Teka Komisji Prawniczej PAN Oddział w Lublinie, t. XII, 2019, nr 2, s. 53–71
https://doi.org/10.32084/tekapr.2019.12.2-4

ROZWÓJ NOWOCZESNYCH TECHNOLOGII W KONTEKŚCIE PROCESU STANOWIENIA PRAWA NA PRZYKŁADZIE STRATEGII AI

Dr hab. Katarzyna Chałubińska–Jentkiewicz, prof. ASzWoj

Katedra Prawa Cyberbezpieczeństwa i Nowych Technologii
Instytut Prawa Akademii Sztuki Wojennej
e-mail: kasiachalubinska@gmail.com; https://orcid.org/0000-0003-0188-5704

Streszczenie. Nowoczesne technologie stanowią obecnie fundament wzrostu gospodarczego i są zasobem o krytycznym znaczeniu, na którym opierają się wszystkie sektory gospodarki. Popularność zdobyły płatności elektroniczne, chmury obliczeniowe oraz komunikacja typu robot – robot. Jednym z istotnych pytań dotyczących wpływu nowoczesnych technologii na proces stanowienia prawa jest pytanie o granice ich rozwoju i oddziaływania. Z jednej strony nowoczesne technologie determinują rozwój, jednak mogą być ograniczane przez prawa, np. przez prawo własności przemysłowej. Z drugiej strony innowacje przyczyniają się do ingerencji w te prawa, utrudniają ich ochronę. W każdej z tych sytuacji mamy do czynienia ze zjawiskiem zagrożenia dla poczucia bezpieczeństwa jednostki i obywatela.

Słowa kluczowe: strategia, regulacja, stosowanie prawa i stanowienie prawa, prawo nowych technologii, nowoczesne technologie, sztuczna inteligencja

Analizując kwestie bezpośrednio nawiązujące do regulacji w obszarze nowych technologii[1], należy podkreślić, iż niezbędny wydaje się podział obszarów regulacji według określonych kategorii. Wynikiem tego zabiegu może być ustalenie zakresu merytorycznego regulacji i dookreślenie podstaw definicji pojęcia prawa nowych technologii. Podkreślić należy, iż w warunkach prawnych, w których często przytacza się definicje słownikowe – pojęcie „technologia" – według takiej definicji oznacza przetwarzanie w sposób celowy i ekonomiczny dóbr naturalnych w dobra użyteczne (produkty), a także wiedzę o tym procesie [Szymczak 1999, 452], natomiast samo słowo „technologia" pochodzi od greckich słów *téchnẽ* – sztuka, rzemiosło oraz *lógos* – słowo, nauka. Pojęcie to ma aspekt szerszy i odnosi się do wszelkich form świadomego przekształcania rzeczywistości [Zubik 2008, 37]. Nowe technologie w potocznym rozumieniu kojarzą się z innowacją, z nowymi rozwiązaniami

[1] „Nowoczesne" czy „nowe" w przypadku technologii stosuje się zamiennie, jednak bardziej właściwe jest użycie pojęcia „technik" niż „technologii", które dotyczą samego procesu tworzenia.

techniki oraz ich zastosowaniem w życiu codziennym. Jednak dzisiaj nowe technologie stają się niezbędnym elementem funkcjonowania człowieka. Podstawowym zagadnieniem staje się kwestia regulacji prawnej samego działania nowoczesnych technologii, jak również regulacji prawnej działania w warunkach nowoczesnych technologii. Problematyka podjęta w artykule dotyczy aspektów procesu tworzenia prawa na etapie ustalania polityk odnoszących się do nowych technologii, które swoje odzwierciedlenie znajdują w strategiach krajowych. W pierwszej kolejności bowiem następuje wyznaczanie celów regulacji, dopiero w następnej dochodzi do procesu stanowienia prawa. Przykładem opracowywania polityk w zakresie przyszłych regulacji jest zagadnienie sztucznej inteligencji.

Nowoczesne technologie wciąż stanowią przedmiot dyskusji społecznej i politycznej, a ostatecznie regulacji, w aspekcie działań ustawodawczych. Przenikające się obszary regulacji i konwergencja prawna powodują, że nowe technologie jako nieodłączny atrybut działań ludzkich, praktycznie w każdej dziedzinie życia, wymagają szczególnych uwarunkowań prawnych. Proces ten następuje w okresie rozwoju technologicznego, rozwoju techniki cyfrowej przy jednoczesnym wzroście potrzeb konsumenckich i globalizacji. Rozwój nowych technologii, jak i związane z nimi procesy zmian społecznych, wymagają nowego podejścia regulacyjnego, a także redefinicji celów interesu publicznego oraz obowiązków państwa w procesie regulacji tych obszarów, które dotykają kwestii kluczowych związanych z funkcjonowaniem jednostki. Procesy konwergencji dotychczas różnie pojmowanych obszarów regulacyjnych przyczyniają się do powstania szczególnego rodzaju konfliktu w obszarze ustaleń co do zakresu i poziomu nowych regulacji. Mówiąc o zmianach, jakie niosą nowe technologie musimy pamiętać, że zjawisko to wymaga podejścia interdyscyplinarnego, łączącego wiedzę i punkty widzenia specjalistów, ekspertów w dziedzinach ekonomii, socjologii, technologii, mediów, politologii, psychologii i kultury oraz nauk o bezpieczeństwie. Współczesne warunki życia w dużym stopniu zależą od stanu funkcjonującej technologii informacyjno-komunikacyjnych w danym państwie. Obecnie jesteśmy świadkami radykalnych zmian w sposobie funkcjonowania społeczeństwa oraz gospodarki światowej, będących rezultatem upowszechnienia się nowatorskich rozwiązań teleinformatycznych. Wraz z rozwojem technologii cyfrowej oraz zmianami społecznymi, związanymi także z procesem tworzenia się tzw. demokracji cyfrowej, pojawiły się nowe obszary działania człowieka określane powszechnie jako środowisko sieci teleinformatycznej, szerzej rozumiane jako cyberprzestrzeń. Mają one wpływ na wszystkie aspekty życia. Odnosi się to także do relacji społecznych, gospodarki, relacji państwo-jednostka oraz realizacji praw podstawowych jednostki. Otwarta i wolna cyberprzestrzeń pozwala na wymianę kultur i doświadczeń między państwami, społecznościami i obywatelami, umożliwiając interakcję oraz wymianę informacji, a w konsekwencji

