STUDIA PRAWA PUBLICZNEGO
2024 • NR 3 (47) ISSN 2300-3936
https://doi.org/10.14746/spp.2024.3.47.3

Dorota Glaza-Jankowska*

Rozwój technologii kwantowej: wyzwania i aspekty regulacyjne. Przegląd wybranych zagadnień prawnych

Review of selected legal issues related to the development of quantum technology: challenges and regulatory aspects

Abstract. In the era of the Fourth Industrial Revolution, quantum technology is entering the scene with the promise of radically changing the technological paradigm. Quantum computing, simulation, quantum communications and the combination of this technology with artificial intelligence are opening up new horizons of innovation that could revolutionize various industries. Along with its enormous potential, this technology brings legal, ethical and social challenges that require detailed analysis and an interdisciplinary approach. The industrial deployment of quantum technology entails dilemmas regarding human rights, cyber security and national security, as well as the risk of exacerbating inequality, technological exclusion and algorithmic discrimination. With regard to artificial intelligence enhanced by quantum computing technology, we can speak of a completely new facet of the problem of the opacity of algorithms, which is determined not only by the cognitive limitations of the human mind, but stems from the indefinability of the world described by the laws of quantum mechanics. In light of the above, the thesis can be advanced that the classical approach to the principle of transparency and the postulates of creating algorithms that will clearly present the path to the final result, which are part of the broad current of creating ethical and explainable artificial intelligence, may prove difficult to realize in relation to Quantum AI. In the era of the Fourth Industrial Revolution, we are therefore faced with the challenge of implementing new instruments for testing, certifying and inspecting algorithms, such as tools for analyzing and visualizing the results of quantum algorithms, which will be suited to the specifics of Quantum AI and ensure the ethical correctness of the systems. This article will identify selected areas of application of quantum technology, and thus the potential benefits and risks of quantum technology, and also analyze the need

* University of Gdansk, Poland | Uniwersytet Gdański, Polska, https://orcid.org/0009-0006-8460-2755, e-mail: dorota.m.glaza@gmail.com.

SPP 3(47), 2024: 55–84. © The Author(s). Published by: Adam Mickiewicz University Press, 2024.

to develop ethical and legal standards that allow for the sustainable and socially responsible development of these disruptive technologies.

Keywords: quantum technology – quantum cryptography – quantum communication – quantum artificial intelligence – black box problem

Wprowadzenie

Inżynieria kwantowa stanowi zespół nauk i technologii opartych na ogólnych zasadach mechaniki kwantowej, takich m.in. jak superpozycja, splątanie, zasada nieoznaczoności Heisenberga, dualizm kwantowy i tunelowanie. Zjawiska te brzmią abstrakcyjnie, niemal metafizycznie i są trudne do wyobrażenia dla większości ludzi, gdyż nie mają one odpowiedników w makroskopowym świecie. Zyskują jednak coraz większe znaczenie dla rozwoju nowej technologii, której wdrożenie w skali przemysłowej może spowodować zmiany w każdym niemal aspekcie naszego życia, otwierając drogi do futurystycznego świata, w którym innowacje i wydajność staną się immanentną cechą rzeczywistości. Przewiduje się, że w przyszłości dziedziny takie jak obliczenia kwantowe, symulacje, komunikacja kwantowa, wykrywanie i metrologia, a także połączenie obliczeń kwantowych ze sztuczną inteligencją przyniosą zmiany paradygmatu w zakresie możliwości technologicznych. Ze względu na transformacyjny wpływ i wartość geopolityczną nowej technologii kwantowej zarówno dla przemysłu cywilnego, jak i obronności rządy państw oraz giganci technologiczni podejmują starania o zwiększenie potencjału w zakresie badań i rozwoju technologii kwantowej, uczestnicząc w wyścigu o ,,kwantową supremację", czyli stan, w którym komputer kwantowy zdoła rozwiązać problem niemożliwy do rozwiązania przez klasyczny komputer cyfrowy w dowolnym czasie rzeczywistym[1]. Stawka jest bardzo wysoka, ponieważ uzyskanie pozycji dominującej w kwantowym świecie może ukształtować globalny układ sił w bezprecedensowy sposób.

[1] Supremacja kwantowa to eksperymentalna demonstracja dominacji i przewagi komputera kwantowego nad klasycznymi komputerami poprzez wykonywanie obliczeń wcześniej niemożliwych z niezrównaną prędkością. Najbardziej znanym przykładem supremacji kwantowej, którą ogłoszono po raz pierwszy w 2019 r., jest obliczenie wykonane przez komputer kwantowy Sycamore, który wykonał obliczenie w 200 sekund, co według szacunków Google zajęłoby 10 tys. lat najszybszemu superkomputerowi klasycznemu Summit, należącemu do firmy IBM. Przy czym należy zaznaczyć, że przewaga kwantowa na chwilę obecną dotyczy bardzo specyficznych i sztucznie stworzonych problemów.

1. Obszary zastosowania technologii kwantowej

Istnieje szereg możliwych zastosowań, w których technologia kwantowa będzie miała szczególnie przełomowe znaczenie. Obecnie możemy wyróżnić sześć kluczowych kierunków rozwoju tej technologii, do których zalicza się: obliczenia kwantowe, komunikację kwantową, wykrywanie kwantowe, symulację kwantową, podstawową naukę kwantową oraz powiązanie ze sztuczną inteligencją[2]. Technologia kwantowa, mimo iż znajduje się na wczesnym etapie rozwoju, roztacza nowe perspektywy dla rozwiązywania złożonych problemów obliczeniowych, które nie są osiągalne dla klasycznych komputerów cyfrowych. Komputery kwantowe są w stanie przetwarzać informacje z prędkością wykładniczo wyższą niż komputery cyfrowe[3]. Wykorzystując fundamentalne zasady fizyki kwantowej, takie jak superpozycja i splątanie, umożliwiają synchroniczną analizę wszystkich dostępnych danych, co powoduje skokowy wzrost mocy obliczeniowej. Stwarza to możliwości dla wykorzystania obliczeń kwantowych do analizy problemów optymalizacyjnych w łańcuchu dostaw, komunikacji, logistyce, materiałoznawstwie, sektorze energetycznym, finansowym i kryptografii. Komercjalizacja technologii kwantowej może przyczynić się do postępu w sektorze farmaceutycznym i tworzenia spersonalizowanej medycyny, m.in. przez modelowanie komputerowe kluczowych funkcji w ludzkim organizmie, co umożliwi rozwój nowych narzędzi diagnostycznych, a także testowanie działania i efektów ubocznych nowych leków szybciej, niż pozwalają na to dotychczasowe metody oraz przy znacznym obniżeniu ryzyka. Spełnieniem marzeń badaczy byłaby możliwość ustalenia przebiegu dowolnej reakcji chemicznej na poziomie atomowym przez wykonanie samej tylko symulacji w komputerze kwantowym, bez konieczności użycia jakichkolwiek związków chemicznych[4]. Wykorzystanie komputerów

[2] A. Dalton, *Quantum Technology Comes of Age*, „Science" 2019, 366(6464), s. 898–900, https://www.science.org/content/article/quantum-technology-comes-age (dostęp: 8 VIII 2024).

[3] F. Bova, A. Goldfarb, R.G. Melko, *Quantum Economic Advatage*, „Management Science" 2022, 69(2), s. 1116–1126, http://www.nber.org/papers/w29724 (dostęp: 18 VIII 2024).

[4] Dziedziną wiedzy, która stosuje programy do modelowania molekularnego implementujące metody chemii kwantowej do rozwiązywania rzeczywistych problemów chemicznych, jest chemia obliczeniowa. Przewiduje się, że pewnego dnia symulacje komputerowe mogą całkowicie wyeliminować konieczność przeprowadzania kosztownych badań w warunkach laboratoryjnych. Zob. M. Kaku, *Kwantowa dominacja. Jak komputery kwantowe odmienią nasz świat*, tłum. B. Bieniok, E.L. Łokas, Warszawa 2023, s. 26.

kwantowych do modelowania zachowania atomów, cząstek elementarnych oraz modelowania natury może przybliżyć ludzkość do zgłębienia wiedzy na temat fundamentalnych procesów związanych z życiem. W dalszej perspektywie otworzy to drogę do odwzorowania wskazanych procesów w warunkach laboratoryjnych, przyczyniając się do opracowania sztucznej fotosyntezy, recyklingu dwutlenku węgla czy odkrycia metody efektywnego pozyskiwania azotu z powietrza w celu produkcji nawozów. Bez wątpienia można zatem stwierdzić, że potencjał transformacyjny technologii kwantowej jest niezwykły i przełomowy.

Obecnie przeprowadzane są również eksperymenty mające na celu połączenie technologii kwantowej ze sztuczną inteligencją. Generatywna sztuczna inteligencja (GenAI, ang. *generative artificial intelligence*) charakteryzuje się umiejętnością uczenia się na własnych błędach, dzięki czemu nadaje się ona do wykonywania coraz bardziej złożonych zadań. Największą barierą dla rozwoju sztucznej inteligencji jest problem jakości i dostępności danych. Dane te muszą być dokładne i reprezentatywne oraz odpowiednio oznaczone, aby algorytmy mogły je prawidłowo interpretować. Dodatkowym ograniczeniem jest konieczność analizowania przez AI dużych zbiorów danych i zasobów informacji, z którymi nie radzą sobie klasyczne komputery cyfrowe[5]. Tymczasem umiejętność przeszukiwania ogromnych zbiorów danych jest domeną komputerów kwantowych. Przewiduje się, że tworzenie systemów z wykorzystaniem mocy obliczeniowej i niedeterministycznego modelu przewidywania mechaniki kwantowej w synergii ze sztuczną inteligencją pozwoli na dynamiczny rozwój i upowszechnienie dobrodziejstw technologii opartej na AI. Społeczny i ekonomiczny wpływ tych przemian będzie tak rozległy, że nawet nie jesteśmy w stanie wyobrazić sobie ich następstw[6].

[5] Trenowanie dużych modeli uczenia maszynowego na komputerach cyfrowych zajmuje wiele miesięcy ze względu na złożoność obliczeń, które należy wykonać. Tytułem przykładu można wskazać, że GPT-3 firmy OpenAI ma 175 mld parametrów. Przekształcenie dostępnej dziś AI w zaawansowaną sztuczną inteligencję wymaga, aby modele te urosły do bilonów parametrów. Poruszany tu problem zasobów obliczeniowych dotyczy w szczególności mniejszych organizacji, czyli takich, które dysponują ograniczonymi środkami finansowymi i technologicznymi.

