

Tadeusz PABJAN  
Centrum Kopernika Badań Interdyscyplinarnych

## ***DRUGA REWOLUCJA KWANTOWA: DZIEDZICTWO JOHNA S. BELLA***

Mechanika kwantowa jest z wielu powodów wyjątkowo wdzięcznym przedmiotem analiz dla filozofii nauki. Jako jedna z najbardziej zaawansowanych matematycznie i najlepiej potwierdzonych empirycznie teorii fizycznych stanowi ona swego rodzaju metodologiczny wzorzec dla wszystkich innych teorii współczesnej nauki, a jednocześnie — jest źródłem bardzo wielu interpretacyjnych kontrowersji, które kładą się cieniem na wszystkich jej pozostałych zaletach. Interesującym — zwłaszcza z metodologicznego punktu widzenia — fenomenem jest to, że matematyczne i technologiczne zaawansowanie mechaniki kwantowej nie idzie w parze z zaawansowaniem konceptualnym: wiele zagadnień o charakterze pojęciowym, które mają fundamentalne znaczenie dla interpretacji formalizmu tej teorii ciągle jeszcze oczekuje na satysfakcjonujące wyjaśnienie. Równie interesujące — nie tylko dla metodologii, ale również dla socjologii i psychologii nauki — są mechanizmy, które odpowiadają za to, że znaczna część fizyków, zajmujących się mechaniką kwantową, w całkowicie bezkrytyczny sposób przyjmuje pogląd szkoły kopenhaskiej, zgodnie z którym wszystkie istotne dla tej teorii problemy o charakterze pojęciowym zostały dawno temu w sposób zadowalający rozwiązane przez jej ojców-założycieli.

Fizykiem, który zwrócił uwagę świata naukowego na bezpodstawność tego ostatniego poglądu, był autor jednego z najważniejszych twierdzeń, dotyczących interpretacji formalizmu mechaniki kwanto-

wej, John S. Bell.<sup>1</sup> Lektura jego artykułów, dotyczących konceptualnych podstaw tej teorii<sup>2</sup>, pozwala nabrać przekonania, że ulubionym zajęciem tego uczonego było kontestowanie stanowiska szkoły kopenhaskiej, i formułowanie (wyjątkowo trafnych!) argumentów za tym, że standardowe sformułowanie mechaniki kwantowej zawiera szereg „fundamentalnych nieścisłości”<sup>3</sup>, które w tak poważnej i zaawansowanej teorii fizycznej, jaką jest mechanika kwantowa, najzwyczajniej w świecie nie mają prawa się pojawiać. Co prawda, Bell nie znalazł jednej prostej odpowiedzi na pytania, dotyczące tego typu interpretacyjnych nieścisłości — chociaż wskazał na kilka rozwiązań, które mogłyby takich odpowiedzi dostarczyć<sup>4</sup> — ale jego analizy okazały się niezwykle skutecznym katalizatorem postępu technologicznego, otwierającego przed mechaniką kwantową zupełnie nowe, nieznanie wcześniej, perspektywy rozwoju. Jeśli pamięta się o tym, że stanowisko szkoły kopenhaskiej przez długie dziesięciolecia traktowane było przez naukowe elity jako „jedynie słuszna” interpretacja mechaniki kwantowej, to trudno nie zgodzić się z przewrotnym wnioskiem, który formułuje Alain Aspect w odniesieniu do wyników, uzyskanych przez Bella: kwestionowanie naukowych dogmatów w pewnych przypadkach może okazać się bardzo owocne.<sup>5</sup>

---

<sup>1</sup>John S. Bell (1928-1990) był irlandzkim fizykiem teoretykiem — „kwantowym inżynierem”, jak zwykł o sobie mawiać. Studia z zakresu fizyki eksperymentalnej (*Queen's University of Belfast*) ukończył w roku 1948. Specjalizował się w fizyce nuklearnej i kwantowej teorii pola (przez wiele lat pracował w ośrodku CERN), ale największą sławę przyniosły mu prace, dotyczące konceptualnych podstaw mechaniki kwantowej, przede wszystkim zaś — praca, zawierająca wynik, znany obecnie jako twierdzenie Bella.

<sup>2</sup>Zob. J. S. Bell, *Speakable and Unsayable in Quantum Mechanics. Collected Papers on Quantum Philosophy*, Cambridge University Press, Cambridge 2004.

<sup>3</sup>Tamże, s. 170.

<sup>4</sup>Teorie w sposób szczególnie faworyzowane przez Bella to teoria fali pilotującej de Broglie'a-Bohma oraz teoria spontanicznego kolapsu funkcji falowej, sformułowana przez G. C. Ghirardiego, A. Rimini i T. Webera.

