”, organizada no MIT em maio de 1981, aparecem dois trabalhos que apontam nesse sentido. Um deles, de Paul Benioff (1982), propunha um modelo de computação semelhante a uma máquina clássica de Turing, mas usando a dinâmica da mecânica quântica (cf. Yeang, 2011). O outro, de Richard Feynman (1982), considerava que somente um computador embasado na mecânica quântica poderia simular, de forma eficiente, as operações da própria mecânica quântica. Embora um computador quântico não possa fazer nada que um computador clássico não possa fazer, ou seja, a noção de computável é a mesma para ambos, a eficiência para simular um sistema quântico não é igual. Um computador clássico precisa uma quantidade ingente de memória para cobrir todo o espaço de Hilbert (para representar um sistema quântico com 100 *qubits*, é necessário escrever 2^{100} números complexos) o que é inviável em qualquer computador embasado na física clássica (cf. Preskill, 2004).

A ideia de Feynman,⁹ ao apelar para a teoria quântica, colocava em questão a versão forte de tese Church-Turing, a saber, que qualquer processo algorítmico poderia ser simulado eficientemente usando a máquina universal de Turing (cf. Nielsen & Chuang, 2010), se essa máquina fosse determinista. Sobre essa questão debruçou-se David Deutsch, procurando definir um dispositivo computacional que fosse capaz de simular eficientemente um sistema físico arbitrário. Deutsch não pertencia ao campo da computação. Segundo ele, sendo aluno de pós-graduação na área de cosmologia na Universidade de Texas, fora apresentado à interpretação dos muitos mundos por Wheeler e DeWitt, e dali começou seu interesse pelo formalismo e os problemas de interpretação da mecânica quântica que o levaram a trabalhar, uma vez doutorado, no campo da computação quântica (Yeang, 2011). A máquina universal proposta por Deutsch (1985a) mantém os mesmo elementos que a máquina universal “clássica” de Turing. A diferença reside em que os estados internos de sua máquina e os dados gravados são ambos estados quânticos que seguem os princípios da mecânica quântica, em particular, a superposição de estados e a não localidade, enfatizando que o poder computacional do computador quântico reside no “paralelismo quântico” (superposição de estados, emaranhamento e resultados probabilísticos das medições). Ou seja, dadas as propriedades da mecânica quântica – os estados de várias partículas podem ser expressos como combinações lineares de suas bases e o estado composto resultante como a soma de acoplamentos (produto tensorial entre vetores no espaço de Hilbert)

⁹ Segundo Yeang (2011, p. 331), embora Feynman não tenha citado os trabalhos relacionados com as desigualdades de Bell, o exemplo que coloca nesse artigo refere-se claramente a essa desigualdade.

entre esses termos nessas combinações lineares –, é possível um processamento da informação em paralelo, usando um computador quântico em série.

No entanto, a superposição de estados e o emaranhamento não são propriedades facilmente manipuláveis. Por uma parte, a coerência entre os estados pode desaparecer facilmente e, por outra, com o esquema que Deutsch propôs nesse artigo, não seria possível recuperar todos os valores ao mesmo tempo (e, portanto, aproveitar todo o potencial do “paralelismo”). É que nesse esquema a medição de um só deles faz que a função de onda colapse e seja destruída a informação contida nos outros estados (cf. Yeang, 2011).

Portanto, era necessário desenvolver esquemas mais complexos para poder lidar com essas questões. Depois da publicação do artigo, Deutsch continuou trabalhando sobre o tema, desenvolvendo algumas portas lógicas e tentando resolver problemas um pouco mais complicados, mas ainda sem aplicações práticas, como, por exemplo, o desenvolvido junto com Richard Jozsa (Deutsch & Jozsa, 1992), que permitia, de forma muitíssimo mais rápida que um computador clássico, determinar se uma função binária, que tomava valores inteiros entre 0 e $2^n - 1$, era constante para todos os valores do argumento (0 ou 1), ou era para a metade 0 e para outra 1.

Segundo Yeang (2011, p. 335), embora Deutsch tenha começado sua carreira na computação quântica trabalhando com questões em fundamentos da ciência (física de computação universal e a possibilidade de uma máquina universal usando os princípios da mecânica quântica), ele terminou descobrindo as aplicações potenciais desses exercícios.¹⁰ Então, de forma semelhante aos cientistas da computação do pós-guerra, transformou sua pesquisa nos fundamentos em uma busca de algoritmos que permitissem transformar as estranhas propriedades da mecânica quântica em recursos computacionais.

Esse primeiro passo notável, dado por Deutsch, foi sendo aprimorado na década seguinte por vários pesquisadores (quando começam a aparecer um número crescente de artigos diretamente relacionados com a computação quântica e o desenvolvimento de algoritmos apropriados), embora ainda tratando de problemas sem muito interesse prático. Esse processo culmina no artigo de Peter Shor (1994) no qual a eficiência de um computador quântico ficou demonstrada.¹¹ Shor é um matemático “prodígio”, sem qualquer formação anterior em mecânica quântica, mas interessado em problemas da

¹⁰ De fato, no mesmo ano (Deutsch, 1985b), ele publica um artigo argumentando que o formalismo da teoria quântica, tanto na interpretação de Copenhague como na de Everett, precisa de uma estrutura adicional.

