

Propozycja modernizacji dyrektywy o produktach wadliwych (PLD) a odpowiedzialność cywilna za systemy sztucznej inteligencji

Jakub Kwaśniak¹

Celem artykułu jest omówienie zmian proponowanych przez UE w ramach projektu nowej dyrektywy o odpowiedzialności za produkty wadliwe (*Product Liability Directive*, PLD) w świetle ich wykorzystania w celu dochodzenia odpowiedzialności cywilnej za sztuczną inteligencję. Omówione zostały kwestie dotyczące wstępnego etapu prac nad projektem, czyli zakres poruszany w ramach konsultacji publicznych. Następnie przeanalizowano poszczególne, najważniejsze zdaniem autora, zmiany samej treści dyrektywy, na które składają się kwestie przedmiotowe, podmiotowe i proceduralne. Omawiane zmiany skupiają się głównie wokół rozszerzenia ram definicyjnych i zastosowania odpowiednich konstrukcji prawnych w celu dopasowania przepisów dyrektywy do specyfiki roszczeń związanych z działalnością systemów sztucznej inteligencji.

Uwagi wstępne

Nie będzie nadużyciem stwierdzenie, że na przestrzeni ostatnich kilku miesięcy sztuczna inteligencja stała się jednym z najchętniej poruszanych tematów technologicznych. Unia Europejska podążyła za tym trendem i w ostatnich latach znacznie zintensyfikowała pracę nad uregulowaniem wielu kwestii związanych z tą branżą². Rezultatem trwających kilka lat prac Unii jest opublikowany przez Komisję Europejską 28.9.2022 r. pakiet regulacyjny³. W jego skład wchodzi propozycja modernizacji dyrektywy o przedmiotach niebezpiecznych (PLD) oraz całkowicie nowy projekt dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję (AILD)⁴.

Oba projekty dotyczą podobnych kwestii, jednak różnią się od siebie w pewnych fundamentalnych założeniach – przede wszystkim AILD dotyczy aspektów wyłącznie formalnych, opartych na prawie krajowym i zasadzie winy, natomiast PLD dotyka także kwestii materialnych i oparta jest na prawie unijnym.

W doktrynie można odnieść wrażenie, że większą uwagę komentujących cieszy się projekt AILD – być może ze względu na bezpośrednie powiązanie z tematem sztucznej inteligencji przez swoją nazwę. Niniejsze opracowanie dotyczy jednak modernizacji PLD i tego, w jaki sposób proponowane w niej przepisy odnoszą się do systemów sztucznej inteligencji. Jako że proces legislacyjny w dalszym ciągu trwa, opracowanie opiera się na treści przepisów zaproponowanych w najnowszej wersji projektu zaprezentowanej przez szwedzką prezydentkę w Radzie UE w kwietniu 2023 r., przy czym należy pamiętać, że nie jest to wersja ostateczna⁵.

Kwestie poruszane w konsultacjach publicznych

Potrzeba modernizacji dyrektywy o odpowiedzialności za produkty niebezpieczne była podnoszona w doktrynie od dłuższego czasu. Argumentowane to było zmianą sposobu wytwarzania i dystrybucji produktów i samych produktów, które stały się znacznie bardziej zależne od niematerialnego,

¹ Autor jest aplikantem radcowskim przy Okręgowej Izbie Radców Prawnych we Wrocławiu, absolwentem stacjonarnych studiów prawa na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. ORCID: 0009-0005-9645-9530. Opracowanie jest zmodyfikowanym rozdziałem pracy magisterskiej autora pt. „Odpowiedzialność cywilna za systemy sztucznej inteligencji na przykładzie propozycji legislacyjnych Unii Europejskiej”.

² G. Borges, Liability for AI Systems Under Current and Future Law An overview of the key changes envisioned by the proposal of an EU-directive on liability for AI, *Computer Law Review International* vol. 24, nr 1/2023, <https://doi.org/10.9785/crl-2023-240102> (dostęp z 8.7.2023 r.).