<sup>5</sup>Por. A. Aspect, „Introduction: John Bell and the second quantum revolution”, w: J.S. Bell, *Speakable and Unsayable in Quantum Mechanics*, dz. cyt., s. xvii-xxxix.

## 1. DWIE REWOLUCJE

Różnica pomiędzy tym, co w mechanice kwantowej działo się w pierwszej połowie XX wieku, i tym, co dzieje się obecnie, jest tak zasadnicza, że mówi się w tym kontekście o dwóch różnych rewolucjach kwantowych: pierwszej i drugiej. Pierwsza z nich doprowadziła do zbudowania teoretycznych i eksperymentalnych podstaw fizyki kwantowej, i miała w rzeczywistości charakter rewolucji konceptualnej, w czasie której radykalnej zmianie uległo zarówno potoczne, jak i ściśle naukowe, wyobrażenie na temat tego, w jaki sposób funkcjonuje fizyczna rzeczywistość na najbardziej podstawowym — to jest kwantowym — poziomie. Druga rewolucja kwantowa pozwoliła na znalezienie konkretnych zastosowań dla reguł, rządzących światem kwantowym, i stała się okresem rozwoju nowych, kwantowych technologii, umożliwiających nie tylko badanie tego świata, ale również jego przekształcanie i dostosowywanie do konkretnych, praktycznych celów. Różnicę pomiędzy pierwszą i drugą rewolucją kwantową w trafny sposób ujmują w jednym ze swoich artykułów J. P. Dowling i G. J. Milburn:

Nie jesteśmy już pasywnymi obserwatorami świata kwantowego, który jest nam dany. W pierwszej rewolucji kwantowej wykorzystywaliśmy mechanikę kwantową, by zrozumieć to, co już istnieje. Mogliśmy wyjaśnić tablicę okresową pierwiastków, ale nie projektować i budować własne atomy. Mogliśmy wyjaśnić, w jaki sposób zachowują się metale i półprzewodniki, ale nie wpływać na to zachowanie. Różnica pomiędzy nauką i technologią polega na możliwości projektowania własnego otoczenia w najdrobniejszych szczegółach, a nie jedynie wyjaśniania go. W drugiej rewolucji kwantowej w sposób aktywny wykorzystujemy mechanikę kwantową po to, aby zmieniać kwantowe oblicze świata przyrody. Tworzymy w nim dla własnych celów zaprojektowane przez siebie sztuczne stany kwantowe. (...) Choć mechanika kwantowa jako nauka dojrzała już całkowicie, inżynieria kwantowa — jako technologia — dopiero teraz pojawia się [i funkcjonuje] na własnych prawach.<sup>6</sup>

---

<sup>6</sup>J. P. Dowling, G. J. Milburn, „Quantum technology: the second quantum revolution”, *Philosophical Transactions of the Royal Society A*, 361 (2003), s. 1656.

Nie ulega wątpliwości, że rewolucja technologiczna nie byłaby możliwa bez radykalnej rewolucji konceptualnej, jaka miała miejsce w pierwszej połowie wieku XX. Zwolennicy szkoły kopenhaskiej utrzymują, że ta ostatnia — to znaczy konceptualna — rewolucja zakończyła się wtedy, gdy twórcy mechaniki kwantowej zbudowali formalizm tej teorii. Zakończyła się — ponieważ wszystkie istotne zagadnienia o charakterze konceptualnym zostały w satysfakcjonujący sposób wyjaśnione przez Bohra, Heisenberga, i innych fizyków, którzy stworzyli formalizm mechaniki kwantowej, i nadali mu stosowną interpretację. Czy rzeczywiście tak było? Wiele wskazuje na to, że — wbrew tej ostatniej opinii — pierwsza rewolucja kwantowa cały czas trwa, a jej bardzo istotny etap dokonał się nie tak dawno właśnie za sprawą Johna S. Bella. Prace tego fizyka uzmysłowiły uczynom, że wiele pojęć i koncepcji, tworzących pojęciowy fundament mechaniki kwantowej, wymaga zasadniczego doprecyzowania.

Szczególną rolę w tym procesie odegrał niepozorny artykuł Bella z roku 1964, dotyczący paradoksu EPR, i zawierający wynik, znany obecnie jako twierdzenie Bella.<sup>7</sup> Publikacja ta umożliwiła przynajmniej częściowe rozstrzygnięcie ciągnącego się od wielu lat sporu, dotyczącego teorii zmiennych ukrytych: dowiodła ona, że żadna tego typu teoria, zgodna z warunkiem lokalnej przyczynowości, nie jest w stanie odtworzyć wszystkich empirycznych predykcji standardowej mechaniki kwantowej.<sup>8</sup> O doniosłości tego wyniku może świadczyć to, że o doświadczeniach, w których empirycznym testom poddano nierówności Bella<sup>9</sup>, dosyć powszechnie zaczęto mówić, iż rozpoczynają

---

<sup>7</sup>J. S. Bell, „On the Einstein-Podolsky-Rosen paradox”, *Physics*, 1 (1964), s. 195-200.