wiedzy, doświadczeń, a także technologii. Można zatem powiedzieć, że brak regulacji zapewnia wymianę technologii, a w konsekwencji rozwój innowacji. Podstawą aksjologiczną wspierającą wymianę jest wolność słowa i wolność komunikowania się. Jednak to tylko wycinek bardzo złożonego zagadnienia, jakim jest rozwój nowoczesnych technologii w kontekście procesu stanowienia prawa. We współczesnych warunkach funkcjonowania jednostki w cyberprzestrzeni wydaje się konieczne podjęcie nowych działań w zakresie ustalenia norm, a uprzednio zasad i wartości, które są standardem w świecie rzeczywistym. Wolność w środowisku internetowym wymaga również bezpieczeństwa i ochrony. Cyberprzestrzeń należy chronić przed incydentami, szkodliwymi działaniami i nadużyciami, przy czym znaczącą rolę w zapewnieniu wolnej i bezpiecznej cyberprzestrzeni odgrywają organy władzy publicznej, a te z kolei w polskim porządku prawnym zgodnie z art. 7 Konstytucji RP[2], działają na podstawie i w granicach prawa. Tym samym wszelkie zadania i kompetencje związane z zapewnieniem porządku i bezpieczeństwa publicznego w cyberprzestrzeni wymagają uprzedniego ustalenia norm kompetencyjnych. Można tu wymienić szereg zadań związanych z zapewnieniem dostępu i otwartości, poszanowaniem i ochroną praw podstawowych w Internecie oraz utrzymaniem niezawodności i interoperacyjności Internetu. Zmiana technologii komunikowania zasadniczo zmieniła zasady funkcjonowania jednostek i całych społeczności. Proces digitalizacji i rozwój sieci powodują, że pojawia się coraz więcej zupełnie nowych uczestników rynku. Powstają platformy multimedialne świadczące usługi drogą elektroniczną, które wymagają zastosowania nowoczesnych rozwiązań technologicznych, a w które najczęściej inwestuje sektor prywatny. Nowoczesne technologie i związane z nimi usługi mogą być katalizatorem rozwoju gospodarczego, zwiększać konkurencyjność gospodarki, tworzyć nowe miejsca pracy, sprzyjać rozwojowi demokracji, regionów, wspomagać nauczanie, ochronę zdrowia, dostęp do dóbr kultury. Są one również niezbędne dla zachowania gotowości obronnej, bezpieczeństwa państwa i obywateli oraz porządku publicznego.

1. POLITYKA REGULACYJNA W WARUNKACH NOWYCH TECHNOLOGII

W efekcie procesu rozwoju nowoczesnych technologii i poszerzania zakresu ich oddziaływania na funkcjonowanie jednostki, ale także instytucji – państwa – nowa polityka regulacyjna wydaje się być niezbędna. Obecnie jesteśmy świadkami radykalnych zmian w sposobie funkcjonowania społeczeństw oraz gospodarki światowej, co stanowi oczywisty rezultat upowszechnienia

[2] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. Nr 78, poz. 483 z późn. zm.

się nowatorskich rozwiązań teleinformatycznych. W wyniku procesu cyfryzacji i poszerzania zakresu usług komunikacji elektronicznej nowa polityka regulacyjna stała się niezbędna. Państwo musi stopniowo ograniczyć zakres sprawowania funkcji zarządczej na rzecz kształtowania strategii i mechanizmów rozwoju, standaryzacji i mediacji. Dotychczasowe metody sprawowania władzy i zarządzania państwem będą po prostu nieskuteczne w społeczeństwie, w którym głównym produktem stała się informacja. Nowoczesne technologie stały się przyczyną konwergencji administracji (*administrative convergence*), czyli procesu polegającego na tworzeniu nowych, wspólnych rozwiązań administracyjnych w miejsce tradycyjnych odrębności administracyjnych [Chałubińska–Jentkiewicz 2016, 21]. Te właśnie obszary podlegają definiowaniu najczęściej na poziomie Unii Europejskiej, a podział ich wyznaczają nowe zagrożenia dla bezpieczeństwa. Jednym z kluczowych celów regulacyjnych w procesie stanowienia prawa jest zapewnienie cyberbezpieczeństwa, które wymaga działań związanych z zachowaniem dostępności i integralności sieci i infrastruktury, poufności zawartych w nich informacji. Zapewnienie bezpieczeństwa staje się podstawowym celem określenia zasad polityki w obszarze cyberprzestrzeni w poszczególnych państwach członkowskich UE oraz na arenie międzynarodowej. Wyznacznikiem tych zasad jest ochrona podstawowych wartości, które muszą mieć taki sam stopień ochrony w cyberprzestrzeni, jak w świecie fizycznym. Dlatego też przepisy i normy mające zastosowanie w innych obszarach naszego codziennego życia muszą mieć również zastosowanie w odniesieniu do cyberprzestrzeni. Skuteczność ochrony bezpieczeństwa w cyberprzestrzeni uzależnia się przede wszystkim od stopnia ochrony praw podstawowych, wolności wypowiedzi, ochrony danych osobowych oraz prawa do prywatności. Zapewnienie cyberbezpieczeństwa może stać się skuteczne tylko wtedy, kiedy zostanie oparte na podstawowych prawach i wolnościach, które stanowią europejski system ochrony praw człowieka od początku zbudowany na założeniu, że istnieje pewien wspólny wszystkim państwom europejskim katalog wartości oraz że państwa te powinny osiągnąć wspólny standard ochrony praw jednostki. Należy tu zauważyć, że cyberbezpieczeństwo ma znaczenie nie tylko dla zapewnienia praw podstawowych jednostki w zakresie ochrony jej prywatności czy prawa własności w sieci. Zagadnienie to odnosi się także do funkcjonowania państwa, zwłaszcza w kontekście realizacji celów interesu publicznego.

Ochrona praw i wolności podstawowych wyznacza granice każdego procesu stanowienia prawa, podyktowanego także względami rozwoju nowoczesnych technologii. Jednocześnie, należy mieć na uwadze fakt, iż ograniczenia tych praw i wolności mogą być podyktowane względami ochrony bezpieczeństwa, ponieważ zapewnienie bezpieczeństwa stanowi jeden z celów interesu ogólnego na poziomie Unii i interesu publicznego na poziomie krajowym państwa członkowskiego. Należy przy tym zauważyć, iż granice

interesu ogólnego w ujęciu europejskim są wyznaczane przez cele interesu publicznego w ujęciu narodowym państw członkowskich. Oczywiście potrzeba takiej ochrony odnosi się raczej do konkretnych treści interesu publicznego [Chałubińska–Jentkiewicz 2011, 124]. Określenie tych treści (w miarę możliwości) należy do władzy publicznej. Definiowanie celów regulacyjnych musi mieć miejsce na poziomie krajowym, podobnie jak wybór środków do ich osiągnięcia. Instrumenty, po które sięga się w sferze publicznej dla potrzeb realizacji celów dobra powszechnego muszą podlegać analizie i określonym zmianom adekwatnie do przemian społecznych związanych z rozwojem technologicznym, ale także odpowiednio do konkretnych potrzeb danego państwa, jego uwarunkowań gospodarczych i politycznych. We współczesnym państwie coraz bardziej niezbędne staje się spojrzenie strategiczne, które w warunkach dotąd nieznanych zagrożeń, związanych z rozwojem społeczeństwa sieci i gospodarki opartej na wiedzy, umożliwia jego prawidłowy rozwój. Istotnym elementem tej funkcji jest określenie prognoz na przyszłość, co wymaga szerokiej analizy złożonych uwarunkowań lokalnych i globalnych, potrzeb i interesów gospodarczych, społecznych i politycznych, a także możliwości zaspokojenia potrzeb jednostkowych. Diagnoza i strategia pozwalają na ustalenie odpowiedniej polityki regulacyjnej. Polityka regulacyjna jest ściśle związana ze strefą zarządzania. Sfera zarządzania rozwojem różni się tym od innych sfer działania administracji publicznej, że zwraca się bardziej ku przyszłości funkcjonowania państwa. Z tego też względu sfera zarządzania rozwojem jest dziś jednym z głównych założeń polityki publicznej, także w obszarze nowych technologii [Chałubińska–Jentkiewicz 2016, 66]. W ramach procesu planowania funkcja władzy publicznej polega na wyznaczaniu działań zmierzających do realizacji określonych celów, ale także redefinicji tych celów z uwzględnieniem wymogów dotyczących rozwoju nowoczesnych technologii. Dlatego tak istotne znaczenie mają strategie.