[6] Szerokie omówienie potencjalnych zastosowań technologii kwantowych zamieszczono w publikacji J.A. Lewis, G. Wood, *Quantum Technology: Applications and Implications*, Center for Strategic and International Studies (CSIS), maj 2023, https://www.csis.org/analysis/quantum-technology-applications-and-implications (dostęp: 19 VIII 2024).

2. Zagrożenia związane z wykorzystaniem nowych technologii kwantowych

Technologia kwantowa bardzo szybko ewoluuje od eksperymentalnych pomysłów do rzeczywistości komercyjnej. Antycypując dalsze spektakularne postępy w nauce kwantowej, należy dostrzec, że wraz ze wzrostem mocy obliczeniowej komputerów kwantowych wzrastają również obawy dotyczące niepożądanego zastosowania technologii *quantum computing*. Komercjalizacja zastosowania komputerów kwantowych niesie za sobą dylematy etyczne i zagrożenia na wielu płaszczyznach, wynikające z nadużyć, niewłaściwego użycia lub niezamierzonych konsekwencji, a dotykające tak delikatnych tkanek i esencjonalnych problemów jak prawa człowieka, cyberbezpieczeństwo i bezpieczeństwo narodowe. Wyzwania te można podzielić na takie, które znoszą istniejące zabezpieczenia, zaostrzają istniejące problemy i tworzą zupełnie nowe klasy zagrożeń.

Wśród podstawowych zagrożeń społecznych zidentyfikowanych do tej pory, wynikających z możliwych kierunków rozwoju i zastosowań technologii kwantowej wymienia się[7]:

1) ryzyko zwiększonej nierówności, monopolizacji poprzez własność intelektualną, efektu ,,zwycięzca bierze wszystko" i niemożliwej do zniwelowania dysproporcji w rozwoju technologii kwantowej na początkowym etapie jej wdrożenia;

2) zagrożenia dla stabilności systemu gospodarczego i finansowego, w tym zagrożenia dla kryptowalut i protokołów *blockchain*;

3) ryzyko związane z naruszeniem prywatności danych i bezpieczeństwem danych, pewnością prawa i zaufaniem;

4) zagrożenia związane z fałszywymi wiadomościami, bańkami filtrującymi, dezinformacją i ich wpływem na procesy demokratyczne;

5) zagrożenie związane z przejmowaniem kontroli nad urządzeniami elektronicznymi przez hakerów i niewłaściwym wykorzystaniem technologii szyfrowania oraz przetwarzania obrazu;

6) ryzyko związane z działalnością przestępczą, taką jak terroryzm, przestępczość zorganizowana i uchylaniem się od płacenia podatków;

[7] M. Kop, *Establishing a Legal-Ethical Framework for Quantum Technology*, „Yale Journal of Law & Technology. The Record", 30 III 2021, https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology (dostęp: 13 VIII 2024). Wskazane zagrożenia należy traktować jako reprezentatywne dla rodzajów ryzyka, które możemy zidentyfikować, a nie jako ostateczną listę wszystkich potencjalnych zagrożeń związanych z wykorzystaniem nowych technologii kwantowych.

7) ryzyko szkód środowiskowych;
8) ryzyko związane z autorytaryzmem, wzmożonym nadzorem i kontrolą państwa;
9) ryzyko zaburzonych stosunków geopolitycznych, kwantowych wyścigów zbrojeń, cyberwojen, zmienionych konstelacji sił i władzy;
10) ryzyko związane ze scenariuszami wyginięcia ludzkości.

3. Kryptoanaliza i kryptografia kwantowa

Uzasadnione obawy wzbudza m.in. dynamiczny rozwój kryptoanalizy kwantowej i potencjalna zdolność komputerów kwantowych do pokonywania konwencjonalnych protokołów szyfrowania opartych na pseudolosowych generatorach klucza, takich jak RSA (algorytm *Rivesta-Shamira-Adlemana*), DH (protokół *Diffiego-Hellmana*) i ECC (kryptografia krzywej eliptycznej). Bezpieczeństwo szyfrowania wyżej wskazanych schematów kryptografii opiera się na trudności faktoryzacji dużych liczb złożonych (RSA), na problemie logarytmu dyskretnego (DH) oraz na złożoności obliczeniowej dyskretnych logarytmów na krzywych eliptycznych (ECC). Konwencjonalne metody szyfrowania wykorzystują problemy matematyczne, które są łatwe do rozwiązania w jednym kierunku, ale bardzo skomplikowane obliczeniowo, lub nawet niewykonalne dla komputerów cyfrowych, w kierunku przeciwnym[8]. Przykładem takiego problemu jest faktoryzacja liczb, czyli proces rozkładu liczb na czynniki pierwsze. Uzyskanie wyniku działania matematycznego opartego na iloczynie dwóch dużych liczb pierwszych nie stwarza problemu, natomiast bardzo trudne obliczeniowo, o ile w ogóle możliwe do przeprowadzenia w rozsądnych ramach czasowych, jest zidentyfikowanie par liczb, które po pomnożeniu dały wstępnie zdefiniowany iloczyn.

Technologia kwantowa wprowadza nowy paradygmat obliczeniowy. Przewiduje się, że w przyszłości duża moc obliczeniowa komputerów kwantowych pozwoli na zastosowanie tzw. algorytmu Shora[9], który jest w stanie stosunkowo szybko dokonać rozkładu na czynniki pierwsze nawet bardzo dużych liczb złożonych. Wprawdzie algorytm Shora, podobnie jak inne algorytmy kwantowe, działa w oparciu o model

[8] V. Jeutner, *The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers*, „Morals & Machines" 2021, nr 1(1), s. 52–59, https://ssrn.com/abstract=3820003 (dostęp: 19 VIII 2024).
[9] M. Kaku, op. cit., s. 101–105.

probabilistyczny, co oznacza, że określa poprawną odpowiedź jedynie z pewnym prawdopodobieństwem, jednak z uwagi na fakt, że uzyskany wynik może zostać szybko zweryfikowany, powtarzanie algorytmu w sposób efektywny doprowadzi w końcu do uzyskania poprawnej odpowiedzi. Naukowcy przewidują, że w nieodległej perspektywie komputery kwantowe wykorzystujące działanie algorytmu Shora będą w stanie złamać protokół szyfrujący RSA, co spowoduje krytyczne zagrożenie dla integralności i bezpieczeństwa cyfrowych systemów finansowych, bezpiecznej komunikacji i podpisu elektronicznego[10]. Oznacza to bowiem, że od chwili złamania mechanizmu szyfrowania opartego o algorytm RSA wszystkie informacje przesyłane w formie zaszyfrowanej przez ten algorytm będą mogły zostać rozszyfrowane – i to z mocą wsteczną – oraz ujawnione osobom niepowołanym[11]. W odniesieniu do powyższych zagrożeń wskazuje się, że ze względu na kosztowność budowy i trudności technologiczne w zastosowaniu komputerów kwantowych, przez wiele lat ich dostępność pozostanie poza zasięgiem prywatnych organizacji i przedsiębiorstw bez dużych, trwałych budżetów. Największe obawy w kontekście zagrożeń dla cyberbezpieczeństwa stwarza w tej sytuacji możliwość wykorzystania technologii kwantowej przez reżimy totalitarne oraz technoautokratyczne, które uczestniczą w wyścigu o kwantową dominację.

W obliczu narastających obaw związanych z zastosowaniem technologii kwantowej w celu obejścia klasycznych protokołów szyfrowania, których działanie opiera się na ograniczeniach obliczeniowych komputerów cyfrowych, administracja Joe Bidena uznała, że ryzyko przegrania wyścigu o innowacje w dziedzinie obliczeń kwantowych z przeciwnikami Stanów Zjednoczonych jest na tyle poważne, że wymaga interwencyjnego działania. W 2022 r. prezydent podpisał Ustawę o przygotowaniu cyberbezpieczeństwa obliczeń kwantowych, na mocy której Biuro Zarządzania i Budżetu (Office of Management and Budget, OMB) uzyskało możliwość wdrażania technologii opartej na kryptografii postkwantowej[12]. Stanowi to kamień milowy w globalnych

[10] Ibidem.

[11] Zob. R. Bieda, D. Skrodzka-Kwietniak, *Jak technologia kwantowa wpłynie na bezpieczeństwo informatyczne – rozmowa z gen. Włodzimierzem Nowakiem*, w: *Metaświat. Prawne i techniczne aspekty przełomowych technologii*, pod red. R. Biedy, Z. Okonia, Warszawa 2023, s. 404.

[12] Quantum Computing Cybersecurity Preparedness Act, treść aktu dostępna na stronie internetowej Kongresu Stanów Zjednoczonych: https://www.congress.gov/bill/117th-congress/house-bill/7535/text5–117th.

wysiłkach na rzecz projektowania, implementacji oraz operacyjnego zarządzania strategiami i systemami cyberbezpieczeństwa odpornego na zagrożenia związane z rozwojem komputerów kwantowych. Z kolei w maju 2022 r. administracja Joe Bidena opracowała memorandum zatytułowane *Promoting United States Leadership in Quantum Cryptographic Systems*, w którym zdefiniowano kluczowe działania niezbędne do utrzymania przewagi konkurencyjnej USA w zakresie informatyki kwantowej oraz zmniejszenia ryzyka implikowanego rozwojem komputerów kwantowych dla bezpieczeństwa cybernetycznego, ekonomicznego i narodowego Stanów Zjednoczonych[13]. Jak wynika z treści memorandum, komputer kwantowy o wystarczającym rozmiarze i zaawansowaniu technologicznym, zdefiniowany jako ,,kryptoanalitycznie istotny komputer kwantowy", będzie w stanie złamać większość kryptografii klucza publicznego używanej w systemach cyfrowych w Stanach Zjednoczonych i na świecie, co rodzi konieczność wdrożenia efektywnych działań związanych z przejściem na kryptografię odporną na złamanie w drodze przetwarzania kwantowego oraz migracji danych do systemów odpornych na kwanty, tak aby w jak największym rozmiarze zniwelować niebezpieczeństwo związane z naruszeniem klasycznych metod szyfrowania.