<sup>8</sup>Co istotne, twierdzenie Bella nie falsyfikuje nielokalnych (a jedynie lokalne) wersji teorii zmiennych ukrytych.

<sup>9</sup>Nierówność Bella jest matematycznym wyrażeniem, które stanowi konstytutywny element twierdzenia Bella, i które umożliwia empiryczne rozstrzygnięcie sporu pomiędzy standardowym sformułowaniem mechaniki kwantowej i lokalną teorią zmiennych ukrytych. Pierwsza z tych teorii przewiduje naruszenie nierówności, druga z nich — nie. Wyniki empirycznych testów nierówności Bella jednoznacznie potwierdzają poprawność mechaniki kwantowej i falsyfikują każdą teorię zmiennych ukrytych, zgodną z warunkiem lokalności.

one erę „eksperymentalnej metafizyki”.<sup>10</sup> Ale praca Bella z roku 1964 odegrała również inną rolę: bezpośrednio przyczyniła się do tego, że uczeni dostrzegli ogromne możliwości związane z praktycznym wykorzystaniem fenomenu kwantowego splątania, i innych niezwyklej własności układów kwantowych. To z kolei doprowadziło do zapoczątkowania gwałtownego postępu technologicznego, będącego najbardziej wyraźnym symptomem drugiej rewolucji kwantowej. Nic dziwnego, że we wstępie do tomu zawierającego artykuły Bella, dotyczące conceptualnych podstaw mechaniki kwantowej<sup>11</sup>, Aspect określa tego fizyka mianem „proroka drugiej rewolucji kwantowej” i podkreśla, że jego naukowe osiągnięcia „wywołały tę rewolucję”.<sup>12</sup>

To właśnie pod wpływem artykułów Bella fizycy zaczęli na nowo bacznie przyglądać się trudnościom, o których przez całe lata sądzono, że zostały raz na zawsze definitywnie rozwiązane przez twórców mechaniki kwantowej, a które w rzeczywistości okazały się ujawniać zasadnicze nieścisłości dotyczące kluczowych koncepcji i pojęć tej teorii. Najlepszym przykładem tego typu trudności jest problem pomiaru, a szczególnie te jego aspekty, które dotyczą nieprecyzyjnie określonej granicy pomiędzy światem kwantowym i makroskopowym. Tym zaś, co dostarczyło bezpośredniego impulsu, rozpoczynającego technologiczną rewolucję mechaniki kwantowej, były prace Bella, dotyczące kwantowego splątania cząstek (twierdzenie Bella), i zawierające teoretyczne podstawy metod, które umożliwiają kwantowy opis pojedynczych obiektów subatomowych.

Co prawda, już w pierwszej połowie XX wieku przedstawiciele szkoły kopenhaskiej podkreślali — zwłaszcza przy okazji dyskusji

---

<sup>10</sup>Por. np.: A. Shimony, „Contextual hidden variables theories and Bell’s inequalities”, *The British Journal for the Philosophy of Science*, 35 (1984) s. 25-45; R. S. Kochen, M. Horne, J. J. Stachel (red.), *Experimental Metaphysics. Quantum Mechanical Studies for Abner Shimony*, vol. I, Kluwer Academic Publishers, Dordrecht 1997; M. L. G. Redhead, *From Physics to Metaphysics*, Cambridge University Press, Cambridge 1995, s. 41-62.

<sup>11</sup>J. S. Bell, *Speakable and Unsayable in Quantum Mechanics*, dz. cyt.

<sup>12</sup>A. Aspect, *Introduction: John Bell and the second quantum revolution*, art. cyt., s. xix, xxxiv.

z Einsteinem i innymi oponentami ich stanowiska<sup>13</sup> — że formalizm standardowej mechaniki kwantowej umożliwia kwantowy opis nie tylko zespołów statystycznych, złożonych z wielkiej ilości cząstek, ale również pojedynczych obiektów kwantowych. Aż do lat 70-tych XX wieku, kiedy to fizykom udało się opracować metody, umożliwiające nie tylko obserwowanie tego typu obiektów, ale również bezpośrednie nimi manipulowanie, była to jednakże tylko i wyłącznie teoretyczna możliwość. Wszystkie istotne doświadczenia, dostarczające empirycznych dowodów na poprawność predykcji, wynikających z formalizmu standardowej mechaniki kwantowej, miały zawsze charakter doświadczeń statystycznych. W tego typu doświadczeniach wykorzystuje się każdorazowo ogromne ilości cząstek kwantowych — np. fotonów lub elektronów — a na dodatek sam eksperyment powtarza się wielokrotnie, aby wykluczyć różnego rodzaju błędy systematyczne, i określić statystyczny rozrzut wyników. Predykcje mechaniki kwantowej mają w tym przypadku charakter probabilistyczny — określają prawdopodobieństwo, z jakim pewna część cząstek zostanie zarejestrowana w danym detektorze, albo z jakim określony procent powtarzanych prób zakończy się takim lub innym wynikiem.