Wszystkie elementy nowoczesnych technologii, do których możemy zaliczyć oprogramowanie, usługi, bazy danych czy urządzenia, charakteryzują te same cechy, czyli szybkość (gwałtowne zmiany rynku w obszarze usług, powiększający się w dużym tempie obszar innowacji technicznej, zwłaszcza w kontekście rozwoju sieci, badań naukowych w zakresie przechowywania danych etc.); globalizacja (nowoczesne technologie umożliwiają globalną wymianę usług w czasie rzeczywistym); przedsiębiorczość (tworzenie karteli w celu wspólnego przeprowadzania badań na rzecz innowacji, partnerstwa publiczno-prywatne); partycypacja społeczna (tworzenie rozwiązań innowacyjnych przez użytkowników sieci, rozwój mediów społecznościowych, *crowdsourcing* – wymiana myśli, koncepcji przyczynia się do rozwoju technologii i innowacji); konwergencja (łączenie wielu obszarów działania człowieka). Konwergencja technologiczna powoduje, że zatracają się granice pomiędzy poszczególnymi obszarami stanowienia prawa, co nie pozwala na wyraźne

zlokalizowanie zagrożeń i ustalenie odpowiedzialności poprzez stanowienie prawa, a także dookreślenie samego reżimu prawnego. Cechy tu wskazane są uzasadnieniem zmian i transformacji pod względem tworzenia nowego systemu zarządzania, przy zastosowaniu odpowiednich instrumentów prawnych. Opierając się na tych istotnych czynnikach rozwoju nowoczesnych technologii, trzeba wskazać na potrzebę zintegrowania systemu prawnego w tym obszarze. Dlatego można mówić o systemie prawa nowoczesnych technologii, który w sposób zupełnie naturalny musi podążać za zmianami technologicznymi i towarzyszącymi im zmianami społecznymi [Chałubińska–Jentkiewicz i Karpiuk 2015, 12]. Ze względu na tempo zmian technologicznych i w konsekwencji gospodarczych system ten musi cechować się elastycznością, a rozwiązania prawne powinny zawierać standardy uniwersalne, pozwalające na ich zastosowanie w różnych warunkach i w różnych sytuacjach. Procesom tym towarzyszy potrzeba zaufania i poczucie pewności ze strony obywateli. Poczucie braku bezpieczeństwa wzmaga potrzebę stanowienia prawa w tych obszarach, które dotychczas wydawać by się mogło były wolne od wszelkiej regulacji. Wraz z rozwojem nowoczesnych technologii wzrasta liczba incydentów mogących spowodować zakłócenia w świadczeniu podstawowych usług, które uznajemy za oczywiste, takich jak np. dostawy wody, opieka zdrowotna, dostawy energii elektrycznej i usługi telefonii komórkowej. Zagrożenia mogą mieć różne źródła – w tym przestępcze, motywowane politycznie, terrorystyczne lub inicjowane przez państwo, jak również mogą być efektem klęsk żywiołowych i niezamierzonych błędów. Nasilenie szpiegostwa gospodarczego i działań inicjowanych przez państwa w cyberprzestrzeni stanowi nową kategorię zagrożeń dla władz publicznych i przedsiębiorców. W krajach spoza UE rządy mogą również nadużywać cyberprzestrzeni w celu inwigilowania i kontrolowania własnych obywateli. UE może przeciwdziałać tej sytuacji poprzez promowanie swobód, a także zapewnianie przestrzegania praw podstawowych w Internecie. Wszystkie te czynniki pomagają zrozumieć, dlaczego rządy na całym świecie zaczęły opracowywać strategie bezpieczeństwa cybernetycznego i dlaczego uważają, że kwestie związane z cyberprzestrzenią stają się coraz bardziej istotnym problemem o wymiarze międzynarodowym – również w obszarze regulacji prawnych.

2. POJĘCIE „NOWOCZESNYCH TECHNOLOGII"

Pojęcie „nowe technologie" posiadało legalne definicje określone m.in. w art. 18b ust. 2 ustawy o podatku dochodowym od osób prawnych[3] oraz

[3] Ustawa z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych, Dz. U. z 2019 r., poz. 865 z późn. zm.

art. 26c ust. 2 ustawy o podatku dochodowym od osób fizycznych[4], które powstały dla celów tych ustaw. Według powyższych przepisów za pomocą pojęcia „nowe technologie" określano wiedzę technologiczną w postaci wartości niematerialnych i prawnych, w szczególności wyniki badań i prac rozwojowych, która umożliwia wytwarzanie nowych lub udoskonalonych wyrobów lub usług i która nie jest stosowana na świecie przez okres dłuższy niż ostatnich 5 lat. Przez nabycie nowej technologii rozumiano nabycie praw do wiedzy technologicznej w drodze umowy o ich przeniesienie lub korzystanie z tych praw. W wymienionej tu ustawie ustawodawca docenił kwestie rozwoju nowych technologii poprzez zmniejszenie obciążenia podatkiem dochodowym w warunkach wprowadzania przez przedsiębiorców nowych technologii. Ustawodawca objął ulgą specyficzną kategorię wydatków ponoszonych w celu korzystania z nowych technologii, w zakresie dostępu oraz praw do wiedzy i rezultatów badań. W innym akcie normatywnym definicja ta obejmuje swoim zakresem technologię w postaci prawa własności przemysłowej lub wyników prac rozwojowych, lub wyników badań aplikacyjnych, lub nieopatentowanej wiedzy technicznej, która umożliwia wytwarzanie nowych lub znacząco ulepszonych, w stosunku do dotychczas wytwarzanych na terytorium Rzeczypospolitej Polskiej, towarów, procesów lub usług[5].

W systemie prawa europejskiego nowe technologie ze względu na swoją specyfikę zostały objęte szczególnym wyłączeniem. Przepisy składające się na rozporządzenie Komisji (UE) nr 316/2014 z dnia 21 marca 2014 r. w sprawie stosowania art. 101 ust. 3 Traktatu o funkcjonowaniu Unii Europejskiej do kategorii porozumień o transferze technologii wprowadzają podstawowy słownik pojęć związany z transferem technologii[6]. Rozporządzenie to zastąpiło wcześniejsze rozporządzenie Komisji (WE) nr 772/2004 z dnia 7 kwietnia 2004 r. w sprawie stosowania art. 81 ust. 3 Traktatu do kategorii porozumień o transferze technologii. Według rozporządzenia Komisji Europejskiej „prawa do technologii" oznaczają *know-how* oraz następujące prawa lub ich połączenie, w tym zgłoszenia lub wnioski o zarejestrowanie tych praw: patenty; wzory użytkowe; prawa do wzorów przemysłowych; topografie układów scalonych; dodatkowe świadectwa ochronne dla produktów leczniczych lub innych produktów, w odniesieniu do których można uzyskać tego rodzaju dodatkowe świadectwa ochronne; prawa do ochrony odmian roślin; oraz prawa autorskie do oprogramowania.