W dobie transformacji technologicznej nie wystarczy zatem dalsze wydłużanie pseudolosowego klucza szyfrującego w celu zwiększenia mocy kryptograficznej klasycznych protokołów szyfrowania, lecz konieczna staje się strategiczna zmiana podejścia do kryptografii[14]. Odpowiedzią na powyższe wyzwanie może być wykorzystanie technologii kwantowej do szyfrowania informacji w taki sposób, aby była ona odporna na rozszyfrowanie przez algorytmy kwantowe. Podążanie za wymogami bezpieczeństwa spowoduje w przyszłości odejście od pseudolosowych generatorów kluczy szyfrujących opartych na faktoryzacji liczb całkowitych na rzecz w pełni losowych kluczy szyfrujących dostarczanych przez generatory kwantowe[15]. Jak wynika z powyższego, rola obliczeń kwantowych w kryptografii i cyberbezpieczeństwie może być postrzegana dualistycznie. Z jednej strony, algorytmy kwantowe mogą zostać wykorzystane do łamania protokołów szyfrujących

[13] Treść Memorandum dostępna na stronie internetowej Białego Domu: https://www.congress.gov/bill/117th-congress/house-bill/7535/text#:~:text=(4)%20The%20rapid%20progress%20of%20quantum%20computing%20suggests%20the%20potential.

[14] Zob. R. Bieda, D. Skrodzka-Kwietniak, *Jak technologia kwantowa…*, s. 406.

[15] Ibidem.

opartych na metodach konwencjonalnych (algorytmy niekwantowe) przez redukcję złożoności obliczeniowej problemów, z drugiej zaś – technologia kwantowa może okazać się remedium na gasnącą moc kryptograficzną metod opartych na asymetrycznych algorytmach kryptograficznych z kluczem publicznym RSA.

Nie możemy jednak oczekiwać, że rozwój kryptografii kwantowej rozwiąże w sposób uniwersalny wszystkie problemy skoncentrowane wokół bezpieczeństwa i integralności danych w dobie czwartej rewolucji przemysłowej. Musimy przy tym uświadomić sobie, iż postęp technologiczny w dziedzinie kryptografii oraz komunikacji kwantowej niesie za sobą w sposób nieunikniony niepożądane skutki, takie jak pogłębianie nierówności, wykluczenie, fragmentaryzacja globalnego Internetu i brak dostępu do informacji. Obliczenia kwantowe należą do technologii, które wymagają znacznych inwestycji w infrastrukturę badawczą oraz zasoby, takie jak energia, wiedza oraz wysoko wykwalifikowana kadra specjalistów. Nie wszystkie państwa i organizacje są w stanie w sposób jednolity wdrożyć rozwiązania oparte na tej technologii, co prowadzi do postępującej polaryzacji oraz pogłębiania przepaści technologicznej. Rodzi to wyzwania zorientowane na zniwelowanie nierówności i stworzenie odpowiednich warunków dla sprawiedliwej dystrybucji korzyści, jakie niesie ze sobą technologia kwantowa. Ma to szczególne znaczenie w odniesieniu do państw i grup interesariuszy o niewystarczających zasobach, które narażone są na wykluczenie i ,,kwantowe ubóstwo". W obliczu powyższych zagrożeń dopilnowanie, aby inżynieria kwantowa nie stała się narzędziem dominacji technologicznej skupionym wyłącznie w rękach wąskiej grupy uprzywilejowanych państw i korporacji z dostępem do infrastruktury badawczej oraz ze środkami na inwestycje kwantowe (zaawansowanej technologicznie ,,globalnej Północy"), powinno stać się imperatywem moralnym kształtującym warunki brzegowe dla rozwoju technologii[16]. Organizacje takie jak ONZ czy OECD powinny podjąć interwencję w celu opracowania globalnych standardów dotyczących rozwoju technologii kwantowej, aby zapewnić zrównoważony i etyczny postęp.

Co więcej, komercyjne zastosowanie rozwiązań opartych na komunikacji kwantowej może również ujawnić zupełnie nowe kategorie

[16] W doktrynie prawa pojawiła się koncepcja tzw. imperatywu kwantowego, którego istotą jest zapewnienie, aby rozwój komputerów kwantowych nie tworzył ani nie pogłębiał nierówności, nie podważał autonomii jednostek, a także nie odbywał się bez konsultacji z kwantowymi interesariuszami. Zob. V. Jeutner, op. cit.

zagrożeń, wynikające z nadmiernego poziomu zabezpieczenia komunikacji i ochrony danych, tzn. takiego poziomu zabezpieczenia, który przewyższa aktualne potrzeby i standardy. Rozumiany w ten sposób nadmiar prywatności w komunikacji kwantowej stawia szereg wyzwań legislacyjnych, które wymagają zrównoważonego podejścia, uwzględniającego zarówno poszanowanie prawa do prywatności, jak i względy bezpieczeństwa publicznego oraz efektywność operacyjną systemów komunikacyjnych, w tym zapewnienie możliwości monitorowania i skutecznego prowadzenia audytu tych systemów.

Przewidując dalszy rozwój technologii opartej na wykorzystaniu unikalnych właściwości kwantowych do przekazywania informacji zapisanych w stanach fizycznych obiektów kwantowych, można spodziewać się powstania kwantowych systemów kryptograficznych, które w perspektywie czasu doprowadzą do tworzenia nieprzeniknionych kanałów komunikacyjnych. Zaawansowane techniki komunikacji kwantowej, w tym kwantowe klucze dystrybucji (QKD), nie mogą zostać złamane przez algorytmy kwantowe, co znacząco utrudni organom ścigania monitorowanie aktywności przestępczej. Systemy komunikacji z kwantową dystrybucją klucza mogą być wykorzystane przez zorganizowane grupy przestępcze do planowania i koordynowania działań bez ryzyka wykrycia, co może prowadzić do wzrostu przestępczości zorganizowanej, w tym handlu narkotykami, cyberprzestępczości i aktów terroryzmu. Szeroko zakrojona możliwość komunikacji, oferująca niespotykany dotąd poziom bezpieczeństwa, zwiększa efektywność takich organizacji, co stawia nowe kategorie wyzwań przed organami ścigania. Wraz z rozwojem komunikacji kwantowej mogą również powstać zupełnie nowatorskie metody oszustw, oparte na bardziej wyrafinowanych technikach phishingowych, wykorzystujących sztuczną inteligencję i zwiększoną moc przetwarzania danych do generowania przekonujących komunikatów, manipulacji i deepfake'ów.

Opisane wyzwania otwierają drogę do rozważań na temat koncepcji prawa do prywatności oraz poszukiwania odpowiedniej równowagi między prywatnością a bezpieczeństwem w świecie postkwantowym[17]. Podejmowanie ewentualnych działań legislacyjnych w obszarze komunikacji kwantowej powinno uwzględniać zasadę proporcjonalności, mając na względzie ochronę obywateli bez naruszenia fundamentalnego

[17] Problematyka relacji między bezpieczeństwem a prywatnością w świecie postkwantowym jest poruszana w artykule L.M. Possati, *Ethics of Quantum Computing: An Outline*, „Philosophy & Technology" 2023, nr 36(48), https://doi.org/10.1007/s13347–023–00651–6 (dostęp: 19 VIII 2024).

wymiaru ich praw, które powinny być chronione bez względu na kontekst technologiczny. Ograniczenie prywatności na rzecz bezpieczeństwa wymaga starannego wyważenia interesów jednostki oraz dobra publicznego, z uwzględnieniem dyrektywy, w myśl której ochrona autonomii jednostki powinna być wartością nadrzędną.

4. Dylematy prawne związane z rozwojem technologii kwantowej

Żeby zapobiec niemożliwej do zniwelowania dysproporcji w rozwoju technologii kwantowej na początkowym etapie jej wdrożenia, postuluje się, aby organizacje i państwa, które są właścicielami komputerów kwantowych, dobrowolnie podzieliły się technologią, zapewniając innym państwom i podmiotom pewien dostęp do swojej infrastruktury za pośrednictwem usług świadczonych w chmurze. Celem tego działania byłoby przynajmniej częściowe łagodzenie efektu nierównomiernej alokacji korzyści uzyskiwanych z technologii kwantowej. W perspektywie miałoby to stanowić narzędzie pozwalające na zbudowanie zróżnicowanej i inkluzywnej społeczności kwantowej[18].

Z drugiej jednak strony technologia kwantowa ma potencjał do szerokiego jej wykorzystania nie tylko w przemyśle cywilnym, ale także do celów militarnych (zaliczana jest do tzw. technologii podwójnego zastosowania – TPZ, ang. *Dual-use goods*). Z tego względu coraz głośniej wybrzmiewa potrzeba objęcia wskazanej technologii ścisłą kontrolą handlu i eksportu, a także zbudowania skutecznych narzędzi mapowania technologii, identyfikacji i zarządzania ryzykiem kwantowym[19]. Aktem prawnym, który ustanawia system kontroli eksportu produktów i technologii podwójnego zastosowania na terenie Unii Europejskiej, jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2021/821 z dnia 20 maja 2021 r., ustanawiające unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania[20].

[18] Jako przykład takiego dostępu można wskazać platformę internetową IBM Quantum Platform (wcześniej znaną jako IBM Quantum Experience), umożliwiającą publiczny dostęp do opartych na chmurze usług obliczeń kwantowych świadczonych przez IBM.

[19] Problematyka ta podejmowana jest m.in. w publikacji M. Kop, op. cit.