¹¹ O artigo de Shor (1994), no qual esses algoritmos foram desenvolvidos, foi publicado em anais de uma conferência sobre computação e tem somente 68 citações. No entanto, Shor (1995), relacionado com a possibilidade da redução da descoerência na memória de um computador quântico e publicado em um periódico de física de alto impacto, tem 1313.

computação, com seus primeiros trabalhos focados em problemas estatísticos e geométricos da computação (cf. Yeang, 2011).¹² Ele demonstrou que dois problemas muito importantes – o problema de encontrar fatores primos a um número inteiro e o problema do “algoritmo” discreto – podiam ser resolvidos, de forma eficiente em um computador quântico. Isso “popularizou” a computação quântica (cf. Yeang, 2011), pois os dois problemas não tinham e não têm ainda uma solução eficiente em um computador clássico (cf. Nielsen & Chuang, 2010), mostrando que os computadores quânticos são mais eficientes para resolver esse tipo de problema que uma máquina de Turing clássica. Cabe salientar que o algoritmo de Shor de fatorização de números inteiros, se implementado em um computador quântico, acabaria com os sistemas de segurança utilizados hoje nos sistemas eletrônicos (chaves RSA), pois os mesmos têm sua segurança associada ao enorme tempo necessário para essa fatorização usando os atuais computadores. Em seguida, Lov Grover (1997), com uma formação semelhante à do Shor, e trabalhando no mesmo *Bell Laboratories*, mostrou que outro problema importante – o de realizar uma busca através de um espaço de busca não estruturado – podia ser resolvido de forma muito rápida em um computador quântico. Assim, esses pesquisadores abordaram problemas com uma enorme importância tanto para as matemáticas puras como aplicadas e transformaram a computação quântica, tal como inicialmente desenvolvida por Deutsch, de uma área que despertava certa curiosidade acadêmica em uma área de interesse internacional, aberta a matemáticos, cientistas da computação e engenheiros. De fato, quando se analisa o número de citações do trabalho de Deutsch, elas claramente dispararam a partir de 1995: das 1285 citações desse artigo que aparecem no ISI até 2012, somente 60 correspondem ao período entre a data de publicação e 1995.

A terceira fonte para o desenvolvimento do campo da informação e da computação quântica é o próprio campo da informação, embora com relações com o campo dos fundamentos da teoria quântica. De forma praticamente paralela à revolução que Turing tinha iniciado no campo da computação, Claude Shannon inicia outra, em 1948, na compreensão da comunicação, definindo de forma matemática e quantificando o conceito de informação.¹³ Shannon estava interessado em conhecer os recursos necessários para enviar informação em um canal de comunicação e a forma pela qual a informação poderia ser transmitida para estar protegida do ruído no canal de comunicação. Essas perguntas foram respondidas em dois teoremas (cf. Shannon & Weaver, 1949),

¹² A propósito, alguns físicos têm sugerido que o ensino da mecânica quântica para os matemáticos e cientistas da computação seja focalizado apenas no formalismo matemático, deixando de lado qualquer questão relacionada com a “compreensão” física desse formalismo (cf. Mermin, 2003).

¹³ Harry Nyquist, entre 1924 e 1928, desenvolveu alguns trabalhos teóricos sobre os requerimentos necessários da banda larga para transmitir informação, que serviram de base aos desenvolvimentos posteriores de Shannon.

conhecidos como o teorema da codificação da fonte e o teorema da codificação de canais-ruidosos, onde define que os códigos de correção de erros podem ser usados para proteger a informação enviada.

Na teoria da informação quântica, ocorreram desenvolvimentos semelhantes. Em 1995, Benjamin Schumacher, um físico teórico formado na Universidade de Texas, encontra a forma de interpretar os estados quânticos como informação,¹⁴ e estabelecer um análogo do teorema de Shannon da codificação da fonte, mas que usa, como mais apropriado para o caso quântico, o conceito de entropia de Von Neumann e não o de Shannon (cf. Schumacher, 1995). Em seu artigo, Schumacher define o “*quantum bit*” ou “*qubit*” como uma fonte física tangível. Embora não exista um equivalente ao teorema da codificação de canais-ruidosos, sobretudo pela impossibilidade da clonagem dos estados, tem sido desenvolvida uma teoria de correção de erros que permitiria aos computadores quânticos computar efetivamente em presença de ruído, assunto sobre o qual trabalha, entre outros, Peter Shor. Cabe assinalar aqui que há pelo menos três conceitos de entropia – e de medida da informação – em uso na área, a saber, o clássico de Shannon, o do von Neumann, utilizado, entre outros, por Fuchs, e aquele proposto por Brukner e Zeilinger, aos quais voltaremos adiante.

Ainda relacionado com a terceira vertente, é necessário destacar as contribuições e a figura de Charles Bennett. Ele é um químico que, junto com Rolf Landauer, ao incorporar-se, depois de doutorado, ao IBM Research Center, passou a dedicar-se à chamada física da computação (um ramo da física dedicado a resolver os problemas de implementações de processos reversíveis em máquinas de Turing que são irreversíveis). Em 1984, ele e Gilles Brassard publicam um artigo (Bennett & Brassard, 1984), no qual usam os estados emaranhados dos experimentos EPR na comunicação, especificamente na criptografia. Eles propõem um protocolo que usa a mecânica quântica para distribuir chaves de decodificação das mensagens entre dois usuários, sem nenhuma possibilidade de que alguém possa descobri-las. Ou seja, temos aqui uma informação “clássica” que é codificada em estados quânticos não ortogonais. Stephen Weisner, nos finais dos anos 1960, havia proposto um mecanismo semelhante ao de Bennett e Brassard. A inspiração de Weisner estava relacionada com a possibilidade de criar uma “moeda quântica” que não poderia ser falsificada, a partir das propriedades particulares do processo de medida na mecânica quântica. O trabalho de Weisner não somente não foi bem recebido pelos seus professores, como tampouco foi aceito para publicação (cf. Nielsen & Chuang, 2010, p. 10), um outro caso semelhante ao de Clauser (cf. Freire Jr., 2006) ou do Herbert (cf. Kaiser, 2011), quando a pesquisa em fundamentos não era bem vista entre os físicos norte-americanos (cf. Freire Jr., 2009). O trabalho de Weisner

¹⁴ Schumacher cita no artigo sua própria tese e a de Everett quando usa o conceito de entropia de von Neumann para o operador densidade, entendido como uma medida teórica da informação do nível de emaranhamento.

ficou circulando em fotocópias entre amigos, um deles Bennett, que tinha sido colega de Weisner na graduação (cf. Kaiser, 2011). Anos depois, Wheeler convidou Bennett a Austin, Texas, interessado pelo seu trabalho na teoria da informação clássica; é quando Bennett toma conhecimento do artigo de Wootters e Zurek sobre a não clonagem. Juntando esse teorema¹⁵ com a proposta de seu amigo, Bennett desenvolve o protocolo BB84. Em 1989, Bennett e Brassard constroem uma demonstração experimental desse protocolo (Bennett & Brassard, 1989).