W wąskim ujęciu pojęcie „nowoczesne technologie" obejmuje zatem dobra niematerialne, które związane są bezpośrednio z zastosowaniem produktów

[4] Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych, Dz. U. z 2019 r., poz. 1387 z późn. zm.

[5] Ustawa z dnia 30 maja 2008 r. o niektórych formach wspierania działalności innowacyjnej, Dz. U. z 2019 r., poz. 1402, art. 2 pkt 9.

[6] Dz. U. UE L 93, 28.03.2014, s. 17–23.

będących efektem zastosowania nowych rozwiązań technicznych. Jednak zważywszy na uwarunkowania rozwoju nowych technologii, ich wpływu na życie społeczne i jednostkowe, obszaru regulacyjnego dotyczącego nowych technologii nie można ograniczać jedynie do dóbr niematerialnych. W sposób oczywisty, w związku z korzystaniem i wdrażaniem nowych technologii, będziemy mieć do czynienia z normami prawnymi, które odnosić się będą do różnych zagadnień, często rozproszonych i obejmujących zakres regulacyjny merytorycznie bardzo szeroki. Do zagadnień tego typu zaliczyć należy kwestie związane z rozwojem sztucznej inteligencji (*Artificial Intelligence*, *AI*); *machine learning*; 5G, czyli nowy standard sieci komórkowej; *Augmented Reality*, czyli rozszerzoną rzeczywistość popularyzowaną przez Google, Facebook czy Apple, która wkracza w obszar medycyny i e-commerce; *Internet of Things* (IoT), czyli konsekwencja rozwoju wszystkiego co inteligentne; *Big Data*; komputery kwantowe.

Z powyższego powodu do kwestii regulacyjnych dotyczących prawa nowych technologii zaliczyć wypada różne płaszczyzny regulacji, począwszy od zasad funkcjonowania władz publicznych, obowiązków i zadań państwa w nowych warunkach rozwojowych, dopuszczalnych granic ingerencji państwa w życie jednostki, całego społeczeństwa i jego poszczególnych grup, z jednoczesnym uwzględnieniem obszaru regulacyjnego odnoszącego się do zagadnień związanych z prawami podstawowymi i wolnościami jednostki, zarówno w relacji państwo – jednostka, jak i jednostka – jednostka. Tym samym, przywołując powyższe definicje, przyjmuję, iż prawo nowych technologii to zespół norm prawnych, które odnoszą się do obszarów niezbędnej regulacji, w sferze relacji o charakterze zarówno publicznym, jak i prywatnym, na które bezpośredni wpływ wywierają nowoczesne technologie [Chałubińska–Jentkiewicz i Karpiuk 2015, 21]. Ustalenie i charakterystyka pojęcia prawa nowych technologii jest kluczem w dookreśleniu celów regulacji nowoczesnych technologii w procesie przyszłego stanowienia prawa.

3. SZTUCZNA INTELIGENCJA W PROCESIE STANOWIENIA PRAWA

Wraz z rozwojem tzw. „nowoczesnych technologii" praktycznie w każdym obszarze życia człowieka, w szczególności w medycynie i w biotechnologii, pojawiają się problemy dotyczące etycznych i prawnych regulacji związanych z zasadami funkcjonowania komputerów i robotów. Pytania, które odnoszą się do kwestii stanowienia prawa w warunkach rozwoju nowoczesnych technologii dotyczą odpowiedzialności człowieka za działania skierowane przeciwko komputerom, przy wykorzystaniu komputerów, ale także odpowiedzialności komputerów za działania w stosunku do człowieka i innych komputerów. Prawne aspekty ochrony dotyczącej dóbr osobistych, w tym integralności ciała, wcześniej nie obejmowały ochrony sztucznej inteligencji.

S. Braman wskazuje na pewne zmiany polityki w USA, które wydają się wychodzić naprzeciw potrzebom stanowienia prawa odnośnie do sytuacji komputerów. Przykładem takiego podejścia jest amerykańska ustawa telekomunikacyjna z 1996 r., która rozróżnia politykę społeczną, czyli związaną z działaniem człowieka i politykę w działaniach komputerów [Braman 2006, 278]. Zdolność komputerów do analizy i rozwiązywania problemów, także w obszarze etyki tworzy interesujące zagadnienia dotyczące odpowiedzi na pytania co jest moralne albo co nie jest moralne, czym jest dobro, a czym jest zło, a w konsekwencji – co jest dozwolone, a co powinno być zakazane w ujęciu prawnym. Te dylematy są podstawowym elementem określającym stopień odpowiedzialności, która stanowi jeden z większych problemów prawnych w kontekście nowoczesnych technologii. Jeśli przyjmujemy, że komputery coraz bardziej są samodzielne w myśleniu i procesie decyzyjnym to czy można przyjąć, że mają one także świadomość istnienia moralności? Wydaje się, że jest to klucz do odpowiedzi na przyszłe pytania związane z odpowiedzialnością prawną za działania w cyberprzestrzeni. Sądy próbują przypisać odpowiedzialność za szkody wyrządzone ludziom przez maszyny kierowane sztuczną inteligencją. Czy sztuczna inteligencja ma osobowość prawną, czy tym samym ma zdolność do czynności prawnych? Czy komputery mogą być odpowiedzialne za swoje działania? Czy odpowiedzialność za komputer ponosi twórca lub właściciel oprogramowania czy posiadacz rzeczy? Wydaje się, że odpowiedzią na te pytania jest kwestia ustalenia posiadania osobowości prawnej. W różnych stanowiskach teoretyków prawa, jak na przykład Ugo Pagallo dowodzi się, iż powinniśmy rozróżniać zachowanie robotów jako narzędzi interakcji międzyludzkich, oraz zachowanie robotów jako podmiotów w sferze prawnej [Pagallo 2013, 79]. To jedno z kluczowych zadań ustawodawcy w najbliższym okresie rozwoju nowoczesnych technologii.

Prawna doktryna cyberodpowiedzialności będzie szczególnie istotna w obliczu zmian życia w warunkach rozwoju sztucznej inteligencji [Chałubińska–Jentkiewicz 2019, 110]. Dzisiaj też zasady odpowiedzialności określa ukształtowane, także w sferze prawa rozróżnienie między *hardware* i *software*. Potencjalne niebezpieczeństwo stwarzane przez sztucznie inteligentne maszyny zwiększa się, gdy stają się one mobilne. Projektowanie technologii czy technik sztucznej inteligencji i cyborga będzie miało istotne znaczenie w tworzeniu przyszłości, w której sztuczna inteligencja w sposób lojalny i etyczny będzie pracować dla człowieka. Oczywiście, zawsze prawo może regulować kwestie odpowiedzialności karnej czy cywilnej za niewłaściwe postępowanie, czyny zabronione, jednak dynamika rozwoju cyberprzestrzeni, sztucznej inteligencji i robotyki znacznie przewyższają możliwości prawodawców. Zaprezentowanie pewnych tendencji regulacyjnych dotyczących sztucznej inteligencji pozwala na kreację co prawda zawężonej, ale obecnej wizji rzeczywistości regulacyjnej. Sztuczna inteligencja nie doczekała się jeszcze definicji

legalnej [Hallevy 2015, 3]. W oparciu o działania AI funkcjonują m.in. programy do automatycznego tworzenia informacji, programy asystentów głosowych (Google Assistant), programy diagnostyczne stosowane w medycynie, rozpoznawania twarzy. Analizę danych i boty, czyli programy wykonujące pewne czynności w zastępstwie człowieka, wykorzystuje się już dziś w marketingu internetowym, przy geotargetowaniu, profilowaniu oraz w szeroko rozumianym *public relations*. Technologia AI może być również wykorzystywana w świadczeniu usług prawnych. Znane są zastosowania AI w informatyce prawniczej, w procesie tworzenia prawa i rozstrzygania sporów *on-line*.