³ W przypadku AILD był to okres od 20.10.2020 r., a w przypadku PLD od 2018 r., s. 1 AILD i s. 1 PLD. W stosunku do PLD opracowywane były raporty (w założeniu co 5 lat), w których dokonywano rewizji efektywności przepisów i ich dostosowania do zmieniającej się rzeczywistości. W 2018 r. opublikowano ostatni, piąty raport, na bazie którego zasugerowano stworzenie grupy eksperckiej, która miała za zadanie opracować nowy projekt Dyrektywy. Grupa ta została podzielona na dwie części – jedna zajmowała się opracowaniem przepisów dotyczących odpowiedzialności za produkt niebezpieczny (*product liability formation*), a druga kwestią nowych technologii (*new technologies formation*). Efektem tych prac jest omawiana regulacja.

⁴ Wniosek – dyrektywa Parlamentu Europejskiego i Rady z 28.9.2022 r. w sprawie odpowiedzialności za produkty wadliwe COM/2022/495 final 2022/0302 (COD), dalej PLD; Wniosek – dyrektywa Parlamentu Europejskiego z 28.9.2022 r. i Rady w sprawie dostosowania przepisów dotyczących pozasądowej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję), 2022/0303 (COD), dalej AILD.

⁵ L. Bertuzzi z EURACTIV.com zaznacza, że jest to już trzecia propozycja zaprezentowana w ramach prezydencji, aczkolwiek głównym celem zmian jest doprecyzowanie znaczenia tekstu, a nie jego znaczna modyfikacja. L. Bertuzzi, EU Council clarifies liability rules for software updates, machine learning, <https://www.euractiv.com/section/digital/news/eu-council-clarifies-liability-rules-for-software-updates-machine-learning/> (dostęp z 8.7.2023 r.).

w klasycznym tego słowa znaczeniu, świata cyfrowego⁶. W ramach prac przeprowadzono również konsultacje społeczne, co do których odzew społeczny był dość wyraźny, zwłaszcza ze strony branży technologicznej, która naturalnie była zainteresowana wyrażeniem zdania dotyczącego przepisów mogących dotknąć ją bezpośrednio w najbliższej przyszłości.

Przedstawiciele producentów opowiadali się za brakiem zmiany samej dyrektywy⁷. Zamiast tego proponowali stworzenie regulacji szczególnych, a w skrajnych przypadkach jedynie niewiążących wytycznych, które miałyby uporządkować praktykę⁸. Wynikało to z obawy przed włączeniem szerokiego katalogu potencjalnych wad w produktach niematerialnych, głównie w oprogramowaniu, pod zastrzeżeniem odpowiedzialności opartą na zasadzie ryzyka⁹. Dodatkowo wyraźny sprzeciw przed ewentualnym rozszerzaniem zakresu przedmiotowego argumentowany był faktem, że produkt niematerialny nie jest w stanie sam spowodować szkody na osobie lub szkody materialnej, ponieważ musi działać on razem z jakąkolwiek rzeczą materialną¹⁰. Mimo to większość zainteresowanych zgodziła się z twierdzeniem, że oprogramowanie jest produktem, który wchodzi w skład PLD, oraz że produkt można uznać za wadliwy ze względu na luki w cyberbezpieczeństwie.

Jednomyślnie obie strony podeszły do kwestii rozszerzenia odpowiedzialności na mocy PLD, a więc na zastrzeżeniu odpowiedzialności wobec podmiotów, które dokonują znacznych modyfikacji produktów, w wyniku czego zmodyfikowany produkt staje się wadliwy i może spowodować szkodę¹¹. Może to mieć kluczowe znaczenie także przy systemach AI, które na takie modyfikacje są narażone.

Pozytywne opinie, chociaż różniące się m.in. co do kwestii odpowiedzialnego podmiotu, dotyczyły również ochrony konsumentów w przypadku zakupów wadliwych produktów bezpośrednio w państwach trzecich, a przy których brak jest producenta i importera mającego siedzibę na terenie UE¹².

Mimo iż nie budzi wątpliwości, że wykazanie wadliwości produktu może być problematyczne, to przedsiębiorcy nie byli chętni rezygnować ze swojej pozycji w celu ułatwienia poszkodowanym dochodzenia swoich żądań ani też obarczać się dodatkową pracą i obowiązkami¹³. Wśród argumentów przeciwko odwróceniu ciężaru dowodów podawano m.in. nadmierne obciążenie zarówno sądów, jak i producentów, którzy zajęci by byli wyłącznie analizą każdego podejrzenia wady systemu zgłoszonej przez użytkowników¹⁴.