Como faz notar Kaiser (2011, p. 225), o BB84 inverte uma impossibilidade – o teorema da não clonagem tem a ver com questões que a mecânica quântica proíbe – em uma ferramenta para códigos de segurança em comunicações clássicas. Assim como no caso da proposta de Deutsch, ou os algoritmos de Shor e Grover, o BB84 exemplifica o que será o movimento característico dentro do campo da computação e da informação quântica – transformar as estranhas propriedades da mecânica quântica em aplicações promissoras.

A partir de então, Bennett se dedicou a estudar esse problema, ou seja, como transmitir informação clássica usando um canal quântico. Nessas pesquisas, ele e sua equipe descobriram formas de manipular estados quânticos EPR para implementar sistemas de transmissão de informação. O primeiro resultado importante dessa linha foi a “codificação superdensa”, de Bennett e Stephen Weisner (1992), ou seja, como transmitir dois *bits* de informação em um só *qubit*. Para isso, desenharam um esquema em que se usava o “feedback EPR” – abrir um par EPR, manipular um dos *qubits* do par e devolver, de alguma forma, o resultado da manipulação ao outro lado. O feedback EPR abriria o caminho para novos efeitos, como a teleportação quântica, um tema sobre o qual começou a trabalhar-se com uma equipe interdisciplinar (cf. Bennett *et al.*, 1993; Yeang, 2011).

Esses trabalhos iniciais nas três áreas apresentadas deram origem, a partir de meados da década de 1990, a uma das áreas atualmente mais importantes de pesquisa, sendo identificada, na maioria dos países, como uma das subáreas de pesquisa básica prioritárias. Do mesmo modo como aconteceu com o desenvolvimento dos transistores, a pesquisa está sendo também patrocinada por empresas privadas. O desafio intelectual e a possibilidade de financiamento tem atraído muitos pesquisadores de diferentes áreas – física, matemática, ciências da computação, engenharia – de todo mundo a trabalhar nesse tema, embora os resultados, em termos de viabilização de um computador quântico sejam ainda modestos e existam dúvidas quanto ao seu potencial tecnológico efetivo (cf. Paraoanu, 2011). Em particular, as questões da criptografia quântica por suas aplicações administrativas e militares têm recebido amplo financia-

¹⁵ Bennett e Brassard citam o artigo de não clonagem de Wootters & Zurek (1979) como principal fonte de motivação para seu trabalho.

mento das agências governamentais em todo o mundo, e as maiores corporações eletrônicas mantêm divisões sobre esse assunto, levando os fundamentos da mecânica quântica, a partir do BB84 e do teorema da não clonagem, às páginas dos periódicos de negócios mais importantes do mundo (cf. Kaiser, 2011).

3 A MESCLA ENTRE FUNDAMENTOS E INFORMAÇÃO: O CASO DE OVIEDO

A mescla entre os três campos anteriormente apontados pode ser ilustrada na evolução das conferências realizadas na Universidade de Oviedo, Espanha, em 1993, 1996 e 2002. Na sua origem e motivações, era um empreendimento típico dos físicos que temos denominado de dissidentes quânticos (cf. Freire, 2009): críticos da interpretação de Copenhague e defensores de uma valorização profissional da pesquisa em fundamentos da teoria quântica. Esse era exatamente o perfil do seu animador, o físico e professor daquela universidade Miguel Ferrero, que se tinha doutorado em 1986, sob a orientação de Emilio Santos, com uma tese em fundamentos, uma temática mal vista entre os físicos da época conforme os alertas de Santos e as lembranças de Ferrero. Santos é um químico que se tem notabilizado, junto com o físico britânico Trevor Marshall, pela defesa da eletrodinâmica estocástica; abordagem que supõe a existência de propriedades estatísticas no campo eletromagnético clássico, as quais reproduzem propriedades do campo de ponto zero da eletrodinâmica quântica. Esse caminho permite, então, a rivalidade entre essa abordagem e a teoria quântica. Em seu trabalho doutoral (Ferrero & Santos, 1985), Ferrero desenvolveu um trabalho anterior, elaborado pelo seu orientador (Marshall, Santos & Selleri, 1983); ambos os trabalhos simulam, a partir dos princípios da eletrodinâmica estatística, os resultados obtidos pelas experiências de Alain Aspect de 1982 e permitem, assim, aos autores a recusa do conflito entre a teoria quântica e o realismo local, com a preservação deste último. Franco Selleri, o mais notável dissidente quântico entre os três autores, inspirou Ferrero no empreendimento das conferências de Oviedo. Ferrero queria dar continuidade às conferências que Selleri havia organizado na década de 1980 na Itália, em particular em Bari onde trabalhava. Ferrero queria também manter o espírito das conferências aberto a todos os cientistas que trabalhavam em fundamentos da teoria quântica, e não apenas aos críticos da interpretação usual e defensores de uma interpretação particular. Ademais, Ferrero visava divulgar o tema dos fundamentos da teoria quântica na Espanha e colocar a Universidade de Oviedo na mapa da física mundial,¹⁶ o que conseguiu com

¹⁶ Na redação desta seção nós nos apoiamos em documentos publicados dessas conferências (Ferrero, 2003a) e em uma entrevista com seu organizador, Miguel Ferrero, realizada por I. Greca em Oviedo, fevereiro de 2012. Sobre Selleri, cf. Freire Júnior, 2009.

os físicos de primeiro nível que assistiram às mesmas, relacionados com os fundamentos da mecânica quântica nas duas primeiras conferências e da informação e computação quântica na última.