Stosowanie technologii AI coraz częściej pociąga za sobą dylematy natury prawnej, a polityka regulacyjna dotycząca AI znajduje odzwierciedlenie w strategiach, które jako podstawowy element w procesie stanowienia prawa kształtują obraz przyszłych regulacji [Dervanović 2018, 209]. Zagadnienie AI i strategie regulacyjne najlepiej odzwierciedlają obecne tendencje ustawodawcze związane z rozwojem nowoczesnych technologii. Należy przy tym zauważyć, iż Wielka Brytania swoją strategię zaprezentowała w kwietniu 2018 r. Francja przyjęła swoją strategię w marcu 2018 r. i konsekwentnie ją realizuje. Niemcy stosują się do swej strategii od listopada 2018 r.

3.1. Wielka Brytania

Działania strategiczne w Wielkiej Brytanii związane ze wsparciem sztucznej inteligencji zostały określone w dokumencie dotyczącym innowacji AI w celu zwiększenia wydajności. Sama strategia odnosi się przede wszystkim do zagadnień związanych z rozwojem przemysłu, a polityka w zakresie stanowienia prawa odnośnie do AI została określona w Białej Księdze. W Strategii Przemysłowej[7] Next Generation Services podnosi się potrzebę stworzenia sieci ośrodków badań nad innowacjami oraz zaplanowanie wspólnych badań i rozwoju w celu opracowania nowych zastosowań sztucznej inteligencji i technologii opartych na danych w takich sektorach, jak m.in. prawo i ubezpieczenia. Jednym z podstawowych wyzwań dotyczących AI jest zapewnienie pewności prawnej w zakresie udostępniania i wykorzystywania danych zgodnie ze wzmocnioną ostatnio ochroną danych osobowych. W dokumentach tych podkreśla się znaczenie ustalenia uczciwych, sprawiedliwych i bezpiecznych ram udostępniania danych, współpracy z głównymi posiadaczami danych, zarówno w sektorze prywatnym, jak i publicznym, wraz ze środowiskiem nauki o danych w celu identyfikacji barier utrudniających udostępnianie danych. W polityce regulacyjnej zaznacza się, iż niektóre z najcenniejszych danych pod względem ich potencjału umożliwiającego innowacje, ulepszania usług w sektorze publicznym – nie mogą zostać otwarte, ponieważ zawierają informacje krytyczne dla państwa, prywatne lub

[7] Zob. https://www.gov.uk/government/publications/life-sciences-industrial-strategy [dostęp: 25.04.2019].

wrażliwe czy handlowe. Obejmuje to także dane, które można wykorzystać do identyfikacji osób. Celem regulacyjnym jest ustalenie pionierskich mechanizmów udostępniania danych, takich jak Data Trusts. Nowe regulacje mają zapewnić ochronę wszystkich zaangażowanych stron, ustalić określone prawa i obowiązki związane z danymi. Głównym celem strategicznym jest także ustanowienie elastycznych ram regulacyjnych zachęcających do budowania nowych modeli biznesowych. Zgodnie z Białą Księgą otoczenie regulacyjne musi ewoluować wraz z pojawieniem się nowych technologii i nowych modeli biznesowych. Jedną z przyszłych regulacji jest kwestia ram prawnych działania samochodów z własnym napędem, bez człowieka. Niezbędna jest tu aktualizacja przepisów postępowania w przypadku testowania zautomatyzowanych pojazdów, a ostatecznie przedstawienie Komisji Prawnej propozycji docelowej regulacji[8]. Jednak w strategii podkreśla się, iż integralność prawa brytyjskiego i bezstronność organizacji zawodowych pozwalają na lokalizację działań biznesowych w Wielkiej Brytanii. Nowoczesne technologie to nowe sposoby robienia interesów i nowe branże często wymagające niezawodnego systemu regulacyjnego. W przypadku autonomicznych pojazdów są to kwestie dotyczące reguł ubezpieczenia. Zdaniem brytyjskich regulatorów system regulacyjny musi odpowiadać nie tylko warunkom dzisiejszej gospodarki, ale także jej przyszłej odmiany.

3.2. Francja[9]

Francja jest jednym z 4 krajów na świecie pod względem produkcji artykułów sztucznej inteligencji na całym świecie, obok Chin, Stanów Zjednoczonych i Wielkiej Brytanii. Raport na temat sztucznej inteligencji (AI) przygotowany przez matematyka i posła Cédrica Villaniego został opublikowany 28 marca 2018 r. Wśród wielu proponowanych sposobów wsparcia rozwoju sztucznej inteligencji jest stworzenie sieci interdyscyplinarnych instytutów sztucznej inteligencji, utworzenie superkomputera zaprojektowanego specjalnie z myślą o aplikacjach sztucznej inteligencji, ponieważ te technologie, które dają maszynom ogromne możliwości analizy daleko wykraczającej poza możliwości ludzi. Ostatnie postępy w AI w wielu dziedzinach (autonomiczne samochody, rozpoznawanie obrazów, wirtualnych asystentów) i jej rosnący wpływ w centrum debaty publicznej przyczyniają się do podjęcia debaty głównie związanej z szerszą refleksją na temat problemów etycznych związanych z rozwojem sztucznej inteligencji i technologii wykorzystującej algorytmy. Prawodawca, naukowcy, przedsiębiorcy i obywatele muszą podjąć dyskusję

[8] Zob. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/ industrial-strategy-white-paper-web-ready-version.pdf [dostęp: 24.04.2019].

[9] Zob. *Stratégie nationale de recherche en intelligence artificielle*, http://www.enseignementsup-recherche.gouv.fr/cid128577/rapport-de-cedric-villani-donner-un-sens-a-l-intelligence-artificielle-ia.html [dostęp: 24.04.2019].