Zasadniczą zmianę tej tendencji przyniosły ostatnie dekady wieku XX, kiedy to fizykom udało się wyizolować (pułapki elektromagnetyczne) i obserwować pojedyncze obiekty kwantowe, takie jak fotony, elektrony, jony i atomy. W krótkim czasie doprowadziło to do opracowania nowych technologii, bazujących na możliwości kontrolowania tego typu obiektów. Na gruncie ewoluującej w taki sposób mechaniki kwantowej pojawiły się zupełnie nowe dziedziny (np. nanoelektronika, nanoinżynieria, nanomedycyna, kwantowa optyka, nanobiotechnologia, nanometrologia), umożliwiające radykalny postęp technologiczny, którego najbardziej charakterystycznym przejawem stała się miniaturyzacja, niemożliwa do uzyskania na drodze tradycyjnego pomniejszania obiektów rządzonych prawami fizyki klasycznej. Wiele wskazuje na to, że żadna z tych dziedzin nie mogłaby ani powstać, ani

---

<sup>13</sup>Por. M. Jammer, *The Philosophy of Quantum Mechanics: the Interpretation of Quantum Mechanics in Historical Perspective*, John Wiley and Sons, New York 1974, rozdział 10.

tym bardziej rozwinąć się w tak szybkim tempie, bez pionierskich prac Bella dotyczących metod umożliwiających przeprowadzanie eksperymentów na pojedynczych obiektach kwantowych.

## 2. KWANTOWA KRYPTOGRAFIA

Wyniki uzyskane przez Bella — a szczególnie jego nierówność, ujawniająca niezwykle własności cząstek splątanych — w najbardziej istotny sposób wpłynęły na powstanie dziedziny określanej ogólnym mianem kwantowej informatyki (*quantum information*)<sup>14</sup>, z której wyodrębniły się kwantowa kryptografia (*quantum cryptography*) i kwantowe przetwarzanie danych (*quantum computation*).<sup>15</sup> Dyscypliny te zajmują się wykorzystaniem własności obiektów kwantowych do celów bezpiecznego przesyłania, kodowania i przetwarzania informacji, a ich powstanie jest pośrednim dowodem na to, że splątanie nie jest jedynie dziwną cechą obiektów kwantowych, ale że może stać się ono „ważnym narzędziem technologicznym”.<sup>16</sup>

Najbardziej wyraźny związek wymienionych dziedzin z naukowym dorobkiem Bella daje się zauważyć w przypadku kwantowej kryptografii.<sup>17</sup> Jak wiadomo, podstawowym celem jakiegokolwiek formy kodowania informacji jest takie jej zabezpieczenie, aby odczytanie tej in-

---

<sup>14</sup>Na temat tej dziedziny, por. np. M. Pavicic, *Quantum Computation and Quantum Communication: Theory and Experiments*, Springer, New York 2006; J. Audretsch (red.), *Entangled World. The Fascination of Quantum Information and Computation*, Wiley-VCH Verlag, Weinheim 2002; J. Stolze, D. Suter, *Quantum Computing: A Short Course from Theory to Experiment*, Wiley-VCH Verlag, Weinheim 2008; A. Whitaker, *Einstein, Bohr and the Quantum Dilemma. From Quantum Theory to Quantum Information*, Cambridge University Press, Cambridge 2006, s. 352-412.

<sup>15</sup>„These new ways of communication and of computation include as a fundamental concept quantum entanglement. It is safe to say that this very recent development would not have been possible without John Bell’s seminal work”; A. Zeilinger, „Bell’s Theorem, Information and Quantum Physics”, w: R. A. Bertlmann, A. Zeilinger (red.), *Quantum [Un]speakables. From Bell to Quantum Information*, Springer, Berlin 2002, s. 246.

<sup>16</sup>J. P. Dowling, G. J. Milburn, „Quantum technology: the second quantum revolution”, art. cyt. s. 1658.