A primeira conferência de Oviedo, em 1993 (cf. Ferrero & van der Merwe, 1995) foi, então, uma típica conferência sobre os fundamentos da teoria quântica, com muitos trabalhos dedicados a interpretações alternativas e a modelos visando a preservação do realismo local. Ferrero começa então a formar uma opinião de que havia muita gente movendo-se para adiante, usando a teoria quântica em novos contextos teóricos e experimentais, e que ele e seus colegas estavam fazendo apenas uma crítica destrutiva. Ele estava particularmente impressionado pelos resultados ligados à teletransportação, codificação superdensa, e outros aspectos do que começava a denominar-se “informação quântica”. A segunda conferência, realizada em 1996 (cf. Ferrero & van der Merwe, 1997), começou a refletir essa tendência com um maior número de trabalhos sobre aspectos experimentais e de aplicação da teoria quântica. Conforme Ferrero,

a sabedoria recebida hoje parece ser que é muito mais produtivo (e excitante) usar [as correlações quânticas] como um novo recurso para fazer coisas que são classicamente impossíveis, do que rejeitar ou negar as correlações apenas porque temos dificuldades para entendê-las. Isso é o que está acontecendo agora na teoria da informação quântica (Ferrero, 2003b, p. 669).

Para a conferência seguinte, Ferrero compreendeu que seria preciso uma ênfase maior ainda no florescente campo de informação quântica. Compreendeu também que o aprofundamento das mudanças na configuração desses eventos não seria feito sem custos. Esse foi o caso de um dos animadores das conferências, Trevor Marshall. Ferrero formou a opinião de que ele precisava prescindir de Marshall no congresso seguinte, porque ele trazia mais problemas que ajuda, em particular, por sua oposição aos experimentos e seus resultados sobre teletransportação, oposição fundada em razões filosóficas e programáticas, pois, na abordagem da eletrodinâmica estocástica, a radiação de ponto zero impediria a teletransportação.¹⁷ A conferência de 2002 adotou em sua denominação a ênfase na informação quântica – “Conferência Internacional sobre Informação Quântica. Fundamentos conceituais, desenvolvimentos e perspectivas” – e foi realizada com grande êxito, contando com a participação de quatro dos oito grupos experimentais mais importantes nesse campo. A conferência caracterizou-se pela apresentação de propostas teóricas e resultados experimentais sobre a aplicação das propriedades da mecânica quântica à informação e computação, com um único trabalho

¹⁷ Sobre as propostas teóricas e as realizações experimentais com teletransportação, cf. Bennett *et al.*, 1993; Bouwmeester *et al.*, 1997.

que tratava do tema das interpretações. Fruto das mudanças ocorridas, e do público de jovens pesquisadores que dela participou, os organizadores optaram por submeter os trabalhos apresentados para publicação, após arbitragem, em número especial de uma revista prestigiada, *Journal of Modern Optics* (Ferrero, 2003a), no lugar de publicação em livros como nas conferências anteriores. Estava finda a transição nas conferências de Oviedo, tanto intelectual quanto profissional, do campo de fundamentos da teoria quântica para o novo campo de informação quântica.

A força do campo de pesquisa da informação quântica encontra-se no desenvolvimento do uso de propriedades estritamente quânticas em problemas de informação e de computação. Contudo, esse campo abriga, também, preocupações com os fundamentos da ciência. Ferrero, para ficarmos em Oviedo, é um exemplo de um cientista dedicado à pesquisa dos fundamentos da informação quântica, os quais têm relação estreita, em última instância, com os problemas de interpretação e de fundamentos da teoria quântica. Ele se dedica, ao longo da última década, ao estudo do que denomina de “interpretação da informação” como um desenvolvimento da interpretação de Copenhague (cf. Ferrero, 2003b; Ferrero, Salgado & Sánchez-Gómez, 2004). Para as questões que nos interessam nas seções restantes deste trabalho, colocamos para Ferrero a questão de saber qual é o conceito de “informação” presente nas pesquisas em informação quântica. Ele considera não poder responder por tratar-se exatamente de questão no centro de seu projeto de investigação. Atento às implicações epistemológicas da questão, ele sustenta não ter claro qual é o papel que a informação pode desempenhar na construção da realidade e assinala que esse problema está relacionado ao velho problema nos fundamentos da teoria quântica: qual o significado da função de onda (Ψ) que descreve o estado na teoria quântica? Ôntico ou epistêmico? Ele não avança formulações definitivas, mas diz que hoje está inclinado a pensar que seria uma mescla das duas possibilidades.

4 A DIVERSIDADE DO CONCEITO DE INFORMAÇÃO NA INFORMAÇÃO QUÂNTICA

O crescimento da pesquisa teórica e experimental no campo da informação quântica trouxe um efeito colateral surpreendente, pelo menos para aqueles que pensavam que as possibilidades tecnológicas entrevistas sufocariam o debate sobre os fundamentos. Ao lado da aplicação dos fenômenos estritamente quânticos para o desenvolvimento do campo, alguns de seus protagonistas reanimaram o debate sobre as interpretações da teoria quântica, em particular, sobre o significado físico, se há algum, dos vetores de estado. A afirmativa mais provocativa nesse sentido – “a teoria quântica dispensa ‘interpretações’” – foi feita pelos físicos Christopher Fuchs e Asher Peres, na influen-