na temat zaistniałych, a także potencjalnych negatywnych skutków AI, które mogą wynikać z faktu, iż nie wszyscy są równi wobec algorytmów, a ich stronniczość ma realny wpływ na życie jednostki. Dlatego trzeba dostosować ochronę praw i wolności w stosunku do potencjału nadużycia przy zastosowaniu AI. We wskazanej powyżej strategii zwraca się uwagę, iż obecne przepisy koncentrują się na ochronie jednostki, podczas gdy funkcjonowanie AI – systemów masowej analizy – może uderzać w prawa zbiorowe. Tym samym niezbędne będzie tworzenie praw zbiorowych na podstawie wykorzystywanych danych. Konieczne jest także określenie odpowiedzialności za szkody organizacji, które wdrażają i korzystają z AI. Jednak prawo nie może stanowić antidotum dla wszelkich problemów związanych z AI. Wynika to ze zmiany paradygmatu w nauce wprowadzonej przez techniki tzw. głębokiej nauki. Najbardziej wydajna technika uczenia maszynowego, sieci głębokich neuronów (*Deep Learning*), nie polega na ustalonych z góry zasadach. Dlatego trudno jest stworzyć reguły prawne dla tego typu rozwiązań. Jednym z kluczowych problemów AI jest jej etyka, która leży u podstaw regulacji. Uczciwość, stronniczość i dyskryminacja to podstawowe problemy w funkcjonowaniu AI. Brak transparentności tych technologii jest tym bardziej niepokojący. Przykładem może być algorytm kierowania reklam z Google, który częściej oferuje oferty pracy dla kobiet mniej płatne, czy algorytm przewidywania przestępstw sprzyja zwiększonemu nadzorowi nad afroamerykańskimi slumsami. W rzeczywistości wszystkie te algorytmy odtwarzają tylko różnicowanie, które już istnieje w danych im dostarczonych. W miarę jak poszerza się sfera oddziaływania AI na naszą codzienność coraz bardziej oczekuje się od nich działania zgodnie z prawem i normami społecznymi już uznanymi [Pagallo, Corrales, Fenwick, i Forgo 2018, 9–10]. Dlatego ważne jest, aby zarządzać zachowaniem systemów sztucznej inteligencji na podstawie przepisów prawa i etyki. Przestrzeganie zasad uznanych za kluczowe w społeczeństwie wymaga rozwoju procedur, narzędzia i nowych metod kontroli tych systemów, a także stałej oceny zgodności z ramami prawnymi i etycznymi. Problem z regulacją tej sfery działania nowoczesnych technologii związany jest z ochroną własności intelektualnej, która obejmuje AI. Organizacje, które zainwestowały w AI niechętnie przekazują własność intelektualną osobom trzecim. Oznacza to, że przeszkodami w tworzeniu nowych ram prawnych mogą być ochrona własności intelektualnej i tajemnice handlowe (tajemnica przedsiębiorcy), ochrona danych osobowych. Z drugiej strony istnieje konieczność podjęcia działań na rzecz porządku i bezpieczeństwa publicznego. Istnieje zatem ogólna potrzeba skonfigurowania funkcji bufora między sferami tajemnic prawnie chronionych, a uzasadnionym przekazywaniem informacji podyktowanym względami bezpieczeństwa i porządku publicznego. W strategii podkreśla się zmianę paradygmatu regulacyjnego na korzyść uprzedniej oceny wpływu rozwiązania AI na etapie jego modelowania

i budowy architektury na prywatność jednostki. Zalecenie dotyczące analizy wpływu na konkurencyjność oraz ochronę danych odnosi się do konkretnej potrzeby posiadania certyfikowanych audytów (moc dowodowa w dziedzinie postępowań spornych). W ten sposób operatorzy danych powinni ocenić wpływ tej działalności AI, aby wprowadzić korekty zapobiegawcze i być w stanie uzasadnić w przypadku kontroli, że wdrożyli wszystkie niezbędne środki do kontroli całego procesu. To porzucenie systemu uprzedniej zgody jest ważną zmianą paradygmatu na rzecz innowacji. W strategii zwraca się uwagę na zjawisko podejmowania decyzji co do zaprzestania danego czynu, a nie na naprawę tak powstałej szkody. Jedynie zaprzestanie czynu zabronionego i brak odszkodowania pomimo uznania statusu ofiary rodzi frustracje co do siły stosowania prawa. Dlatego proponuje się zintegrowanie procedur dochodzenia praw grupowych odszkodowania za poniesioną szkodę.

W ramach procesu stanowienia prawa według reguł tzw. Sprawiedliwości XXI w. otwarto akcję grupową dotyczącą „danych osobowych" (art. 22 RODO – „Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa") umożliwiono stowarzyszeniom ochrony konsumentów i ochrony danych osobowych do działania w przypadku naruszenia obowiązujących przepisów. Obecnie zmienia się także podejście do odpowiedzialności za działania AI przechodząc od indywidualnej odpowiedzialności (osoby podejmującej decyzję, projektant danego algorytmu lub technologii) do odpowiedzialności kaskadowej. Wreszcie rozwój tych technologii musi nas doprowadzić do pytania o miejsce automatyzacji w ludzkich decyzjach. Czy istnieją obszary, w których ludzki osąd, bez względu na to, jak omylny, nie może być zastąpiony przez maszynę? Niezbędna także tu jest regulacja prawna. W strategii zwraca się także uwagę na kwestie regulacji na poziomie międzynarodowym zastosowania tzw. broni autonomicznej.

3.3. Niemcy[10]

W niemieckiej strategii dotyczącej AI podkreślono, iż rząd federalny angażuje się zarówno w badania, jak i rozwój AI. Niemcy mają stać się wiodącą lokalizacją AI na świecie, zwłaszcza poprzez wszechstronny i szybki transfer technologii. W strategii wskazano na obowiązek używania sztucznej inteligencji w sposób odpowiedzialny i dobroczynny we współpracy z nauką, przemysłem i państwem oraz społeczeństwem obywatelskim, uwzględniając europejskie wartości, takie jak nienaruszalność ludzkiej godności, poszanowanie prywatności. Istotnym celem strategicznym jest zapewnienie bezpieczeństwa systemów informatycznych, które używają i wdrażają AI tak, aby

[10] Zob. https://www.bmbf.de/files/180718%20Eckpunkte_KI-Strategie%20final%20Layout.pdf [dostęp: 25.04.2019].

wyeliminować manipulację, nadużycia i wszelkie inne zagrożenia dla bezpieczeństwa publicznego tej wrażliwej technologii. Jednym z elementów tej polityki jest utworzenie ram prawnych dla programistów i użytkowników technologii AI poprzez ustalenie prawnych ograniczeń stosowania AI. Kluczowa tu jest pewność prawna, ponieważ rosnące zastosowanie sztucznej inteligencji może wymagać zmian w ramach regulacyjnych. W tym zakresie niezbędne jest dokonanie przeglądu i w razie potrzeby, dostosowanie ram prawnych dotyczących wykorzystania danych w pracy AI. W ramach zastosowania sztucznej inteligencji, niezbędne jest w szczególności wyjaśnienie stosunku prawnego między uczestnikami tej relacji. Konieczne wydaje się zapewnienie przejrzystości, identyfikowalności i weryfikowalności systemów, tak aby była skuteczna ochrona przed zakłóceniami i dyskryminacją, manipulacją lub innym niewłaściwym użyciem, szczególnie podczas użytkowania opartego na algorytmach prognozowania i systemach podejmowania decyzji. Istotne też jest promowanie rozwoju innowacyjnych aplikacji samostanowienia, partycypacji społecznej i ochrony prywatności obywateli. W strategii istotne znaczenie ma dostosowanie ram prawa autorskiego do eksploracji tekstu i danych (TDM) jako podstawy uczenia maszynowego do celów komercyjnych i niekomercyjnych z zachowaniem równowagi poszczególnych interesów.