<sup>17</sup>Por. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, „Quantum cryptography”, *Reviews of Modern Physics*, 74 (2002), s. 145-195.

formacji było możliwe dla tych odbiorców, którzy mają do tego uprawnienia, i nie było możliwe dla tych, którzy takich uprawnień nie posiadają. W klasycznej kryptografii zasadniczą rolę w procesie bezpiecznego kodowania i odczytywania zakodowanej informacji ma tak zwany klucz szyfrujący, który — w przypadku algorytmów symetrycznych — występuje zawsze w dwóch identycznych kopiach dostępnych jedynie nadawcy i odbiorcy informacji.<sup>18</sup> Podstawowe znaczenie dla skuteczności całego procesu kryptograficznego ma w tym przypadku to, że aby nadawca mógł bezpiecznie przekazywać informację odbiorcy, najpierw obydwaj oni muszą mieć pewność, że są w posiadaniu jednej z dwu identycznych kopii klucza, i że nikt inny takiej kopii nie posiada. W przypadku klasycznym nadawca i odbiorca informacji nigdy nie mogą mieć absolutnej pewności, że klucz nie został przechwycony przez nieupoważnionych do tego, postronnych obserwatorów.

Kwantowa kryptografia pozwala w stosunkowo prosty sposób uporać się z tą trudnością. Co istotne, o istnieniu takiej możliwości fizycy dowiedzieli się właśnie dzięki pracom Bella dotyczącym skorelowanych cząstek układu EPR. Tego typu układy tworzą (najczęściej dwie<sup>19</sup>) cząstki pozostające w stanie „splątanych”, który charakteryzuje się tym, że pomiar pewnej własności jednej z tych cząstek powoduje natychmiastowe — niezależnie od dzielących cząstki odległości — określenie tej samej własności drugiej cząstki. Artur Ekert, który jako jeden z pierwszych fizyków już w 1991 roku wykazał, że zjawisko kwantowego splątania może zostać wykorzystane do bezpiecznego przesyłania klucza szyfrującego, podkreśla, że sama idea kwantowej kryptografii jest warta właśnie w twierdzeniu Bella:

Wpływ twierdzenia Bella znacznie wykracza poza problematykę dotyczącą odrzucenia lokalnych zmiennych ukrytych. Metoda, którą John Bell wykorzystał do zbadania konceptualnych

---

<sup>18</sup>W kryptografii asymetrycznej występuje powszechnie dostępny klucz publiczny, służący do szyfrowania informacji, i klucz prywatny, dostępny jedynie określonej odbiorcy informacji, który służy do jej deszyfrowania. Dodatkowo, klucz prywatny służy do generowania podpisów cyfrowych, a klucz publiczny do ich weryfikowania.

<sup>19</sup>Obecnie przeprowadza się już doświadczenia EPR z trzema (lub nawet z większą liczbą) splątanych cząstek.



podstaw mechaniki kwantowej, została zastosowana do rozwiązania odwiecznego problemu absolutnie bezpiecznej komunikacji.<sup>20</sup>

Na czym polega metoda, o której pisze Ekert? Zgodnie z podstawowymi zasadami mechaniki kwantowej, nie jest możliwy taki pomiar, który nie powodowałby żadnego zaburzenia układu poddawanego temu pomiarowi. O obecności postronnego obserwatora usiłującego przechwycić klucz szyfrujący, można się zatem przekonać na podstawie pozostawionego przez niego śladu: jakakolwiek ingerencja w kwantowy układ złożony z nadawcy i odbiorcy informacji powoduje bowiem niemożliwe do wyeliminowania zaburzenie, które można potraktować jako dowód obecności szpiega. Brak takiego zaburzenia — to znaczy śladu pozostawionego przez nieupoważnionego obserwatora — daje absolutną pewność, że przekazywana informacja nie została przez żadną postronną osobę odczytana.<sup>21</sup>

Praktyczną realizację przedstawionego powyżej schematu umożliwiają eksperymenty ze splątanymi cząstkami układu EPR. Aby wygenerować unikatowy i niemożliwy do przechwycenia klucz szyfrujący, wystarczy wykorzystać skorelowane pary tego typu cząstek. Nadawca przeprowadza pomiar na jednej, a odbiorca na drugiej, cząstce splątanej pary. Ponieważ rezultaty takich pomiarów są przypadkowe, ale doskonale skorelowane, każdy z nich otrzymuje identyczny wynik. Kilukrotne powtórzenie przeprowadzonego w opisany sposób pomiaru pozwala wygenerować dwie identyczne kopie klucza szyfrującego o całkowicie przypadkowej kolejności znaków, tworzących zawartą w tym kluczu informację. Co istotne, tego typu klucz — w dwóch identycznych kopiach — pojawia się dopiero w momencie dokonywania pomiarów przez nadawcę i odbiorcę, a przed tym momentem klucz ten w ogóle nie istnieje. Z analizy układu EPR wynika bowiem, że wyników pomiaru przeprowadzanego na takim układzie w żaden sposób nie

---

<sup>20</sup>A. Ekert, „Secret Sides of Bell’s Theorem”, w: *Quantum [Un]speakables*, dz. cyt., s. 210.