te revista *Physics Today* (2000a, 2000b). Os autores argumentaram contra as interpretações que buscam atribuir alguma realidade física ao vetor de estado independente de nossos experimentos, como variáveis escondidas, muitos mundos, histórias consistentes, e colapso espontâneo, argumentando que elas não aprimoram o poder preditivo da teoria quântica e são responsáveis pelos conhecidos paradoxos que assolam essa teoria, a exemplo do colapso do vetor de estado durante os processos de medição. A tese básica dos autores é que os vetores de estado têm como objeto apenas informação sobre os sistemas quânticos, e não os sistemas quânticos em si mesmos. Conforme Fuchs e Peres,

contrariamente àqueles desejos, a teoria quântica *não* descreve a realidade física. O que ela faz é prover um algoritmo para calcular *probabilidades* para os eventos macroscópicos (“cliques de detectores”) que são as consequências de nossas intervenções experimentais. Esta definição estrita do escopo da teoria quântica é a única interpretação necessária, seja por cientistas teóricos ou experimentais. As probabilidades quânticas, como todas probabilidades, são calculadas usando a informação disponível (2000, p. 70).

À primeira vista, tal proposição pareceria uma mera reafirmação do que tem se convencionalmente denominado de “interpretação instrumentalista mínima”, a qual, conforme Redhead (1987), reúne o algoritmo da quantização e o algoritmo estatístico, além da premissa, positivista em termos epistemológicos, de que as teorias na física são apenas dispositivos para expressar regularidades entre as observações. Logo, seria uma reedição de uma interpretação com trânsito entre os cientistas, mas criticável em uma perspectiva filosófica realista. Essa explicação redutora, contudo, enfrenta duas objeções. A primeira é que Fuchs e Peres explicitamente rejeitam a inspiração positivista. “Nós não fomos levados a rejeitar uma realidade autônoma no mundo quântico devido a uma predileção pelo positivismo. Chegamos a essa posição por causa da mensagem massiva que a teoria quântica está tentando enviar-nos” (Fuchs & Peres, 2000, p. 90). A segunda é que boa parte da “mensagem” referida por esses cientistas diz respeito ao conjunto de fenômenos quânticos recentemente identificados, a exemplo do emaranhamento e da teleportação. Logo, a renovação do debate sobre a interpretação da teoria quântica certamente deve portar sobre aspectos epistemológicos, os quais envolvem a natureza das leis físicas, da objetividade, da experimentação e do realismo, mas precisam levar em conta a ampla gama de fenômenos hoje em exploração no campo da informação quântica.

Christopher Fuchs tem se dedicado ao estudo da teoria quântica da comunicação – foi aluno de Wheeler na Universidade do Texas e colaborou com Jozsa, Bennett, e

Schumacher, além de Asher Peres, na proposição da teleportação (cf. Bennett *et al.*, 1993). Ele continua a desenvolver a abordagem à teoria quântica que havia propugnado com Peres. Como vimos, eles têm em comum a premissa de que não seria fecunda a busca de limites à validade da mecânica quântica. Propõem também acabar com as discussões de interpretações sobre a realidade dos estados quânticos, e avançar sobre as coisas novas e produtivas que podem ser feitas, explorando as propriedades da mecânica quântica. Para Fuchs, um sistema quântico é alguma coisa real, independente de nós, mas o estado quântico é uma coleção de graus subjetivos de crenças sobre alguma coisa que se pode fazer com o sistema. Ou seja, é uma informação subjetiva e, portanto, não é nem pode ser uma descrição completa do sistema quântico. Os estados quânticos são, então, estados de informação, de conhecimento ou de crenças, mas não estados da natureza. Com base nessa ideia geral, Fuchs (2003) considera que adotando a teoria de probabilidades de Bayes, cujo objetivo é desenvolver métodos fiáveis de raciocínio e de tomada de decisões quando existe informação incompleta, podem ser evitadas algumas questões problemáticas da mecânica quântica, como o colapso da função de onda. Assim, o processo de medida pode ser descrito como a passagem de um estado inicial para um estado final, o que envolve o refinamento e reajuste das nossas crenças iniciais, a partir do resultado obtido no processo de medida. Todo processo de medida seria simplesmente a aplicação da regra de Bayes – um refinamento arbitrário de nossas crenças – juntamente com alguma consideração de que as medições são intervenções sobre a natureza.

Caslav Brukner e Anton Zeilinger (2001, 2005) são outros físicos que propõem tomar a informação como o conceito básico da mecânica quântica, uma ideia que já havia sido formulada antes por Carl F. von Weizsäcker em 1958 (cf. *apud* Brukner & Zeilinger, 2005, p. 47) e Wheeler. Assim, a teoria quântica passa a ser primariamente uma ciência sobre o conhecimento que temos da realidade, não sobre a realidade. Para eles,

a física quântica versa sobre informação; assim, devemos perguntar-nos que significado nós queremos atribuir a um sistema quântico. É então imperativo evitar atribuir qualquer variante de objetividade clássica ingênua aos estados quânticos. Ainda mais, é então natural assumir que o sistema quântico é apenas a noção à qual as probabilidades se referem, e nada mais. A noção de uma realidade existindo objetivamente torna-se assim vazia (Brukner & Zeilinger, 2005, p. 56).

Para medir essa informação, Brukner e Zeilinger não usam a medida de Shannon, pois consideram que ela só é válida para observáveis comutáveis. O menor sistema possível é aquele que representa um *bit* de informação; portanto, somente pode represen-

tar sim/não como resposta a uma pergunta. Se ao sistema é feita uma outra pergunta, a resposta necessariamente deve ser aleatória. Portanto, a aleatoriedade é uma característica fundamental de nosso mundo, o que, para eles, é a base para a explicação da complementaridade.