W duchu powyższych założeń uchwalono nowelizację prawa o ruchu drogowym[11] stanowiącą o obowiązku przebywania prowadzącego pojazd przez cały czas na wypadek nagłej potrzeby przejęcia kontroli nad pojazdem zgłoszonej przez system autonomicznego sterowania. Podczas jazdy w trybie autonomicznym kierowca może skorzystać ze smartfonu lub tabletu pod warunkiem, że jest połączony z samochodem. W przypadku, gdy człowiek będzie musiał przejąć kontrolę nad pojazdem, to wówczas dostęp do urządzeń mobilnych ma być zablokowany. Kolejnym obowiązkiem jest instalacja w samochodzie urządzeń rejestrujących poszczególne etapy jazdy, czyli tzw. czarnej skrzynki. Będzie ono potrzebne szczególnie wtedy, gdy dojdzie do awarii, kolizji lub wypadku. Zebrane informacje mają służyć w celu dokonania analizy zdarzenia i ustalenia odpowiedzialności. Kierowca będzie ponosił odpowiedzialność za każdy incydent, chyba że zawiodą systemy bezpieczeństwa i nie uda się zachować kontroli nad pojazdem poruszającym się w autonomicznym trybie. Wówczas odpowiedzialność ponosi producent. Dodatkowo określono podstawowe zasady dotyczące użytkowania AI. Minister transportu Niemiec Alexander Dobrindt powiedział, iż interakcje pomiędzy ludźmi i maszynami skłaniają do stawiania nowych pytań etycznych, zwłaszcza w dzisiejszych

[11] Zob. Autonomes und automatisiertes Fahren auf der Straße – rechtlicher Rahmen Aktenzeichen: WD 7 – 3000 –111/18. Abschluss der Arbeit: 22. Mai 2018 Fachbereich: WD 7: Zivil-, Straf- und Verfahrensrecht, Umweltschutzrecht, Bau und Stadtentwicklung, https://www.bundestag.de/resource/blob/562790/c12af1873384bcd1f8604334f97ee4b9/wd-7-111-18-pdf-data.pdf [dostęp: 25.04.2019].

czasach cyfryzacji i samouczących się systemów. Posłużył się trzema tzw. prawami robotów ustalonymi w 1942 r. przez pisarza Isaaca Asimova. Nowe zasady odnoszące się do autonomicznych pojazdów są wariacją tych praw i przedstawiają się następująco: 1) uszkodzenie mienia zawsze poprzedza krzywdę osobistą; 2) nie może być żadnej dyskryminacji ludzi, na przykład ze względu na wzrost, wiek itp.; 3) w przypadku zaistnienia szkody, odpowiedzialny jest producent.

Ze wskazanych powyżej strategii wynika jednoznaczna potrzeba zmian regulacyjnych, podyktowanych względami etyki AI. Konieczność ta związana jest z wartościami o charakterze powszechnym – ochroną danych, prawem do prywatności, ochroną własności intelektualnej, ustaleniem zasad odpowiedzialności karnej i cywilnej[12]. Cele przyszłej regulacji wydają się być tu oczywiste i standardowe. Jednak w kontekście samego stanowienia prawa we wskazanym obszarze polityki poszczególnych państw zasadniczo się różnią. Państwa członkowskie UE minimalizują swoje zaangażowanie w stanowieniu nowego prawa odnośnie do AI oczekując regulacji na poziomie Parlamentu Europejskiego[13]. Uzasadnieniem zmian strategicznych, a następnie regulacyjnych jest potrzeba stworzenia dogodnych warunków konkurencji rynkowej, która nie znosi przeregulowania (Wielka Brytania), z drugiej strony istnieje potrzeba zmian rewolucyjnych poprzez wprowadzenie monitoringu państwa i pogłębionej ochrony praw grupowych (Francja). Pojawiają się także regulacje praktyczne, które wdrażane są *ad hoc* wobec tendencji rozwojowych w danej dziedzinie – i wydaje się, iż ta ostatnia koncepcja jest uzasadniona naturą samych nowoczesnych technologii. Z całą pewnością należy zaznaczyć, iż sztuczna inteligencja to zagadnienie interdyscyplinarne, co obrazują przywołane strategie. W tych okolicznościach wymagana jest strategia wypracowana w oparciu o złożoną analizę uwzględniającą wiele aspektów zjawiska AI [Hildebrandt 2013, 42].

[12] Na marginesie dodać należy, iż takie założenia zawiera także chińska strategia „Nowa generacja planowania rozwoju sztucznej inteligencji z 8 lipca 2017 r." Zgodnie ze strategią prowadzenie badań w kwestiach prawnych, takich jak potwierdzenie odpowiedzialności cywilnej i karnej, ochrona prywatności i praw własności oraz wykorzystanie bezpieczeństwa informacji związanych z aplikacjami sztucznej inteligencji, ustanowienie systemu identyfikowalności odpowiedzialności oraz wyjaśnienie przedmiotu sztucznej inteligencji i powiązanych praw, obowiązków.

[13] Zob. Rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki, 2015/2103(INL). Dokumentem o znacznie niższej randze jest Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Sztuczna inteligencja dla Europy", Bruksela (25.04.2018), COM (2018) 237 final.

PODSUMOWANIE

Warunkiem stworzenia właściwych ram regulacyjnych w obszarze nowych technologii jest stworzenie wieloaspektowej strategii państwa, która wyznaczać powinna kierunki regulacyjne i cele interesu publicznego. Jednym z kluczowych zadań państwa jest stworzenie jednolitego systemu takiej regulacji, wypracowanie ram prawnych, które nie powinny zawierać postanowień odrębnych dla różnych obszarów technologicznych (zasada neutralności technologicznej). W pierwszej kolejności wymagane jest wypracowanie jednego systemu polityki stanowienia prawa nowoczesnych technologii, która obejmować powinna całość działań w środowisku cyberprzestrzeni. Oczywiste jest, że takie ramy regulacyjne muszą powstawać w oparciu o prawa podstawowe. Obszar ten można podzielić na trzy kategorie: 1) regulację kwestii dotyczących nowoczesnych technologii jako przedmiotu ochrony oraz regulację kwestii dotyczących ochrony dóbr związanych z korzystaniem z nowoczesnych technologii; 2) regulację zwianą z funkcjonowaniem jednostki w warunkach rozwoju nowoczesnych technologii oraz 3) regulację dotyczącą granic zastosowania nowoczesnych technologii. Analizując kwestie bezpośrednio nawiązujące do regulacji w obszarze nowoczesnych technologii, należy podkreślić, iż dobra niematerialne, które są bezpośrednio związane z zastosowaniem produktów będących efektem nowoczesnych technologii, stanowią odrębny przedmiot regulacji od samych technologii.

Koniecznym etapem przyszłych regulacji jest zdefiniowanie celów interesu publicznego w nowych warunkach technologicznych. Definiowanie celów interesu publicznego w warunkach funkcjonowania cyfrowego społeczeństwa informacyjnego wymaga ponownego zdefiniowania społeczeństwa obywatelskiego w jego cyfrowej odmianie, a także określenia i klasyfikacji zagrożeń, jakie wiążą się z rozwojem technologii i globalizacją sieci. W procesie tych ustaleń należy odpowiedzieć na pytania: jaki jest zakres oddziaływania nowych technologii na sferę publiczną i indywidualną jednostkę w warunkach cyfrowych? Jakie są źródła politycznej autonomii współczesnych sieci, w jakim kontekście należy badać ich zróżnicowanie w sferze publicznej i prywatnej przy zastosowaniu metody porównawczej? Jak zredefiniować zadania publiczne realizowane w warunkach nowych technologii, jak należy ustalić nową rolę i znaczenie administracji publicznej w kontekście realizacji polityki państwa narodowego wobec ochrony jednostki przed zagrożeniami, jakie niosą nowe technologie? Jak polityka informatyzacji, polityka kryzysu w warunkach rozwoju nowych technologii sprawdza się wobec zadań dotyczących cyberprzestępczości i zagrożeń bezpieczeństwa narodowego, czy stanowi jedyny sposób rozwoju? Jakie instrumenty prawne można zastosować, aby za ich pomocą nowoczesne państwo narodowe mogło w sposób bezpieczny dla siebie oddziaływać na zakres procesu dostosowawczego, przy uwzględnieniu

nowoczesnych rozwiązań technologicznych oraz specyfiki nowych wspólnot sieci? To tylko wstępna lista koniecznych rozważań.