<sup>21</sup>Por. A. Ekert, „Quantum cryptography based on CityBell’s theorem”, *Physical Review Letters*, 67 (1991), s. 661-663; C. H. Bennet, G. Brassard, N. D. Mermin, „Quantum cryptography without Bell’s theorem”, *Physical Review Letters*, 68 (1992), s. 557-559.

da się przewidzieć. Podstawową zaletą tego rozwiązania jest więc to, że potencjalny szpieg nie może w tym przypadku przechwycić klucza wcześniej niż zostanie on wygenerowany przez nadawcę i odbiorcę; nie ma on również możliwości ukrycia swoich prób przechwycenia klucza w trakcie jego generowania.

Należy podkreślić, że przedstawiony powyżej schemat oparty jest w całości na teoretycznych analizach Bella, których słuszność została ostatecznie potwierdzona wynikami empirycznych testów nierówności Bella. Aspect nie bez racji zauważa, że „nierówności Bella odgrywają pierwszoplanową rolę w tym schemacie: ich naruszenie daje pewność, że cząstki, docierające do [nadawcy i odbiorcy] nie zostały podstępnie przygotowane przez [szpiega] w taki sposób, że zna on ich stan, i to umożliwi mu odszyfrowanie wiadomości pomiędzy nadawcą i odbiorcą”.<sup>22</sup> Warto w tym miejscu dodać, że omówiony schemat kwantowej kryptografii nie jest jedynie teoretyczną dywagacją na temat potencjalnej możliwości wykorzystania fenomenu kwantowego splątania. W ostatnich latach przeprowadzono wiele eksperymentów, które potwierdziły skuteczność tej metody szyfrowania danych, a najlepszym dowodem że metoda ta sprawdza się w praktyce jest to, że rozpoczęto już produkcję i sprzedaż urządzeń służących do przesyłania — np. przy pomocy światłowodów — kwantowych kluczy szyfrujących.<sup>23</sup>

### 3. KWANTOWY KOMPUTER

Z innych, pokrewnych dziedzin, przed którymi za sprawą mechaniki kwantowej otwierają się obecnie ogromne możliwości, warto w tym miejscu wspomnieć o kwantowym przetwarzaniu danych.<sup>24</sup> Pierwsze plany zbudowania kwantowego komputera pojawiały się już na początku lat 80. ubiegłego wieku za sprawą takich fizyków, jak Ri-

---

<sup>22</sup>A. Aspect, „Introduction: John Bell and the second quantum revolution”, art. cyt., s. xxxii-xxxiii.

<sup>23</sup>Zob. G. Stix, „Kwantowy strażnik poufności”, *Świat Nauki*, luty 2005, s. 59-63; G. Milburn, *Inżynieria kwantowa*. J. A. Kozubowski (tłum.), Prószyński i S-ka, Warszawa 1999, rozdział 5.

<sup>24</sup>Por. M. A. Nielsen, I. Chuang-Isaac, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge 2000.

chard Feynman, Paul Benioff, Peter Shor, David Deutsch, czy Artur Ekert. Ich projekty zakładały wykorzystanie praw mechaniki kwantowej do znacznego (eksponencjalnego) zwiększenia mocy obliczeniowej tradycyjnego komputera. W komputerze kwantowym odpowiednikiem tradycyjnego procesu obliczeniowego jest odpowiednio zaplanowana ewolucja stanów kwantowych całego układu, złożonego z kwantowych bramek logicznych. Różnica pomiędzy klasycznymi i kwantowymi bramkami logicznymi polega na tym, że w przypadku tych ostatnich zakres wartości podstawowej jednostki informacji (tzw. kubitu) nie jest ograniczony jedynie do dwóch możliwości, to znaczy do 0 i 1. Zakres ten obejmuje również wiele wartości pośrednich, które odpowiadają kwantowym superpozycjom stanów wyjściowych układu. Kwantowe bramki logiczne przetwarzają zatem więcej informacji niż bramki klasyczne, dzięki czemu komputery kwantowe mogą wykonywać równolegle wiele obliczeń, i na dodatek potrafią to robić znacznie szybciej niż ich tradycyjne odpowiedniki.<sup>25</sup>