A proposta de Brukner e Zeilinger tem, entretanto, sido recebida com críticas (cf. Timpson, 2003). Mais importante ainda, um teorema recentemente formulado por Matthew Pusey, Jonathan Barrett e Terry Rudolph sugere que a tese dos estados como representações apenas de informação sobre a probabilidade de futuras medições pode estar em conflito com a própria teoria quântica. Conforme esses autores, em teorema já denominado de teorema PBR, “nós mostramos que qualquer modelo no qual o estado quântico represente mera informação sobre um estado físico subjacente ao sistema, (...) deve fazer previsões que contrariam aquelas da teoria quântica” (Pusey; Barrett, & Rudolph, 2012, p. 476). O teorema gerou um debate acirrado antes mesmo de sua publicação (cf. Aaronson, 2012) e é uma indicação tanto da possibilidade de levar tais questões de fundamentos e interpretações para as bancadas de laboratório, como foi feito antes com o teorema de Bell, como uma indicação de que a palavra final sobre o significado dos vetores de estado da teoria quântica ainda está por ser proferida.

As ideias de Brukner e Zeilinger, contudo, parecem menos radicais que as ideias de John Archibald Wheeler, famoso por jogar com as palavras para expressar conceitos científicos relevantes. Em 1990, antes mesmo da configuração do campo da informação quântica, ele havia criado o “*It from bit*”: “cada *it* – cada partícula, cada campo de força, incluindo o contínuo espaço tempo, deriva sua função, seu significado, sua existência, ainda se em alguns contextos indiretamente, das respostas de aparatos a perguntas sim ou não, escolhas binárias, *bits*” (Wheeler, 1990, p. 310). Para Wheeler o que chamamos realidade aparece, em última análise, quando colocamos perguntas sim/não e as respostas são registradas no equipamento que usamos para fazê-las, ou seja, todas as coisas físicas são teórico-informáticas na origem.¹⁸ Ideias semelhantes têm coalescido na tese da representação do universo como um processador, ou mais precisamente, como um computador quântico. Um dos defensores da tese é Seth Lloyd, professor de Engenharia Mecânica do MIT e construtor do primeiro computador quântico. A tese pode ser considerada uma metáfora, típica dos tempos da centralidade da informação (cf. Gleick, 2011) e sucessora da metáfora do universo como um grande relógio que foi própria do período de emergência do mecanicismo no século XVII. Para Lloyd (2006), contudo, ela é mais do que uma metáfora. Seu argumento está baseado nos trabalhos de Edward Fredkin e Tommaso Toffoli que, no início da década de 1980, mostraram que um modelo mecânico de um gás poderia reproduzir as operações lógi-

¹⁸ A contribuição de Wheeler para o estabelecimento das relações entre informação e teoria quântica foi muito significativa, o que está a merecer estudo histórico e epistemológico.

cas básicas da computação e nos desenvolvimentos da informação quântica que mostram que um computador quântico pode simular sistemas regidos pela teoria quântica. Para Lloyd, “uma simulação do universo em um computador quântico é indistinguível do próprio universo” (2006, p. 154).

Uma das consequências da abordagem à teoria quântica centrada no conceito de informação – colocada como pergunta aberta por Brukner e Zeilinger e como consequência natural por Wheeler – é o abandono do conceito de “contínuo”, que somente pode ser concebido como uma idealização, não havendo nenhuma prova de que seja uma categoria universal da natureza. Cabe salientar que uma ideia semelhante é mantida por físicos que trabalham na área de simulações dos autômatos celulares na interface entre a biologia e a física, sem conexões com a teoria quântica, mas sim com os computadores, com a sugestão de que o mundo físico é uma rede espaço-temporal discreta de *bits* de informação (cf. Vichniac *apud* Keller, 2003).

CONCLUSÕES

A pesquisa em informação quântica vicejou de uma confluência entre fundamentos da teoria quântica e as ciências da informação e, em alguns casos, de uma mescla dessas duas áreas. Colocando em perspectiva os últimos 25 anos da relação entre a teoria quântica e a informação, parece-nos que dois movimentos históricos distintos podem ser identificados. Em um primeiro momento, o campo da informação quântica adquiriu impulso pelas mãos dos que buscaram a aplicação dos novos fenômenos quânticos ao campo da informação, sem a ênfase anterior na crítica aos fundamentos da teoria quântica, embora esses novos efeitos tenham emergido do reaquecimento da discussão sobre os fundamentos ocorrida nos 15 anos precedentes. Nesse sentido, pode dizer-se que os dissidentes quânticos (cf. Freire, 2009) foram substituídos pelos engenheiros quânticos (cf. Yeang, 2011). Outra metáfora, que poderia ser usada, seria dizer que o campo da informação quântica emerge do transformar os “sapos conceituais” da teoria quântica (seus conceitos que não conseguimos engolir dentro de uma postura realista) em “príncipes promissores”. Essa metáfora com os contos de fadas, pode ser estendida para afirmarmos que, como no conto de fadas, não sabemos se o final será o prometido. Em um segundo momento, a engenharia quântica, como assinalado por Yeang, trouxe consigo novos problemas conceituais, mas também atualizou o velho problema da interpretação do objeto da teoria quântica. Temos assim uma espécie de movimento em espiral entre os fundamentos e as aplicações, quiçá semelhante ao acontecido quando ocorreu o estabelecimento da teoria quântica e diferente da época em que o debate sobre os fundamentos foi afastado da física.

Escapa ao escopo deste trabalho uma revisão exaustiva da farta literatura que estabelece as relações entre o conceito de “informação” e o objeto da teoria quântica. Do mesmo modo, não caberia aqui revisar as críticas a essas posições. Para os nossos objetivos, é suficiente notarmos que a emergência do campo da informação quântica trouxe consigo a proposição de colocar a informação como o objeto da própria teoria quântica e que dentre os defensores dessas ideias existem controvérsias sobre qual o conceito de informação mais adequado a esse objetivo. Devemos notar, portanto, que estamos na fronteira mesma do conhecimento, com o conceito de “informação” emergindo com centralidade em uma área avançada da ciência, mas convivendo com distintas formulações.