Obszary wymagające nowego podejścia władzy publicznej dzieli się na zagadnienia dotyczące: wprowadzenia „ładu technologicznego" poprzez nowe rozwiązania systemowe, wprowadzenia „ładu moralnego" w szerokim ujęciu, dotyczyć to będzie kwestii ochrony dóbr osobistych, dzieci i młodzieży, przyjętego systemu aksjologicznego, tożsamości narodowej, dziedzictwa narodowego (digitalizacja archiwum), prawa do prywatności, praw autorskich i pokrewnych, wiarygodnych źródeł informacji czy wszystkich innych elementów, które składają się na pojęcie bezpieczeństwa narodowego; wprowadzenia „zasad realizacji i powierzania zadań publicznych", można tu mówić o wszelkich środkach prawnych służących realizacji tzw. misji publicznej w ramach wykonywania zadań publicznych przez państwo, a związanych z rozwojem nowych technologii.

Obecnie mamy do czynienia z fragmentarycznością regulacji. Nowe rozwiązania prawne dotyczą spraw newralgicznych społecznie, np. ochrony prawa autorskiego, świadczenia usług drogą elektroniczną w zakresie ochrony konsumenckiej czy ochrony dzieci i młodzieży. Dlatego niezwykle ważne jest wprowadzenie regulacji systemowej, która odnosiłaby się konsekwentnie do różnych obszarów interaktywności, operując jednak w sposób elastyczny jednolitym zakresem pojęciowym. Przykład przywołanych strategii europejskich wskazuje, iż proces stanowienia prawa w sferze nowych technologii ma charakter ograniczony do bardzo określonego obszaru potrzeb, nie jest zsynchronizowany, nie tworzy projektu jednolitych ram prawnych z powodu ograniczonych możliwości, związanych ze specyfiką nowoczesnych technologii. Pewna konsolidacja regulacji usług sieciowych występuje w przepisach regulujących dziedzinę telekomunikacji, ale nie jest to wystarczające rozwiązanie dla ochrony cyberbezpieczeństwa oraz praw i wolności jednostki. Ochrona prywatności w cyberprzestrzeni ma szczególne znaczenie i wymiar niemal aksjologiczny. Kwestia zakresu tej ochrony odnosi się do zagadnienia granic regulacji i dozwolonej konstytucyjnie ingerencji władz publicznych w przestrzeń prywatną jednostki, także w sytuacji zagrożeń związanych ze sztuczną inteligencją. Ochrona godności i prywatności jednostki to jedno z kluczowych zadań państwa. Innowacje i wynalazczość wpływają bezpośrednio nie tylko na charakter czy sposób życia ludzkiego, ale także poprzez rozwój sztucznej inteligencji na samą jego naturę.

PIŚMIENNICTWO

Braman, Sandra. 2006. *Change of State: Information, Policy, and Power*. Cambridge: MIT Press.

Chałubińska–Jentkiewicz, Katarzyna. 2011. *Media audiowizualne. Konflikt regulacyjny w dobie cyfryzacji*. Warszawa: Wolters Kluwer Polska.

Chałubińska–Jentkiewicz, Katarzyna. 2014. „Metoda zarządzania publicznego w procesie cyfryzacji na przykładzie zasobów archiwalnych." W *Procesy kierowania w systemie administracji publicznej*, red. Jan Łukasiewicz, 65–75. Rzeszów: Wydawnictwo Towarzystwo Naukowe Organizacji i Kierownictwa Oddział w Rzeszowie.

Chałubińska–Jentkiewicz, Katarzyna. 2016. "European administrative unification in the field of culture security." In *Legal Context in the Chosen Order and Security Area*, ed. Paweł Kobes, Gerald G. Sander, and Piotr Nadybski, 9–22. Hamburg: Verlag Dr. Kovač.

Chałubińska–Jentkiewicz, Katarzyna. 2019. *Cyberodpowiedzialność*. Toruń: Wydawnictwo Adam Marszałek.

Chałubińska–Jentkiewicz, Katarzyna, i Mirosław Karpiuk. 2015. *Prawo nowych technologii.* Warszawa: Wolters Kluwer Polska.

Dervanović, Dena. 2018. "Inhuman Lawyer:Developing Artificial Intelligence in the Legal Profession." In *Robotics, AI and the Future of Law*, ed. Marcelo Corrales, Mark Fenwick, and Nikolaus Forgo, 209–34. Singapore: Springer.

Hallevy, Gabriel. 2015. *Liability for Crimes Involving Artificial Intelligence Systems*. Switzerland: Springer.

Hildebrandt, Mireille. 2013. "From Galatea 2.2 to Watson- and back?" In *Human Law and Computer Law: Comparative Perspectives*, ed. Mireille Hildebrandt, and Jeanne Gaakeer, 23–45. Dordrecht: Springer.

Pagallo, Ugo. 2013. *The Laws of Robots Crimes, Contracts, and Torts*. Dordrecht Heidelberg New York: Springer.

Pagallo, Ugo, Marcelo Corrales, Mark Fenwick, and Nikolaus Forgo. 2018. "The Rise of Robotics & AI: Technological Advances. Normative Dilemmas." In *Robotics, AI and the Future of Law*, ed. Marcelo Corrales, Mark Fenwick, and Nikolaus Forgo, 1–13. Singapore: Springer.

Szymczak, Mieczysław, red. 1999. *Słownik języka polskiego*. T. 3. Warszawa: Wydawnictwo Naukowe PWN. Zubik, Marek. 2008. „Nowe technologie jako wyzwanie i zagrożenie dla prawa, statusu jednostek i państwa." W *Prawo wobec nowoczesnych technologii*, red. Piotr Girdwoyń, 37–50. Warszawa: Liber.

THE DEVELOPMENT OF MODERN TECHNOLOGIES IN THE CONTEXT OF THE LAWMAKING PROCESS ON THE EXAMPLE OF AI STRATEGY

Summary. Modern technologies create foundations for economic growth and they are of crucial importance for all sectors of economy and society. I'm sure you will agree with me that these days electronic payments, computing clouds and robot – robot communication are becoming more and more popular. The question is what are the borders of development and influence of technology on law making? On the one hand, new technologies determine development but they have to be limited by certain rights, for example the law of industrial property. On the other hand, these technological innovations interfere with these rights and it's more difficult to protect them. That's why this situation poses threat to the safety of individuals and citizens. What's more, practically in every area of human life appear problems of ethical and legal regulations connected with functioning of robots and computers.

Key words: strategy, regulation, application of law and lawmaking, new technology law, modern technologies, artificial intelligence

Information about Author: Katarzyna Chałubińska–Jentkiewicz, hab. Ph.D., University Professor – Department of Cybersecurity Law and New Technologies, Institute of Law at the War Studies University; e-mail: kasiachalubinska@gmail.com; https://orcid.org/0000-0003-0188-5704