Prace nad zbudowaniem w pełni funkcjonalnego kwantowego komputera trwają; fizycy zaangażowani w realizację tego programu mogą już poszczycić się pewnymi osiągnięciami — takimi jak np. skonstruowanie pierwszych kwantowych bramek logicznych<sup>26</sup> — choć do pełnego sukcesu pozostała jeszcze długa droga. Zasadniczą trudnością jest w tym przypadku wyeliminowanie wszystkich zewnętrznych czynników, które mogłyby zniszczyć koherentną superpozycję splątanych stanów kwantowych, zanim komputer wykona stosowne obliczenia. Pojawiają się tu interpretacyjne trudności dotyczące problemu dekoherencji: do dzisiaj nie wiadomo, czy dekoherencja jest procesem nieuniknionym dla określonej ilości — a jeśli tak, to dla jakiej ilości — splątanych cząstek kwantowego komputera, czy też można ją skutecz-

---

<sup>25</sup>Na ten temat, por. np. G. Milburn, *Inżynieria kwantowa*, dz. cyt., rozdział 6; G. Johnson, *Na skróty przez czas. Czy nadchodzi era komputerów kwantowych?*, K. Masłowski (tłum.), Prószyński i S-ka, Warszawa 2005.

<sup>26</sup>Zob. np. T. Sleator, H. Weinfurter, „Realizable Universal Quantum Logic Gates”, *Physical Review Letters*, 74 (1995), s. 4087-4090; C. Monroe, D. M. Meekhof, B. E. King, W. Itano, D. J. Wineland, „Demonstration of a fundamental quantum logic”, *Physical Review Letters*, 75 (1995), s. 4714-4717.

nie wyeliminować na drodze odpowiednich, technologicznych innowacji.<sup>27</sup>

Warto zauważyć, że zagadnienie to pojawia się w nieco innym kontekście również u Bella. Jednym z aspektów problemu nieprecyzyjnie określonej granicy pomiędzy światem kwantowym i makroskopowym, któremu w swoich pracach Bell poświęcał wiele uwagi, jest trudność dotycząca makroskopowych superpozycji stanów kwantowych. Z niewiadomych powodów — a w każdym razie niewiadomych dla standardowej mechaniki kwantowej — superpozycje można zaobserwować w przypadku obiektów kwantowych i mezoskopowych, ale nigdy makroskopowych. Aby wyjaśnić tę trudność, fizycy końca XX i początku XXI wieku odwołują się najczęściej właśnie do teorii dekoherencji. Jak na razie żaden z nich nie zdołał jednakże odpowiedzieć na to samo pytanie, które zadawał sobie Bell, a mianowicie — gdzie dokładnie znajduje się hipotetyczna granica, poza którą proces dekoherencji zachodzi w sposób konieczny i nieunikniony.<sup>28</sup> Aspect zauważa — oceniając wkład Bella w rozwój kwantowej technologii — że w tym przypadku nie jest również wyjaśnione w sposób zadowalający to, czy w ogóle istnieje możliwość takiego odizolowania układu (np. kwantowego komputera) od jego otoczenia, by zewnętrzne fluktuacje nie niszczyły koherentnej superpozycji stanów kwantowych, i jaka relacja zachodzi pomiędzy wielkością tych fluktuacji, a wielkością samego układu podlegającego dekoherencji.<sup>29</sup> Niezależnie od tego, czy fizykom uda się przewyciężyć te trudności, i czy kwantowy komputer rzeczywiście zostanie kiedyś skonstruowany, nie ulega wątpliwości, że sama idea wykorzystania procesów kwantowych do przetwarzania da-

---

<sup>27</sup>Por. C. Monroe, D. Wineland, „Future of quantum computing proves to be debatable”, *Physics Today*, 49/11 (1996), s. 107-108.

<sup>28</sup>Por. S. L. Adler, „Why decoherence has not solved the measurement problem: a response to P. W. Anderson”, *Studies in History and Philosophy of Science B*, 34/1 (2003), s. 135-142.

<sup>29</sup>„Nobody knows, however, where there is a hypothetical limit beyond which decoherence would be inevitable, or whether we always can, at least in principle, take sufficient precautions to protect the system against perturbations, no matter how large it is. A clear answer to that question would have immense consequences, both conceptually and for future quantum technologies”; A. Aspect, „Introduction: John Bell and the second quantum revolution”, art. cyt., s. xxxi.

nych ustala całkowicie nową jakość w dziedzinie współczesnych technik obliczeniowych.

Warto w tym miejscu nadmienić, że gwałtowny rozwój kwantowej informatyki, jaki daje się zauważyć w ostatnich latach, jest dla niektórych autorów argumentem za tym, iż mechanikę kwantową należy interpretować właśnie w kategoriach informacji. Anton Zeilinger — jeden ze zwolenników tego typu interpretacji — zauważa w kontekście tego zagadnienia, że nie miał racji Bell, zaliczający termin „informacja” do „niepoprawnych słów”<sup>30</sup>, które nie powinny pojawiać się w tej teorii.<sup>31</sup> Jeśli nawet wniosek ten jest słuszny — co nie jest oczywiste, bo Bell nie występował przeciwko samej *koncepcji* informacji, ale raczej przeciwko nie dość precyzyjnemu stosowaniu *pojęcia* informacji; poza tym nie kwestionował on stosowania tego pojęcia w obszarze *interpretacji* mechaniki kwantowej, ale jedynie w jej *sformułowaniu*<sup>32</sup> — to i tak nie zmienia to faktu, że to właśnie ten fizyk przyczynił się w istotnym stopniu do powstania i rozwoju kwantowej informatyki.