[20] Zob. w wersji przekształconej – Dz.Urz. UE L z 2021 r., Nr 206, dalej: Rozporządzenie 2021/821. Na szczeblu krajowym zastosowanie znajdują przepisy Ustawy z dnia 29 XI 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu

Definicja legalna towarów podwójnego zastosowania przyjęta na gruncie polskiej ustawy referuje wprost do przepisów unijnych. Zgodnie z art. 2 pkt 1 Rozporządzenia 2021/821, „produkty podwójnego zastosowania" oznaczają produkty, włącznie z oprogramowaniem i technologią, które mogą być stosowane zarówno w celach cywilnych, jak i wojskowych oraz obejmują produkty, które mogą być wykorzystane do projektowania, rozwijania, produkcji lub stosowania broni jądrowej, chemicznej lub biologicznej bądź środków jej przenoszenia, w tym wszystkie produkty, które mogą być użyte zarówno w zastosowaniach niewybuchowych, jak i w jakikolwiek sposób do wspomagania wytwarzania broni jądrowej lub innych urządzeń do wybuchu jądrowego. Wśród towarów zakwalifikowanych w przepisach Rozporządzenia 2021/821 jako towary podwójnego zastosowania wymienione zostały m.in. urządzenia i oprogramowania realizujące funkcje kryptograficzne, w tym algorytmy asymetryczne określane jako odporne na komputery kwantowe lub postkwantowe, a także zaprojektowane lub zmodyfikowane do wykorzystania kryptografii kwantowej. W przyszłości katalog ten z pewnością będzie ulegał stopniowemu rozbudowaniu, a to z uwagi na potencjał zastosowania technologii kwantowej w przemyśle militarnym oraz ryzyko jej wykorzystania do wewnętrznych represji, a także do prowadzenia niejawnego nadzoru osób fizycznych poprzez monitorowanie, pobieranie, gromadzenie lub analizowanie danych, w tym danych biometrycznych (cyberinwigilacji). Przepisy Rozporządzenia 2021/821 przewidują wprost, że mechanizmy kontroli eksportu obejmują także przekazywanie oprogramowania i technologii podwójnego zastosowania za pomocą środków komunikacji elektronicznej, faksu lub telefonu do miejsc przeznaczenia poza obszarem celnym Unii, a ponadto wskazują na potrzebę zbudowania instrumentów pozwalających na stosowanie zharmonizowanej wykładni przepisów w odniesieniu do niektórych rodzajów przekazywania, takich jak przekazywanie danych do chmury. Dążenie do wypełnienia luki technologicznej w krajach rozwijających się poprzez transfer i adaptację innowacji powinno w założeniu prowadzić do wzrostu parytetu technologicznego, jednakże mechanizmy dystrybucji technologii kwantowej powinny uwzględniać instrumenty minimalizujące ryzyko wykorzystania technologii przez niepowołanych użytkowników końcowych. Wymaga to opracowania

strategicznym dla bezpieczeństwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. 2000 Nr 119, poz. 1250).

na szczeblu międzynarodowym odpowiednich regulacji dotyczących określenia celów dostępu do technologii kwantowej, które powinny pozostawać zgodne z Celami Zrównoważonego Rozwoju ONZ (ang. *Sustainable Development Goals* – SDGs)[21]. Kluczową kwestią pozostaje opracowanie zasad i wytycznych, na podstawie których państwa i korporacje z dostępem do technologii kwantowej będą mogły dzielić się technologią z państwami i interesariuszami słabiej rozwiniętymi w taki sposób, aby wyeliminować ryzyko jej wykorzystania z uszczerbkiem dla wolności i praw człowieka, a także ryzyko negatywnych implikacji w stosunkach geopolitycznych.

Monopol na wiedzę w dziedzinie technologii kwantowej skupiony w rękach nielicznych korporacji i instytucji badawczych może prowadzić do nierównowagi sił w stosunku do rządów krajowych (organów regulacyjnych)[22], a także do skutków o potencjale antykonkurencyjnym. Instrumentem prawnym wywierającym szeroki wpływ na transfer nowej technologii i przeciwdziałanie jej nadmiernej koncentracji, w myśl zasady ,,zwycięzca bierze wszystko", jest niewątpliwie podejmowanie inicjatyw prawodawczych w celu ograniczenia zakresu przedmiotowego i czasowego praw własności intelektualnej, w tym praw z patentów. W społeczności kwantowej wyrażono potrzebę ustanowienia przepisów regulujących tworzenie i dystrybucję własności intelektualnej w sposób generujący dostęp do technologii kwantowej dla instytucji publicznych i obywateli[23].

Technologia kwantowa i jej komponenty mogą być przedmiotem różnych praw własności intelektualnej, m.in. oprogramowanie (formalne wyrażenie kodu źródłowego) jest uważane za dzieło i jako takie podlega ochronie wynikającej z przepisów o prawie autorskim, z kolei komponenty sprzętowe, takie jak: pamięć kwantowa, interfejs kwantowo-klasyczny, kwantowe urządzenia interferencyjne, dekodery, silniki kompilatorów, kwantowe układy scalone, bloki kwantowe, procesory kwantowe, kwantowy blok wykonawczy, z zastrzeżeniem, że ich działanie oparte jest na rozwiązaniach o charakterze technicznym, które

[21] Quantum Computing Governance Principles, World Economic Forum, styczeń 2022 r., s. 17 – zbiór zasad opracowany w ramach wielostronnej inicjatywy Governance Workstream of the World Economic Forum's Quantum Computing Network, mającej na celu stworzenie ram zarządzania umożliwiających odpowiedzialne projektowanie i wdrażanie obliczeń kwantowych. Zob. https://www.weforum.org/publications/quantum-computing-governance-principles (dostęp: 9 VIII 2024).

[22] Ibidem.

[23] Ibidem.

są nowe, posiadają odpowiedni poziom wynalazczy i nadają się do przemysłowego zastosowania, są objęte ochroną patentową. Do ochrony patentowej nie kwalifikują się natomiast kategorie takie jak teorie naukowe i prawa mechaniki kwantowej, jak również metody matematyczne, które na mocy art. 28 ust. 1 pkt 1 Ustawy z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej zostały wyłączone z definicji legalnej wynalazku. Zasadniczo każdy komponent komputera kwantowego może ponadto zawierać stale odnawialne znaki towarowe, a wygląd komputera kwantowego, jego marka i projekt funkcjonalny mogą być chronione przez prawa do wzoru, prawa do nazwy handlowej itp.[24] Klamrą domykającą system ochrony jest tajemnica handlowa i tajemnica przedsiębiorstwa. Ten rodzaj ochrony powstaje automatycznie (nie wymaga rejestracji) i jest nieograniczony w czasie, tzn. trwa, dopóki technologia będąca przedmiotem tajemnicy nie zostanie niezależnie odkryta lub ujawniona publicznie przez dotychczasowego właściciela. Dodatkowym jej atutem jest możliwość objęcia ochroną projektów oprogramowania, kodów i algorytmów. W doktrynie wskazuje się, że niepewność co do zdolności patentowej kwantowych systemów obliczeniowych oraz nielimitowany czas trwania tajemnicy handlowej mogą uczynić z niej bardzo atrakcyjne narzędzie ochrony własności intelektualnej obejmującej technologię kwantową, w tym kwantowe aplikacje obliczeniowe[25].

Ochrona wynikająca z przepisów prawa własności intelektualnej z jednej strony ma na celu stymulowanie innowacji poprzez zachęcanie wynalazców do ujawnienia, produkowania i wprowadzania na rynek swoich wynalazków z perspektywą zwrotu nakładów poniesionych na inwestycje. Z drugiej jednak strony nadmierne mnożenie praw wyłącznych może prowadzić do antykonkurencyjnych skutków o przewidywanie negatywnym wpływie na innowacyjność, a także na uczciwą dystrybucję i sprawiedliwy dostęp do technologii[26]. W dobie transformacji przemysłowej napędzanej zdobyczami technologii kwantowej stajemy w obliczu pilnej potrzeby dokonania przeglądu obowiązujących źródeł prawa własności intelektualnej, które w wielu obszarach

[24] M. Kop, M. Aboy, T. Minssen, *Intellectual Property in Quantum Computing and Market Power: A Theoretical Discussion and Empirical Analysis*, „Journal of Intellectual Property Law & Practice" 2022, nr 17(8), s. 613–628, https://doi.org/10.1093/jiplp/jpac060 (dostęp: 19 VIII 2024).

[25] Ibidem.

[26] Ibidem.

przewidują rozwiązania anachroniczne i nieprzystające do zmieniającej się dynamicznie rzeczywistości. Przykładem takich nieadekwatnych rozwiązań mogą być zbyt długie okresy ochrony własności intelektualnej, nieprzystające do wykładniczego tempa innowacji. Część środowiska naukowego opowiada się wprost za złagodzeniem ochrony wynikającej z praw wyłącznych, ponieważ – jak uzasadnia – aktualnie przepisy prawa przewidują tak szeroko zakreślony wachlarz praw ochronnych, że odpowiednie ich wykorzystanie może skutkować nieograniczonym w czasie trwaniem globalnych wyłącznych praw do eksploatacji[27]. Postulują oni wprowadzenie krótszych okresów ochrony własności intelektualnej, wynoszących od 3 do maksymalnie 10 lat dla dzieł, a także wynalazków opartych na technologii kwantowej i sztucznej inteligencji oraz wprowadzenie instytucji obowiązkowej licencji lub licencji ustawowej o stałej cenie, co ma przyczynić się do pewności prawa, wspierania konkurencji i uczciwego transferu wiedzy, a w perspektywie tworzyć dobrze zorganizowany i zrównoważony rynek technologii kwantowej sprzyjający dalszemu jej rozwojowi[28]. Dokonanie zmian w prawie na poziomie krajowym oraz międzynarodowym powinno zostać poprzedzone szeroką debatą publiczną, budowaniem świadomości kwantowej[29] i wymaga odpowiedniego wyważenia przeciwstawnych interesów poszczególnych grup interesariuszy. Z jednej strony należy uwzględnić interes twórców oraz właścicieli technologii kwantowej w dążeniu do uzyskania możliwie jak najszerszej ochrony przed naruszeniem ich własności intelektualnej, z drugiej zaś – szeroko pojęty interes społeczny wynikający z potrzeby demokratyzacji dostępu do zdobyczy nowych technologii. Z uwagi na ramy niniejszego artykułu, którego zasadniczym celem jest zidentyfikowanie potencjalnych wyzwań prawnych, jakie niesie ze sobą rozwój i komercjalizacja technologii kwantowej, tematyka możliwych kierunków zmian w prawie własności intelektualnej w dobie postkwantowej nie będzie szeroko omawiana. Niewątpliwe

[27] Ibidem.

[28] Ibidem.