Outro aspecto, mais epistemológico, a considerar é que a ciência moderna foi constituída tendo como objeto a materialidade dos fenômenos da natureza, ainda que estes, para serem tomados como objeto de pensamento, sejam tomados como objetos conceituais. Agora, o desenvolvimento da física quântica parece sugerir, pelo menos para os autores que consideramos, a necessidade de incluirmos a informação sobre um sistema como o objeto da própria teoria científica. Ou seja, uma teoria científica cujo objeto não é um objeto real no sentido usual até agora. Ao adotar uma centralidade para o conceito de informação, contudo, a física não se encontra isolada. Os desenvolvimentos da genética em fins do século xx levaram à colocação de problemas análogos. Ademais, tanto a própria constituição, ao longo do século xx, de uma ciência da informação, quanto a onipresença das tecnologias da informação nas sociedades contemporâneas parecem apontar, ao lado desses aspectos da física e da biologia, para uma centralidade do conceito de “informação” na ciência contemporânea, tendência que o escrito James Gleick (2011) denominou de “virada informacional” (*information turn*).⁹

Olival FREIRE JUNIOR

Professor Doutor do Instituto de Física,

Universidade Federal da Bahia.

Pesquisador do Conselho Nacional de Pesquisas

Científicas e Tecnológicas, Brasil.

freirejr@ufba.br

Ileana Maria GRECA

Professora Departamento de Didáticas Específicas,

Facultad de Humanidades y Educación,

Universidad de Burgos, Espanha.

ilegreca@hotmail.com

ABSTRACT

Research in quantum information suggests a close connection between information and quantum theory. The aim of this article is to analyze nuances involved in this connection. Scientists in this field are divided into two overlapping camps. Some are motivated only by the use of quantum features to improve information processing, in spite of concerns about the foundations of the quantum theory, while others recognize deep conceptual problems of this theory, and attempt to solve them. This article has modest ambitions. It aims only to chart, by way of historical and conceptual analysis, the diverse possibilities available, indicating the strengths and weaknesses of each of them.

KEYWORDS • Quantum theory. Quantum information. Information. Entropy. Oviedo's conferences. Entanglement. Teleportation.

REFERÊNCIAS BIBLIOGRÁFICAS

- AARONSON, S. Get real. *Nature Physics*, 8, p. 443-4, 2012.
- BENIOFF, P. Quantum mechanical hamiltonian models of discrete processes that erase their own histories: application to Turing machines. *International Journal of Theoretical Physics*, 21, p. 177-201, 1982.
- BENNETT, C. & BRASSARD, G. Quantum cryptography: public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computer Systems and Signal Processing*. New York: IEEE, 1984. p. 175-9.
- _____. The dawn of a new era in quantum cryptography: the experimental prototype is working. *ACM SIGACT News*, 20, p. 78-83, 1989.
- BENNETT, C. et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70, 13, p. 1895-9, 1993.
- BENNETT, C. & WEISNER, S. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69, 16, p. 2881-4, 1992.
- BOHR, N. Natural philosophy and human cultures. In: *The philosophical writings of Niels Bohr. Essays 1932-1957 on atomic physics and human knowledge*. Woodbridge: Ox Bow, 1987 [1938]. v. 2, p. 23-31.
- BOUWMEESTER, D. et al. Experimental quantum teleportation. *Nature*, 390, p. 575-9, 1997.
- BROMBERG, J. L. Device physics vis-à-vis fundamental physics in Cold War America: the case of quantum optics. *Isis*, 97, 2, p. 237-59, 2006.
- BRUKNER, C. & ZEILINGER, A. Conceptual inadequacy of the Shannon information in quantum measurements. *Physical Review*, A, 63, p. 022113, 2001.
- _____. & _____. Quantum physics as a science of information. In: ELITZUR, A.; DOLEV, S & KOLENDA, N. (Ed.). *Quo vadis quantum mechanics?* New York: Springer, 2005. p. 47-61.
- DEUTSCH, D. Quantum theory, the church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A*, 400, p. 97-107, 1985a.
- _____. Quantum-theory as a universal physical theory. *International Journal of Theoretical Physics*, 24, 1, p. 1-41, 1985b.
- DEUTSCH, D. & JOZSA, R. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A*, 439, p. 553-8, 1992.