Twierdzono także, że jest to rozwiązanie zbyt radykalne i może spowodować zahamowanie innowacyjności rynku¹⁵. Spowolnienie rynku z powodu wprowadzenia regulacji ograniczających swobodę działania branży Tech w stosunku do innych części świata może jednak nie być całkowicie realnym scenariuszem i należy się zastanowić, czy nie powinno się interpretować tego argumentu jako element strategii przed-

siębiorstw, które próbują wpłynąć na legislatorów. Rynek europejski zdaje się być bowiem zbyt istotnym i zbyt zasobnym rynkiem dla większości firm, aby móc sobie pozwolić na wycofanie się z wprowadzania innowacji analogicznych do tych, które są wprowadzane w innych regionach. Taki wniosek wydaje się racjonalny, nawet jeśli uwzględnimy dodatkowe koszty i czas, których wymaga stworzenie systemów zasadniczo lepiej chroniących konsumenta.

Kolejną odmiennością było podejście do kwestii zniesienia minimalnego progu wartości szkody majątkowej oraz długości trwania okresu, w którym producenci są odpowiedzialni za produkt wadliwy po wprowadzeniu go do obrotu. Strona konsumentcka uznawała obecny próg w wysokości 500 euro za nadmiernie wysoki, natomiast 10-letni okres

⁶ B.A. Koch, J.-S. Borghetti, P. Machnikowski, P. Pichonnaz, T. Rodríguez de las Heras Ballell, Ch. Twigg-Flesner, Ch. Wendehorst, Response of the European Law Institute to the Public Consultation on Civil Liability – Adapting Liability Rules to the Digital Age and Artificial Intelligence, *Journal of European Tort Law*, vol. 13, no. 1, 2022, <https://doi.org/10.1515/jetl-2022-0002> (dostęp z 8.7.2023 r.).

⁷ Dobrym przykładem jest opinia Google, w której zaproponowano stworzenie osobnej kategorii quasi-produktów, które miałyby uregulowanie za pomocą węższych regulacji wzorowanych np. na rozporządzeniu w sprawie wyrobów medycznych. Opinia Google: Consultation on the inception impact assessment for adapting liability rules to the digital age and circular economy, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Dyrektywa-w-sprawie-odpowiedzialnosci-za-produkty-dostosowanie-przepisow-dotyczacych-odpowiedzialnosci-do-ery-cyfrowej-gospodarki-o-obiegu-zamknietym-i-globalnych-%C5%82ancuchow-wartosci/F2663311_pl (dostęp z 8.7.2023 r.).

⁸ Zob. Uzasadnienie PLD, s. 9.

⁹ Computer&Communications Industry Association (CCIA) w swojej odpowiedzi stanowczo opowiedziała się przeciwko rozszerzaniu definicji produktu na rzeczy niematerialne, gdyż ich zdaniem wprowadzenie odpowiedzialności na zasadzie ryzyka było nieproporcjonalne i niedopasowane co do specyfiki systemów AI., <https://ccianet.org/news/2021/12/ccia-responds-to-eu-consultation-on-civil-liability-and-ai/> (dostęp z 8.7.2023 r.).

¹⁰ Zob. Opinia: Fujitsu, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13601-Liability-rules-for-Artificial-Intelligence-The-Artificial-Intelligence-Liability-Directive-AILD-/F2663318_pl (dostęp z 8.7.2023 r.).

¹¹ Zob. Uzasadnienie PLD, s. 9.

¹² 64% respondentów zgodziło się z tym lub zdecydowanie się zgodziło, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52022PC0495>.

¹³ Komisja obliczyła, że 77% respondentów uznało, że produkty skomplikowane technicznie powodują trudności pod względem ciężaru dowodów spoczywającego na poszkodowanym, jednak widać tu znaczną dysproporcję – wśród konsumentów aż 95% opowiadało się za tym stanowiskiem, natomiast wśród przedsiębiorców jedynie 38%.

¹⁴ DJI – Public Consultation – Civil liability: adapting liability rules to the digital age and AI https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Dyrektywa-w-sprawie-odpowiedzialnosci-za-produkty-dostosowanie-przepisow-dotyczacych-odpowiedzialnosci-do-ery-cyfrowej-gospodarki-o-obiegu-zamknietym-i-globalnych-%C5%82ancuchow-wartosci/F26633259_pl (dostęp z 5.1.2023 r.).