[29] Prowadzenie dyskursu bez elementarnej wiedzy na temat zastosowania technologii kwantowych i ich potencjalnego wpływu na życie społeczne, gospodarcze oraz szeroko pojęte bezpieczeństwo jest niemożliwe, na co zwracają uwagę etycy prawa i współtwórcy Quantum Computing Governance Principles, wskazując z jednej strony na potrzebę zidentyfikowania kluczowych grup interesariuszy zaangażowanych lub dotkniętych transformacją kwantową, z drugiej – na budowanie odpowiedniej świadomości, wiedzy i kompetencji kwantowych w społeczeństwie. Zob. Quantum Computing Governance Principles, World Economic Forum styczeń 2022 r., s. 22–25.

należy jednak stwierdzić, że obecne regulacje prawne w tej dziedzinie nie zostały skrojone dla technologii czwartej rewolucji przemysłowej i wymagają interwencji ustawodawcy.

5. Przetwarzanie danych osobowych w dobie postkwantowej

Możliwości oferowane przez technologię kwantową prawdopodobnie zmienią krajobraz przetwarzania danych osobowych. Wzrastające ryzyko złamania przez algorytmy kwantowe klasycznych standardów szyfrowania aktualizuje pytania o adekwatność środków technicznych i prawnych stosowanych przez przedsiębiorstwa i instytucje w celu zapewnienia zgodności z przepisami dotyczącymi ochrony danych osobowych (RODO[30]) oraz w kontekście cyberbezpieczeństwa (przestrzeganie dyrektywy NIS1[31], NIS2[32] i Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa). Przyjmując założenie o neutralności technologicznej i podejście oparte na analizie ryzyka, można przypuszczać, że unijne przepisy regulujące kwestie przetwarzania danych osobowych oraz cyberbezpieczeństwa w zasadniczych obszarach zachowają aktualność w dobie technologii kwantowej. Nie można przy tym całkowicie wykluczyć, że unikalne cechy obliczeń kwantowych zmaterializują potrzebę wprowadzenia pewnych zmian w obowiązującym prawie. Poważnym wyzwaniem będzie natomiast dostosowanie wymogów technicznych i organizacyjnych do postępującej technologii kwantowej, co spowoduje konieczność stałego monitorowania przez podmioty przetwarzające dane osobowe rozwoju tej technologii i uwzględniania stanu jej zaawansowania przy cyklicznej ocenie ryzyka, tak aby w odpowiednim momencie dokonać identyfikacji zagrożeń

[30] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 IV 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne Rozporządzenie o Ochronie Danych) (Dz.Urz. UE L z 2016 r., Nr 119, s. 1), dalej „RODO".

[31] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 VII 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L z 2016 r., Nr 194, s. 1).

[32] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 XII 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Tekst mający znaczenie dla EOG) (Dz.Urz. UE L z 2022 r., Nr 33, s. 80).

i wdrożyć odpowiednie środki zaradcze[33]. Sprostanie powyższym wyzwaniom będzie wymagało ustanowienia solidnych protokołów monitorowania oraz skutecznych mechanizmów reagowania na incydenty w celu wykrywania potencjalnych zagrożeń dla bezpieczeństwa danych, w tym danych genomicznych i biometrycznych, a także opracowania polityk regulacyjnych w celu zapewnienia ochrony danych osobowych w erze kwantowej. Będzie to wiązało się z koniecznością poniesienia przez przedsiębiorstwa i instytucje znacznych nakładów finansowych na wdrożenie rozwiązań zapewniających bezpieczeństwo i integralność danych, w tym rozwiązań z zakresu kryptografii postkwantowej (kryptografii odpornej na zagrożenia związane z rozwojem komputerów kwantowych)[34], a także wzmocnienia technik anonimizacji zbiorów danych w celu ich zabezpieczenia przed atakami komputerów kwantowych. Osiągnięcie powyższych założeń nie będzie możliwe bez podniesienia świadomości społecznej na temat zagrożeń dla danych osobowych i dla cyberbezpieczeństwa, jakie wiążą się z rozwojem kryptoanalizy kwantowej, a także bez budowania kompetencji kwantowych i ścisłej interdyscyplinarnej współpracy z ekspertami w tej dziedzinie technologii.

Problemem, który nabiera szczególnego znaczenia w kontekście przetwarzania danych osobowych zgodnie z przepisami RODO, jest przestrzeganie obowiązków wynikających z zasady przejrzystości. Zasada przejrzystości w zakresie ochrony danych jest jedną z naczelnych zasad przetwarzania danych osobowych statuowanych w art. 5 ust. 1 RODO. Celem tej zasady jest zapewnienie zaufania do procesów, które mają wpływ na obywatela, dzięki umożliwieniu mu zrozumienia tych procesów, a w razie konieczności również zgłoszenia wobec nich

[33] R. Bieda, D. Skrodzka-Kwietniak, *Kierunki prac legislacyjnych oraz wybrane wyzwania prawne dotyczące technologii kwantowej*, w: *Metaświat. Prawne i techniczne aspekty…*, s. 398–399.

[34] Jednym z obiecujących podejść jest kwantowa dystrybucja kluczy (Quantum Key Distribution, QKD), która wykorzystuje zasady mechaniki kwantowej do ustanowienia bezpiecznych kanałów komunikacji i dystrybucji kluczy szyfrujących. W QKD klucze szyfrujące są zakodowane w stanach kwantowych, takich jak polaryzacja lub spin poszczególnych fotonów. Każda próba przechwycenia lub zmierzenia tych stanów kwantowych wprowadziłaby wykrywalne zakłócenia, ostrzegając komunikujące się strony o obecności podsłuchiwacza. Ta właściwość mechaniki kwantowej zapewnia, że klucze szyfrowania pozostają bezpieczne, nawet w obliczu mocy obliczeniowej komputerów kwantowych. Powyższa tematyka została szeroko omówiona w: J. Mielczarek,*Rozpinanie kwantowej sieci*, 24 XII 2022, https://jakubmielczarek.com/2020/12/24/rozpinanie-kwantowej-sieci (dostęp: 30 VII 2024).

sprzeciwu. Stanowi ona również urzeczywistnienie i emanację zasady rzetelności w odniesieniu do przetwarzania danych osobowych, o których mowa w art. 8 Karty praw podstawowych Unii Europejskiej[35]. Z zasady rozliczalności statuowanej w art. 5 ust. 2 RODO wynika z kolei, że administrator zobowiązany jest do wykazania przed ewentualną kontrolą, że dane osobowe przetwarzane są w sposób przejrzysty dla osoby, której dane te dotyczą. Problem jednak w tym, że algorytmy używane do zautomatyzowanego podejmowania decyzji i uczenia maszynowego nie zostały zaprojektowane z myślą o klarowności dla osób je stosujących. Ich działanie jest nieintuicyjne, przy czym o ile w przypadku algorytmów klasycznych (działających w prostym systemie 0–1) brak przejrzystości algorytmów ma charakter *stricte* epistemiczny, o tyle w przypadku algorytmów kwantowych nieprzejrzystość ich działanie nie wynika wyłącznie z ludzkich ograniczeń poznawczych, ale także z samej istoty fundamentalnych praw mechaniki kwantowej[36]. W kontekście powyższego należy postawić pytanie, jak daleko będzie sięgał obowiązek zapewnienia przejrzystości przetwarzania danych osobowych w ekosystemie sztucznej inteligencji wzmocnionej technologią kwantową i czy urzeczywistnienie zasady transparentności wyrażonej w RODO będzie w ogóle możliwe w rzeczywistości postkwantowej.

6. Określenie ram dla przyszłej legislacji

Biorąc pod uwagę poziom gotowości technologicznej komputerów kwantowych w kontekście możliwości ich komercyjnego użycia, wydawać mogłoby się, że mamy jeszcze dostatecznie dużo czasu na to, aby

[35] Grupa Robocza art. 29, Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679, przyjęte dnia 29 XI 2017 r., ostatnio zmienione i przyjęte w dniu 11 IV 2018 r., zatwierdzone przez EROD, dostępne na: https://ec.europa.eu/newsroom/article29/items/622227/en, s. 4–5. Grupa Robocza została powołana na podstawie art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

[36] Zob. L.M. Possati, op. cit.: ,,W kwantowym systemie obliczeniowym możliwe stany są ontologicznie i epistemologicznie nieokreślone […]. W rzeczywistości stan układu kwantowego jest nieokreślony w tym sensie, że jedyną rzeczą, jaką możemy o nim wiedzieć, jest zbiór prawdopodobieństw i ich interpretacji, tak zwanych amplitud prawdopodobieństwa. Bit kwantowy, czyli kubit, ma dwa stany kwantowe analogiczne do klasycznych stanów binarnych. Podczas gdy kubit może znajdować się w dowolnym stanie, może również istnieć w superpozycji między tymi dwoma stanami" – tłum. D.G.L.

martwić się o etyczne i prawne implikacje ich rozwoju, jednak w obliczu potencjalnych ryzyk i transformacyjnego wpływu omawianej technologii pojawia się coraz więcej głosów nawołujących do wprowadzenia już dziś mechanizmów kontrolnych i regulacyjnych, które mogą przeciwdziałać zidentyfikowanym zagrożeniom oraz zachęcać do zrównoważonych innowacji[37]. Z kolei przeciwnicy podejmowania inicjatywy prawodawczej w celu zakreślenia ram dla dalszego rozwoju technologii, która nie osiągnęła jeszcze wystarczającego poziomu dojrzałości technologicznej i biznesowej, wskazują na ryzyko przeregulowania i tamujący wpływ mechanizmów kontrolnych oraz regulacyjnych na innowacyjność. Ze względu na ogromną potencjalną moc obliczeń kwantowych, które w połączeniu ze sztuczną inteligencją mogą uzasadniać jej zakwalifikowanie do kategorii AI wysokiego ryzyka[38], zdecydowanie trzeba się opowiedzieć za podejściem regulacyjnym, wskazując na konieczność stworzenia odgórnego mandatu dla rozwoju etycznie odpowiedzialnej technologii, która będzie osadzona w wartościach demokratycznych i podporządkowana zostanie zasadzie ochrony szeroko rozumianego dobrostanu człowieka w styczności z nowymi technologiami.

Technologia kwantowa, podobnie jak ma to zastosowanie w odniesieniu do systemów AI, powinna zostać poporządkowana nadrzędnym

[37] Na konieczność objęcia technologii kwantowych regulacją prawną i solidnymi podstawami etycznymi zwraca uwagę M. Kop, op. cit.