\*\*\*

Kwestionowanie naukowych dogmatów jest owocne, ale tylko wtedy gdy jest połączone z odpowiednim stopniem zawodowych kompetencji (uczony, który pozwala sobie na podważanie uświęconych tradycją rozwiązań, musi w przekonujący sposób swoją propozycję uzasadnić, i gdy idzie w parze z cywilną odwagą (musi on liczyć się z realną możliwością lekceważenia, a nawet napiętnowania przez przedsta-

---

<sup>30</sup>Zob. J. S. Bell, *Speakable and Unsayable in Quantum Mechanics*, dz. cyt., s. 215.

<sup>31</sup>„By now, the reader might have gathered that the present author does not agree with John Bell’s statement. In contrast it is suggested that information is the most basic notion of quantum mechanics, and it is information about possible measurement results that is represented in the quantum states”; A. Zeilinger, „Bell’s Theorem, Information and Quantum Physics”, art. cyt. s. 252. Na temat informacyjnej interpretacji mechaniki kwantowej, por. np. R. Nakmanson, „Informational interpretation of quantum mechanics”, arXiv:physics/0004047v1.

<sup>32</sup>„Information [...] that notion should not appear in the formulation of fundamental theory”; J. S. Bell, *Speakable and Unsayable in Quantum Mechanics*, dz. cyt., s. 215.

wicieli obowiązującego paradygmatu), a także naukową intuicją, która w ogromnej ilości zagadnień błahych pozwala dostrzegać problemy o charakterze fundamentalnym (musi on przewidywać, albo przynajmniej przeczuwać, konsekwencje własnych propozycji). Najlepszym dowodem na to, że Bell spełnił każdy z tych warunków, jest niezwykle szeroki zakres rewolucji technologicznej — wiele wskazuje na to, że nanotechnologia będzie w przewidywalnej przyszłości wkraczać w kolejne dziedziny nauk ścisłych — a także znaczne tempo, w jakim ta rewolucja się dokonuje.

Interesującym aspektem tego procesu jest to, że wydaje się on ujawniać stopniowe zacieranie się metodologicznych granic pomiędzy różniącymi się w istotny sposób dziedzinami nauk ścisłych. Jeśli bowiem technologiczne innowacje mechaniki kwantowej znajdują swoje zastosowanie w takich dziedzinach, jak np. medycyna, optyka, informatyka czy biologia, to siłą rzeczy metodologiczny status tych dziedzin ulega zasadniczej modyfikacji. Wiele wskazuje na to, że można w tym przypadku mówić o ewolucji metody naukowej, i że konsekwencje tego procesu nie ominą również samej mechaniki kwantowej. Czy druga rewolucja kwantowa rzeczywiście umożliwi ostateczne wyjaśnienie wszystkich problemów, związanych z interpretacją matematycznego formalizmu tej teorii? Czy zaawansowanie technologiczne pozwoli na usunięcie sygnalizowanych przez Bella „fundamentalnych nieścisłości” interpretacji standardowej? Mechanika kwantowa jest niedokończoną powieścią napisaną przed wiekiem przez twórców tej teorii. Należy mieć nadzieję, że odpowiedzi na te pytania wcześniej czy później ułożą się w brakujący epilog tej powieści.

### *SUMMARY*

#### *THE SECOND QUANTUM REVOLUTION: THE LEGACY OF JOHN S. BELL*

The history of quantum mechanics is divided into two periods which are labeled as the first and the second quantum revolutions. During the first of these periods mathematical formalism of quantum theory was formulated and interpreted, during the second — new quantum technologies were developed. It turns out that conceptual revolution of the first period enabled technolog-

---

ical revolution of the second. In this article it is argued, that Irish physicist, John S. Bell, played an important role in the process of triggering the second quantum revolution. His work on quantum entanglement of the EPR particles made possible elaborating some new methods and theoretical approaches clarifying the quantum description of single objects. These methods and approaches became the core of new scientific domains which are hybrids of quantum mechanics and some classical sciences. The quantum cryptography and the quantum computation are examples of such domains and in the paper special attention is paid to them. It is showed that theoretical analyses of John S. Bell provide a conceptual background for these disciplines and this is why it's not improper to call this physicist — as Alain Aspect did — a prophet of the second quantum revolution.