- DEWITT, B. & GRAHAM, N. (Ed.). *The many-worlds interpretation of quantum mechanics*. Princeton: Princeton University of Press, 1973.
- DIEKS, D. Communication by EPR devices. *Physics Letters A*, 92, 6, p. 271–2, 1982.
- EINSTEIN, A. Reply to criticisms. In: SCHILPP, P. A. (Ed.). *Albert Einstein – philosopher-scientist*. La Salle (Illinois): Open Court, 1982. p. 663–8.
- ELITZUR, A.; DOLEV, S & KOLENDA, N. (Ed.). *Quo Vadis quantum mechanics?* New York: Springer, 2005.
- EVERETT III, H. The theory of the universal wave function. In: DEWITT, B. & GRAHAM, N. (Ed.). *The many-worlds interpretation of quantum mechanics*. Princeton: Princeton University of Press, 1973.
- FERRERO, M. Special issue: International conference on quantum information. Conceptual foundations, developments and perspectives, 13–18 July 2002, *Journal of Modern Optics*, 50, 6–7, p. 867–71, 2003a.
- _____. The information interpretation and the conceptual problems in quantum mechanics. *Foundations of Physics*, 33, 4, p. 665–76, 2003b.
- FERRERO, M.; SALGADO, D. & SÁNCHEZ-GÓMEZ, J. L. Is the epistemic view of quantum mechanics incomplete? *Foundations of Physics*, 34, 12, p. 1993–2003, 2004.
- FERRERO, M. & SANTOS, E. Local realistic photon model compatible with Malus’ law for experiments testing Bell’s inequalities. *Physics Letters A*, 108, 8, p. 373–6, 1985.
- FERRERO, M. & VAN DER MERWE, A. *Fundamental problems in quantum physics*. Dordrecht: Kluwer Academic Publishers, 1995.
- _____. *New developments on fundamental problems in quantum physics*. Dordrecht: Kluwer Academic Publishers, 1997.
- FEYNMAN, R. P. Simulating physics with computers. *International Journal of Theoretical Physics*, 21, p. 467–88, 1982.
- FREIRE JR., O. *David Bohm e a controvérsia dos quanta*. Campinas: Centro de Lógica e Epistemologia da Ciência – Unicamp, 1999.
- _____. Philosophy enters the optics laboratory: Bell’s theorem and its first experimental tests (1965–1982). *Studies in History and Philosophy of Modern Physics*, 37, p. 577–616, 2006.
- _____. Quantum dissidents: research on the foundations of quantum theory circa 1970. *Studies in History and Philosophy of Modern Physics*, 40, p. 280–9, 2009.
- FUCHS, C. A. Quantum mechanics as quantum information, mostly. *Journal of Modern Optics*, 50, 6–7, p. 987–1023, 2003.
- FUCHS, C. A. & PERES, A. Quantum theory needs no “interpretation”. *Physics Today*, 53, 3, p. 70–1, 2000a.
- _____. Quantum theory needs no “interpretation”. Letters. *Physics Today*, 53, 9, p. 11–90, 2000b.
- GLEICK, J. *The information. A history. A theory. A flood*. New York: Pantheon, 2011.
- GROVER, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79, 2, p. 325–8, 1997.
- HERBERT, N. FLASH- a superluminal communicator based upon a new kind of quantum measurement. *Foundations of Physics*, 12, p. 1171–9, 1982.
- JAMMER, M. *The philosophy of quantum mechanics. The interpretations of quantum mechanics in historical perspective*. New York: Wiley, 1974.
- KAISER, D. *How the hippies saved physics*. New York: W. W. Norton & Company, 2011.
- KELLER, E. F. Models, simulations and “computer experiments”. In: RADDER, H. (Ed.). *The philosophy of scientific experimentation*. Pittsburg: Pittsburgh University Press, 2003. p. 198–215.
- LLOYD, S. *Programming the universe – a quantum computer scientist takes on the cosmos*. New York: Knopf, 2006.
- MARSHALL, T ; SANTOS, E. & SELLERI, F. Local realism has not been refuted by atomic cascade experiments. *Physics Letters*, 98A, 1–2, p. 5–9, 1983.

- MERMIN, N. D. From Cbits to Qbits: teaching computer scientists quantum mechanics. *American Journal of Physics*, 71, p. 23, 2003.
- NIELSEN, M. A. & CHUANG, I. L. *Quantum computation and quantum information*. New York: Cambridge University Press, 2010.
- OSNAGHI, S.; FREITAS, F. & FREIRE JR., O. The origin of the everettian heresy. *Studies in History and Philosophy of Modern Physics*, 40, p. 97-123, 2009.
- PARAGANU, G. S. Quantum computing: theoretical versus practical possibility. *Physics in Perspective*, 13, p. 359-72, 2011.
- PRESKILL, Notes of the course "quantum computation", 2004. Disponível em: <<http://www.theory.caltech.edu/~preskill/ph229>>. Acesso em: 15 out. 2012.
- PUSEY, M. F.; BARRETT, J. & RUDOLPH, T. On the reality of the quantum state. *Nature Physics*, 8, p. 476-9, 2012.
- RADDER, H. (Ed.). *The philosophy of scientific experimentation*. Pittsburg: Pittsburgh University Press, 2003.
- REDHEAD, M. *Incompleteness, nonlocality, and realism: a prolegomenon to the philosophy of quantum mechanics*. Oxford: Oxford University Press, 1987.
- SCHILPP, P. A. (Ed.). *Albert Einstein – philosopher-scientist*. La Salle (Illinois): Open Court, 1982.
- SCHUMACHER, B. Quantum coding. *Physical Review A*, 51, p. 2738-47, 1995.
- SHANNON, C. E. & WEAVER, W. *The mathematical theory of communication*. Urbana: University of Illinois Press, 1949.
- SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In: Goldwasser, S. (Ed.). *Proceedings of the 35th annual symposium on foundations of computer science*. Santa Fé: IEEE Computer Society Press, 1994. p. 124-34.
- _____. Scheme for reducing decoherence in quantum computer memory. *Physics Review A*, 52, p. R2493-6, 1995.
- _____. Fault-tolerant quantum computation. In: *Proceedings, 37th annual symposium on fundamentals of computer science*. Los Alamitos: IEEE Press, 1996. p. 56-65.
- STEANE, A. M. Multiple particle interference and quantum error correction. *Proc. R. Soc. London A*, 452, p. 2551-76, 1996.
- TIMPSON, C. G. On a supposed conceptual inadequacy of the Shannon information in quantum mechanics. *Studies in History and Philosophy of Modern Physics*, 34, p. 441-68, 2003.
- TURING, A. M. On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc.* 2, p. 42-23, 1936.
- Weeler, J. A. Information, physics, quantum: the search for links. In: Zurek, W. (Ed.). *Complexity, entropy, and the physics of information*. Redwood City: Addison-Wesley, p. 309-36.
- WIGNER, E. P & YANASE, M. M. Information contents of distributions, *Proceedings of the National Academy of Sciences of the United States of America*, 49, 6, p. 910-8, 1963.
- WOOTTERS, W. K. & ZUREK, W. H. Complementarity in the double-slit experiment: quantum non separability and a quantitative statement of Bohr's principle. *Physical Review D*, 19, 2, p. 473-84, 1979.
- _____. A single quantum cannot be cloned. *Nature*, 299, p. 802-3, 1982.
- YEANG, C. P. Engineering entanglement, conceptualizing quantum information. *Annals of Science*, 68, 3, p. 325-50, 2011.