[38] Przesłanki zakwalifikowania systemów sztucznej inteligencji do systemów AI wysokiego ryzyka zostały określone w art. 6 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 VI 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (Akt w sprawie sztucznej inteligencji) (Dz.Urz. UE L z 2024 r., Nr 1689, s. 1). Zgodnie z przywołaną regulacją, system AI uznaje się za system wysokiego ryzyka, jeżeli spełnione zostaną następujące warunki: (a) system AI jest przeznaczony do wykorzystania jako związany z bezpieczeństwem element produktu objętego unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I lub sam system AI jest takim produktem; (b) produkt, którego związanym z bezpieczeństwem elementem jest zgodnie z lit. a) system AI, lub sam system AI jako produkt podlegają – na podstawie unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku I – ocenie zgodności przez stronę trzecią w związku z wprowadzeniem tego produktu do obrotu lub oddaniem go do użytku. Oprócz systemów AI wysokiego ryzyka, o których mowa w art. 6 ust. 1 Rozporządzenia, za systemy wysokiego ryzyka uznaje się systemy AI, o których mowa w załączniku III. Do systemów AI wysokiego ryzyka co do zasady zalicza się zatem takie systemy, które w sposób znaczący mogą zagrażać zdrowiu, bezpieczeństwu, prawom podstawowym, środowisku, demokracji lub praworządności.

zasadom o wymiarze uniwersalnym: poszanowania ludzkiej godności i kontroli przez człowieka, technicznej solidności i bezpieczeństwa, poszanowania prywatności i ochrony danych, transparentności (urzeczywistnienie tej zasady w klasycznym jej rozumieniu będzie szczególnie utrudnione, o ile w ogóle możliwe), niedyskryminacji, sprawiedliwości i promowania różnorodności, funkcjonowania dla osiągnięcia dobrobytu społecznego oraz poszanowania środowiska naturalnego.

Przewodnia i nadzorcza rola człowieka oznacza, że systemy oparte na wykorzystaniu nowych technologii, takich jak AI lub komputery kwantowe, powinny być rozwijane i stosowane jako narzędzia służące ludziom, szanujące godność ludzką i autonomię osobistą oraz działające w sposób, który może być odpowiednio kontrolowany i nadzorowany przez człowieka. Solidność techniczna i bezpieczeństwo oznaczają wykorzystanie technologii w taki sposób, aby okazały się wytrzymałe w przypadku wystąpienia problemów oraz odporne na próby zmiany ich przeznaczenia lub skuteczności działania, co pozwoli zapobiec bezprawnemu wykorzystaniu przez osoby trzecie i zminimalizować niezamierzone szkody. Wymaga to opracowania mechanizmów standaryzacji, certyfikacji i kontroli technologii kwantowej[39]. Ochrona prywatności i zarządzanie danymi stawiają wymaganie, żeby systemy te rozwijały się zgodnie z przepisami dotyczącymi prywatności i ochrony danych, przy czym przetwarzanie danych powinno spełniać wysokie standardy pod względem jakości i integralności. Przejrzystość oznacza z kolei, że technologia *quantum computing* oraz systemy oparte na jej synergii z AI powinny być projektowane i wykorzystywane w sposób umożliwiający odpowiednią identyfikowalność, informując ludzi o tym, że komunikują się z systemem AI wzmocnionym technologią kwantową, a także o zdolnościach i ograniczeniach tej technologii, w tym o działaniu komputerów kwantowych w oparciu o algorytm probabilistyczny (co oznacza, że poprawność wyniku działania takiego algorytmu nigdy nie jest całkowicie pewna). Niepewność immanentnie związana z technologią obliczeń kwantowych uzasadnia ponadto stawianie wymogu informowania o podjętych działaniach w celu wykluczenia błędów oraz o poziomie pewności obliczeń[40]. Różnorodność, niedyskryminacja i sprawiedliwość oznaczają natomiast, że technologia kwantowa

[39] W literaturze przedmiotu wskazuje się, że certyfikacja nie powinna być przyznawana przez podmioty prywatne o celach komercyjnych, ale przez niezależne publiczne organy nadzoru. Tak: M. Kop, op. cit.

[40] R. Bieda, D. Skrodzka-Kwietniak, *Kierunki prac legislacyjnych…*, s. 401.

powinna być rozwijana i stosowana w sposób, który angażuje różne podmioty i propaguje równy dostęp, równouprawnienie płci i różnorodność kulturową, jednocześnie unikając dyskryminujących skutków i niesprawiedliwej stronniczości, zakazanych przez prawo międzynarodowe lub prawo krajowe. Urzeczywistnienie zasad funkcjonowania dla osiągnięcia dobrobytu społecznego oraz poszanowania środowiska naturalnego oznacza, że nowa technologia kwantowa powinna być rozwijana w sposób zrównoważony, przyjazny dla środowiska i przynoszący korzyści wszystkim ludziom, jednocześnie przewidując długoterminowy wpływ tych systemów na osoby fizyczne, społeczeństwo i demokrację.

Mimo iż nie znamy jeszcze wszystkich możliwych zastosowań technologii kwantowej, w pewnym stopniu możemy przewidzieć rezultaty postępu naukowego w tej dziedzinie. Odpowiednio wczesne podjęcie inicjatywy w zakresie zaprojektowania ram prawnych dla rozwijającej się technologii stwarza szanse, że wartości aksjologiczne leżące u podstaw takich regulacji będą wywierały modulacyjny wpływ na kierunki transformacji i wdrożenia tej technologii, a nie tylko działały wstecz. Warto zatem już dziś podjąć wysiłek nadania tym wartościom solidnych podstaw demokratycznych, tak aby uniknąć problemów etycznych, a przynajmniej łagodzić skutki problemów, jakie wyłoniły się na gruncie niekontrolowanej ekspansji sztucznej inteligencji. Wyzwaniem jest oczywiście zaprojektowanie ram etyczno-prawnych dla technologii, która obecnie ma niezdefiniowane możliwości zastosowania. W doktrynie wyrażono postulaty, aby posiłkować się w tym zakresie istniejącymi już zasadami i regulacjami dotyczącymi sztucznej inteligencji[41].

Powiązanie etyki oraz aksjologii prawa leżącej u podstaw tworzenia norm regulujących zastosowanie technologii kwantowej z istniejącymi już zasadami i wymogami dotyczącymi sztucznej inteligencji wydaje się dlatego logiczne i uzasadnione, że zazwyczaj komponenty systemów opartych na technologii kwantowej są wyposażone w sztuczną inteligencję[42]. Ponadto, jak zostało to już wyżej zasygnalizowane, technologia kwantowa wykazuje bardzo ścisły związek ze sztuczną inteligencją

[41] M. Kop, op. cit.

[42] Tytułem przykładu można wskazać, że interfejs oprogramowania binarnego i kwantowego wykorzystuje uczenie maszynowe i technologię sieci neuronowych. Więcej informacji na temat platform sprzętowych do obliczeń kwantowych i standaryzacji interfejsów programowania aplikacji (API), zob. M. Vizard, *QCI Rises to the Quantum Computing Portability Challenge*, VentureBeat, 17 II 2021, https://venturebeat.com/2021/02/17/qci-rises-to-the-quantum-computing-portability-challenge/ (dostęp: 13 VIII 2024).

i może znacząco oddziaływać na kierunki rozwoju AI, poprawiając szybkość, efektywność i precyzję działania systemów bazujących na sztucznej inteligencji. Połączenie sztucznej inteligencji i obliczeń kwantowych w przyszłości doprowadzi do powstania kwantowej sztucznej inteligencji (Quantum AI) o wykładniczo zwiększonej mocy obliczeniowej, a tym samym o zdolności przetwarzania zbiorów danych na niespotykaną dotąd skalę. W doktrynie prawa wskazuje się, że przyszłe rozwiązania technologiczne oparte na połączeniu komputerów kwantowych oraz sztucznej inteligencji będą miały charakter hybrydowy i dlatego podstawowe zasady, jakim zostanie poddana technologia kwantowa, powinny być metodycznie powiązane i osadzone w istniejących już regulacjach dotyczących AI[43].

W odniesieniu do komputerów kwantowych można zatem racjonalnie oczekiwać wprowadzenia regulacji opartej na analizie ryzyka, na kształt regulacji odnoszącej się do technologii opartej na działaniu sztucznej inteligencji, z uwzględnieniem kategorii systemów zakazanych oraz kategorii wysokiego ryzyka, jak również wprowadzenia rozwiązań mających zapewnić nadzór człowieka. Wprowadzenie listy praktyk zakazanych w zakresie kwantowej sztucznej inteligencji obejmować może m.in. takie systemy technologiczne, jak: systemy kategoryzacji biometrycznej wykorzystujące wrażliwe cechy, systemy punktacji społecznej, rozpoznawanie emocji w miejscu pracy i instytucjach edukacyjnych oraz systemy, które manipulują ludzkim zachowaniem w celu obejścia woli człowieka. W doktrynie sformułowano również postulaty, aby systemy oparte na synergistycznym działaniu sztucznej inteligencji i technologii kwantowej zaliczyć *ipso iure* do systemów sztucznej inteligencji wysokiego ryzyka, ze wszystkimi skutkami wskazanej kwalifikacji prawnej[44].

7. Kwantowa sztuczna inteligencja – problem dyskryminacji algorytmicznej i czarnej skrzynki

Wizja powstania AI z dostępem do wszystkich zasobów informacyjnych globalnego Internetu i z mocą obliczeniową komputerów kwantowych skłania do rozważań na temat etycznego wymiaru korzystania z tej technologii i wyzwań, jakie stoją przed prawem w kontekście jej właściwego

[43] M. Kop, op. cit.
[44] R. Bieda, D. Skrodzka-Kwietniak, *Kierunki prac legislacyjnych…*, s. 401.

uregulowania. Oprócz wielu korzyści zastosowania Quantum AI, należy założyć również jej wykorzystanie w sposób nieetyczny. Technologia ta dostarczać może nowych, potężnych narzędzi do praktyk manipulacji, represji, wyzysku i kontroli społecznej, a ponadto doprowadzić do zwiększenia ryzyka naruszeń prywatności i dyskryminacji algorytmicznej. Na pozór mogłoby wydawać się, że decyzja podjęta przez algorytm, bez udziału człowieka, powinna być dostatecznie zobiektywizowana i pozbawiona podejścia opartego na stereotypach. W istocie jednak działanie algorytmów bardzo często prowadzi do dyskryminacji, co wynika w szczególności z uprzedzeń społecznych, które są immanentnie wpisane w dane wejściowych algorytmu. W literaturze przedmiotu podkreśla się, że podejmowanie stronniczych i dyskryminacyjnych decyzji jest jednym z największych wyzwań sztucznej inteligencji[45]. Działanie algorytmu jest bowiem niczym innym jak ekstrapolacją danych historycznych, na których operuje algorytm.

Terminy „stronniczość algorytmiczna" i „dyskryminacja algorytmiczna" używane są do opisania szeregu problemów etycznych związanych z działaniem i wynikami algorytmów. Pojęcie „stronniczość" jest przy tym bardziej pojemne znaczeniowo niż dyskryminacja, gdyż odnosi się do systematycznego błędu dowolnego rodzaju w wyniku operacji algorytmicznych, a nie tylko błędów „niesprawiedliwych". Może zatem obejmować błędy o charakterze statystycznym, poznawczym, społecznym, strukturalnym lub instytucjonalnym[46]. W porównaniu z tradycyjnymi formami dyskryminacji dyskryminacja algorytmiczna jest bardziej nieintuicyjna, a przez to trudna do wykrycia i udowodnienia[47]. Brak świadomości istniejącego ryzyka dyskryminacji zwiększa błędne przekonanie o neutralności aksjologicznej algorytmów.

Dla lepszego zrozumienia zjawiska dyskryminacji algorytmicznej warto wyjaśnić pokrótce, w jaki sposób działają systemy uczenia maszynowego i jakie determinanty wpływają na algorytmiczne podejmowanie decyzji przez AI. Zasadniczym celem uczenia maszynowego jest praktyczne zastosowanie sztucznej inteligencji do tworzenia

[45] M. Otto, *Dyskryminacja algorytmiczna w zatrudnieniu. Zarys problemu*, „Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2022, nr 29(2), s. 145–160.

[46] European Commission, Directorate-General for Justice and Consumers, J. Gerards, R. Xenidis, *Algorithmic Discrimination in Europe: Challenges and Opportunities for Gender Equality and Non-discrimination Law*, Luxembourg 2021, https://data.europa.eu/doi/10.2838/544956 (dostęp: 15 VIII 2024).

[47] M. Otto, op. cit.

zautomatyzowanego systemu, który posiada umiejętność doskonalenia się na bazie doświadczenia (czyli danych wejściowych) i nabywania na tej podstawie nowej wiedzy. W uproszczeniu można stwierdzić, że proces ten polega na znalezieniu pewnej matrycy w dostarczonych danych, która następnie zostanie zaimplementowana do udzielenia odpowiedzi na pytanie o nieznany zbiór danych. Działanie uczenia maszynowego jest uzależnione od dwóch podstawowych elementów: zestawu reguł zwanych algorytmami (instrukcji matematycznych, których celem jest rozwiązywanie problemów, odpowiadanie na pytania lub wykonywanie określonych zadań) oraz danych, czyli zestawu zmiennych wejściowych[48]. Algorytmy bazują na danych wejściowych, które zostały zdefiniowane przez człowieka. W każdym algorytmie zakodowane są określone wartości, stanowiące emanację wartości, z którymi w sposób bardziej lub mniej uświadomiony identyfikuje się projektodawca algorytmu, w konsekwencji i same algorytmy nie są obiektywne oraz aksjologicznie neutralne[49]. Bazując na danych uwarunkowanych kulturowo, w których odwzorowane zostały społeczne stereotypy, uprzedzenia i nierówności strukturalne, algorytmy powielają i utrwalają te schematy.

Algorytmy uczenia maszynowego i głębokiego uczenia się są zaprojektowane i wyszkolone m.in. w celu analizowania danych w określony sposób, śledzenia korelacji i wyszukiwania odpowiednich wzorców, a także przewidywania przyszłych zachowań (predykcji). Ich operowanie na dużych zbiorach danych (*Big Data*) polega m.in. na sortowaniu, grupowaniu i kategoryzowaniu danych poprzez wyszukiwanie podobieństw i różnic. Kultura algorytmów opiera się zatem na redukcji, uproszczeniu i budowaniu modeli[50]. Szerokie rozpowszechnienie algorytmów zautomatyzowanego podejmowania decyzji lub wspierających podejmowanie decyzji przez człowieka przyczynia się do zwiększenia szybkości i wydajności procesów decyzyjnych. Szczególne cechy algorytmicznego procesu decyzyjnego mogą jednak powodować rozprzestrzenianie się dyskryminacji algorytmicznej.

Problem nietransparentności działania algorytmów sztucznej inteligencji, w tym głębokiego uczenia się opartych na sieciach neuronowych, określany jest problemem czarnej skrzynki. Odnosi się on do trudności

[48] Ibidem.

[49] Ł. Iwasiński, W. Furman, *Jak być świadomym użytkownikiem algorytmów? O potrzebie rozwijania kompetencji algorytmicznych*, „Zagadnienia Informacji Naukowej – Studia Informacyjne" 2022, nr 60(2), 25–43, https://doi.org/10.36702/zin.910 (dostęp: 19 VIII 2024).

[50] M. Szpunar, *Kultura algorytmów*, „Zarządzanie w Kulturze" 2018, nr 19(1), s. 1–9.

w interpretacji sposobu, w jaki algorytmy dochodzą do konkretnych wniosków lub decyzji. Znamy dane wejściowe i znamy wynik działań. Nie wiemy jednak, w jaki sposób sztuczna inteligencja uzyskała określony rezultat. Problem czarnej skrzynki ma również głębokie następstwa etyczne. Nieprzejrzystość w procesach decyzyjnych AI może prowadzić do trudno uchwytnych uprzedzeń i dyskryminacji. Te z kolei mają poważne konsekwencje, zwłaszcza gdy wpływają na newralgiczne obszary życia jednostki ludzkiej, takie jak: dostęp do systemu usług zdrowotnych, ocena zdolności finansowej i dostęp do usług bankowych, ocena w procesie rekrutacji i w procesie zatrudnienia, dostęp do edukacji czy wymiar sprawiedliwości. W obliczu rzeczywistości, w której nie jesteśmy w stanie zrozumieć i zrekonstruować pełnego przebiegu procesu decyzyjnego AI, nie możemy również dokonać jego walidacji, co utrudnia identyfikację i eliminowanie ewentualnych błędów, w tym utrwalonych i powielanych przez AI uprzedzeń. Wysoki stopień złożoności technologicznej procesów przetwarzania danych przez AI utrudnia również odwołanie się od rozstrzygnięć podjętych przez algorytmy zautomatyzowanego podejmowania decyzji, co w przyszłości może mieć szczególne znaczenie w przypadku ich potencjalnego zastosowania w obszarach wymiaru sprawiedliwości.

W jaki sposób technologia kwantowa może przyczynić się do spotęgowania problemu dyskryminacji algorytmicznej i efektu czarnej skrzynki? Przede wszystkim przez skokowe zwiększenie tempa uczenia maszynowego i procesów decyzyjnych przeprowadzanych za pomocą algorytmów sztucznej inteligencji wzmocnionych technologią kwantową. Antycypując dalszy dynamiczny postęp w dziedzinie obliczeń kwantowych i coraz bliższą perspektywę nastania Quantum AI, można zaryzykować stwierdzenie, że w przyszłości będziemy mierzyli się z rzeczywistością, w której technologia ta przestanie być podatna na nadzór człowieka, nie wspominając już o zapewnieniu przejrzystości działania algorytmów kwantowych.

W przeciwieństwie do klasycznej sztucznej inteligencji, jej kwantowa gałąź koduje informacje w rzeczywistych stanach kwantowo-fizycznych. Tym, co wyróżnia Quntum AI od klasycznej sztucznej inteligencji, jest element niepewności typu kwantowego (obiektywnego)[51], który zostaje

[51] Element niepewności typu kwantowego odnosi się do zasady nieoznaczoności Heisenberga, która jest fundamentalnym aspektem mechaniki kwantowej. Zasada ta stanowi, że nie można jednocześnie z dokładnością określić pewnych par wielkości fizycznych, takich jak położenie i pęd cząstki. W kontekście obiektywności oznacza to,

wprowadzony do algorytmów skonstruowanych według reguł mechaniki kwantowej. W klasycznym cyfrowym systemie obliczeniowym istnieją tylko dwa możliwe stany – 0 i 1. Istotą obliczeń kwantowych jest natomiast stan kwantowy, reprezentowany przez podstawową jednostkę informacji określaną jako bit kwantowy (kubit), który może znajdować się jednocześnie w obydwu wskazanych wyżej stanach oraz w superpozycji między tymi stanami. Z punktu widzenia ontologicznego stan układu kwantowego jest zatem stanem nieokreślonym[52].

Unikatowe cechy technologii kwantowej, w szczególności zaś niektóre z kluczowych właściwości cząstek kwantowych, które leżą u podstaw zasad mechaniki kwantowej, takich jak superpozycja, splątanie oraz twierdzenie o nieklonowaniu[53], podobnie jak niedeterministyczne zachowania algorytmów kwantowych, sprawiają, że zinterpretowanie procesów decyzyjnych i wykrywanie błędów w oprogramowaniu komputerów kwantowych jest wielokrotnie trudniejsze niż w przypadku klasycznych programów komputerów. Dodatkowo, ze względu na potencjalną interferencję pomiaru ze stanami kwantowymi, obserwacja wewnętrznego zachowania programów kwantowych staje się właściwie niemożliwa. Pomiar powoduje zakłócenie stanu kwantowego i niszczy stan mierzonego układu w sposób nieodwracalny. Oznacza to, że nie można odtworzyć stanu sprzed pomiaru na podstawie wyniku pomiaru, natomiast stan po pomiarze jest ściśle wyznaczony przez ten wynik. Dlatego też kwestia przejrzystości działania algorytmów kwantowych jest znacznie bardziej złożona niż programów opartych na binarnym kodowaniu liczb. W przeciwieństwie do klasycznych algorytmów, algorytmy kwantowe nie mają bezpośrednich odpowiedników w świecie makroskopowym, co utrudnia ich interpretację i zrozumienie. Dodatkowym czynnikiem, który komplikuje analizę algorytmów kwantowych,

że wyniki pomiarów w mechanice kwantowej są z natury probabilistyczne i nie można ich przewidzieć z absolutną pewnością. Ta niepewność nie wynika z ograniczeń narzędzi pomiarowych, ale jest wbudowana w samą naturę rzeczywistości kwantowej. Zob. A. Łukasik, *Mechanika kwantowa a problem obiektywności*, „Zagadnienia Naukoznawstwa" 2015, nr 2(204), https://journals.pan.pl/Content/94148/mainfile.pdf (dostęp: 19 VIII 2024).

[52] Stan układu kwantowego jest uważany za nieokreślony ontologicznie z kilku powodów, w tym superpozycji stanów, zjawiska interferencji, splątania kwantowego, nielokalności oraz nieokreśloności pomiaru.

[53] Fundamentalne twierdzenie w mechanice kwantowej, zgodnie z którym niemożliwe jest stworzenie identycznej kopii dowolnego nieznanego stanu kwantowego. Twierdzenie to wynika z liniowości mechaniki kwantowej, która zabrania tworzenia urządzenia, które może idealnie skopiować dowolny stan kwantowy.

jest ich podatność na błędy i zakłócenia. Nawet niewielkie zakłócenia mogą prowadzić do zmian w wynikach, co utrudnia śledzenie i zrozumienie procesu decyzyjnego[54].

W odniesieniu do sztucznej inteligencji wzmocnionej technologią obliczeń kwantowych możemy zatem mówić o zupełnie nowej odsłonie problemu nieprzejrzystości algorytmów, który ma wymiar nie tylko epistemiczny, lecz także ontologiczny, co oznacza, że nie tylko jest determinowany ograniczeniami poznawczymi umysłu ludzkiego, ale przede wszystkim wynika z fundamentalnej natury kwantów i niedefiniowalności świata opisywanego przez prawa mechaniki kwantowej[55].

W świetle powyższego można postawić tezę, że klasyczne podejście do zasady przejrzystości i postulaty tworzenia algorytmów, które będą przedstawiały w sposób klarowny ścieżkę dojścia do wyniku końcowego, wpisujące się w szeroki nurt tworzenia etycznej i wyjaśnialnej sztucznej inteligencji, nie będą możliwe do zrealizowania w odniesieniu do Quantum AI. W dobie czwartej rewolucji przemysłowej stoimy zatem przed wyzwaniem wdrożenia nowych instrumentów testowania, certyfikacji i kontroli algorytmów (takich jak narzędzia do analizy i wizualizacji wyników kwantowych algorytmów), które będą adekwatne do specyfiki Quantum AI i zapewnią etyczną poprawność działania systemów zautomatyzowanego podejmowania decyzji opartych na obliczeniach kwantowych. Może to spowodować odejście od rysującej się koncepcji prawa podmiotowego określanego jako prawo do wyjaśnienia działania algorytmów (ang. *right to explanation*), którego treścią miałoby być w założeniu zagwarantowanie każdemu dostępu do wiedzy o czynnikach, logice i technikach działania algorytmów kwantowych na rzecz bardziej uniwersalnego i pojemnego konglomeratu uprawnień, składających się na treść prawa do rzetelności działania systemów opartych na algorytmach kwantowych.

Podsumowanie

Technologia kwantowa wkracza na scenę z ogromnym potencjałem, jednak wiążą się z nią złożone wyzwania prawne, które wymagają

[54] *Obliczenia kwantowe: 8 ważnych aspektów przyszłości obliczeń*, Julien Florkin, https://julienflorkin.com/pl/technologia/informatyka-kwantowa/informatyka-kwantowa (dostęp: 19 VIII 2024).

[55] Zagadnienie nowej formy nieprzejrzystości algorytmów kwantowych jest szeroko omawiane w: L.M. Possati, op. cit.

szczegółowej analizy oraz interdyscyplinarnego podejścia. Na krawędzi rewolucji technologicznej stajemy w obliczu zagadnień dotyczących m.in. ochrony danych osobowych i prywatności, bezpieczeństwa narodowego, niwelowania przepaści technologicznej oraz etyki zastosowań kwantowych. Należy również rozważyć kwestię odpowiedzialności prawnej za decyzje podejmowane przez sztuczną inteligencję operującą na systemach kwantowych. Tradycyjne podejście oparte na założeniu, że algorytmy działają zgodnie z przewidywalnymi regułami, nie znajduje tu zastosowania, co może prowadzić do trudności w dochodzeniu roszczeń lub przypisywaniu winy w sytuacjach spornych. Kwestia odpowiedzialności wiąże się także z problemem transparentności. Algorytmy operujące na zasadach kwantowych działają w sposób nieprzejrzysty, właściwie nieosiągalny dla ludzkiego rozumienia. W związku z tym stajemy przed pytaniem o interakcję między użytkownikami i algorytmami. Jak można zapewnić, że jednostki posiadają na tyle wystarczającą wiedzę o działaniu tych algorytmów, aby mogły świadomie wyrazić zgodę na ich wykorzystanie? W obliczu nakreślonych wyzwań konieczne staje się wypracowanie nowych norm prawnych i etycznych, które w sposób adekwatny odpowiedzą na specyfikę działania sztucznej inteligencji wzmocnionej technologią kwantową. Ta adaptacyjna rewizja norm prawnych powinna odbywać się w kontekście partycypacji wielostronnej, w której głos mają nie tylko prawnicy, lecz także inżynierowie, etycy oraz przedstawiciele organizacji społecznych.

Przewodnia i nadzorcza rola człowieka jest kluczowa, aby technologia ta służyła ludziom, szanując ich godność i autonomię osobistą. Solidność techniczna i bezpieczeństwo wymagają opracowania mechanizmów standaryzacji, certyfikacji i kontroli, które zapobiegną bezprawnemu wykorzystaniu technologii oraz zminimalizują niezamierzone szkody. Współpraca międzynarodowa w zakresie standaryzacji i certyfikacji może pomóc w ustanowieniu globalnych norm, które będą chronić prawa jednostki na całym świecie. Wreszcie, edukacja i świadomość społeczna na temat technologii kwantowej są kluczowe, aby społeczeństwo mogło aktywnie uczestniczyć w debacie na temat jej etycznego i prawnego wykorzystania. W kontekście dynamicznego rozwoju technologii kwantowej konieczne jest proaktywne podejście do legislacji, tak aby przepisy prawa chroniły autonomię jednostki, nie stając się jednocześnie balastem dla innowacji.

BIBLIOGRAFIA

Bieda R., Skrodzka-Kwietniak D., *Jak technologia kwantowa wpłynie na bezpieczeństwo informatyczne – rozmowa z gen. Włodzimierzem Nowakiem*, w: *Metaświat. Prawne i techniczne aspekty przełomowych technologii*, pod red. R. Biedy, Z. Okonia, Warszawa 2023, s. 403–410.

Bieda R., Skrodzka-Kwietniak D., *Kierunki prac legislacyjnych oraz wybrane wyzwania prawne dotyczące technologii kwantowej*, w: *Metaświat. Prawne i techniczne aspekty przełomowych technologii*, pod red. R. Biedy, Z. Okonia, Warszawa 2023, s. 387–402.

Bova F., Goldfarb A., Melko R.G., *Quantum Economic Advantage*, „Management Science" 2022, nr 69(2), s. 1116–1126.

Dalton A., *Quantum Technology Comes of Age*, „Science" 2019, nr 366(6464), s. 898–900.

European Commission, Directorate-General for Justice and Consumers, J. Gerards, R. Xenidis, *Algorithmic Discrimination in Europe: Challenges and Opportunities for gender Gender Equality and Non-discrimination Law*, Luxembourg 2021, https://data.europa.eu/doi/10.2838/544956 (dostęp: 15 VIII 2024).

Iwasiński Ł., Furman W., *Jak być świadomym użytkownikiem algorytmów? O potrzebie rozwijania kompetencji algorytmicznych*, „Zagadnienia Informacji Naukowej – Studia Informacyjne" 2023, nr 60(2), s. 25–43.

Jeutner V., *The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers*, „Morals & Machines" 2021, nr 1(1), s. 52–59, https://ssrn.com/abstract=3820003 (dostęp: 19 VIII 2024).

Kaku M., *Kwantowa dominacja. Jak komputery kwantowe odmienią nasz świat*, tłum. B. Bieniok, E.L. Łokas, Warszawa 2023.

Kop M., *Establishing a Legal-Ethical Framework for Quantum Technology*, „Yale Journal of Law & Technology. The Record" 2021, https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology (dostęp: 13 VIII 2024).

Kop M., Aboy M., Minssen T., *Intellectual Property in Quantum Computing and Market Power: A Theoretical Discussion and Empirical Analysis*, „Journal of Intellectual Property Law & Practice" 2022, nr 17(8), s. 613–628, https://doi.org/10.1093/jiplp/jpac060 (dostęp: 19 VIII 2024).

Lewis J.A., Wood G., *Quantum Technology: Applications and Implications*, Center for Strategic and International Studies 2023, https://www.csis.org/analysis/quantum-technology-applications-and-implications (dostęp: 19 VIII 2024).

Łukasik A., *Mechanika kwantowa a problem obiektywności*, „Zagadnienia Naukoznawstwa" 2015, nr 2(204), s. 137–145, https://journals.pan.pl/Content/94148/mainfile.pdf (dostęp: 19 VIII 2024).

Mielczarek J., *Rozpinanie kwantowej sieci*, 24 XII 2022, https://jakubmielczarek.com/2020/12/24/rozpinanie-kwantowej-sieci, (dostęp: 30 VII 2024).

Otto M., *Dyskryminacja algorytmiczna w zatrudnieniu. Zarys problemu*, „Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2022, nr 29(2), s. 145–160.

Possati L.M., *Ethics of Quantum Computing: An Outline*, „Philosophy & Technology" 2023, nr 36(48), https://doi.org/10.1007/s13347–023–00651–6 (dostęp: 19 VIII 2024).

Szpunar M., *Kultura algorytmów*, „Zarządzanie w Kulturze" 2018, nr 19(1), s. 1–10.
Vizard M., *QCI Rises to the Quantum Computing Portability Challenge*, VentureBeat, 17 II 2021, https://venturebeat.com/2021/02/17/qci-rises-to-the-quantum-computing-portability-challenge/ (dostęp: 13 VIII 2024).