Podobnie wypowiadało się także CCIA, które w swojej opinii stwierdziło, że odwrócenie ciężaru dowodu doprowadzi do masowego występowania z lekkomyślnymi i nieuczciwymi roszczeniami (ang. frivolous and fraudulent – tłum. Autor) <https://ccianet.org/news/2021/12/ccia-responds-to-eu-consultation-on-civil-liability-and-ai/> (dostęp z 8.7.2023 r.).

¹⁵ Zob. Uzasadnienie PLD, s. 10.

Można spotkać się nawet z opiniami, przykładowo opinią wyrażoną przez CCIA, że nadmierna ilość roszczeń spowoduje nieproporcjonalną szkodę dla rynku, *op. cit.* (dostęp z 8.7.2023 r.).

odpowiedzialności za zbyt krótki. Producenci zajęli zaś stanowisko odmienne. Również wydłużenie okresu odpowiedzialności w przypadku produktów wykorzystujących różne formy oprogramowania, w tym systemy AI, nie został przez nich zaaprobowany¹⁶.

Cele, które w ramach konsultacji społecznych zostały przez Komisję zaproponowane, wpisują się w ogólny kierunek działań Unii, które może być określane mianem sztucznej inteligencji z ludzką twarzą¹⁷. Stąd też nie dziwi sceptyczne podejście przedstawicieli branży. Unia Europejska musiała więc – i cały czas musi – balansować między interesem producentów, których działalność, zwłaszcza w branży technologicznej stanowi istotną gałąź gospodarki Wspólnoty, a interesem obywateli, potencjalnych użytkowników systemów AI, którzy oczekują od prawodawców jak najszerzej ochrony.

Definicja produktu

Pierwszą kwestią, która rzuca się w oczy przy analizie propozycji Komisji, jest jej znacznie większa objętość w stosunku do pierwotnej wersji dyrektywy. W celu ułatwienia korzystania z przepisów i uniknięcia problemów interpretacyjnych wprowadzono słowniczek ustawowy. W nim przedstawiono nową definicję produktu, która została rozszerzona względem dotychczasowo obowiązującej. W skład produktu wchodzić mają także m.in. cyfrowe pliki produkcyjne oraz oprogramowanie. Dodatkowo termin części składowej, charakterystyczny dla klasycznej formy produktów, został określony terminem „rzeczy ruchomej, nawet jeżeli jest ona zintegrowana z inną rzeczą ruchomą lub nieruchomą”, przy czym, w przeciwieństwie do pierwszej propozycji KE, nie chodzi tu wyłącznie o integrację dokonaną przez producenta lub pod jego kontrolą.

Z produktem jest związana także definicja powiązanej usługi, która oznacza „usługę cyfrową, która jest zintegrowana z produktem lub wzajemnie z nim połączona w taki sposób, że jej brak uniemożliwiłby realizację przez produkt jednej z jego funkcji”, jednak wyłączono tu m.in. usługę dostępu do Internetu zgodnie z dyrektywą PE i Rady 2018/1972.

Podział na „części składowe”, a więc – innymi słowy – treści cyfrowe (*digital content*) i „powiązaną usługę”, czyli usługi cyfrowe (*digital services*), wywodzi się z Dyrektywy w sprawie niektórych aspektów umów sprzedaży towarów (*Sales of Goods Directive*), która stosuje analogiczne terminy¹⁸.

Samo pojęcie oprogramowania zawiera w sobie także systemy AI, które powinny być rozumiane jako szczególnie rodzaj oprogramowania, przy czym wyłączone zostały systemy AI wysokiego ryzyka¹⁹. Definicja oprogramowania nie jest jednak pełna. Zgodnie z motywem 13 Preambuly (zastanawiać może, dlaczego tylko w Preambule) w celu uniknięcia ewentualnego ograniczenia innowacji czy badań, dyrektywy nie stosuje się do tzw. oprogramowania „open-source”,

a więc „darmowego i otwartego oprogramowania, które jest opracowywane i dostarczane poza działalnością handlową”²⁰. Może to wzbudzać wątpliwości na gruncie systemów AI, które – przynajmniej przy obecnym stopniu rozwoju – często są oferowane w ramach oprogramowania open-source. Zainteresowanymi modelami AI opartymi na oprogramowaniu open-source są nie tylko start-upy, ale także potentaci branży Tech²¹. W tym wypadku nie wiadomo, na ile takie rozwiązanie ograniczy możliwość efektywnego dochodzenia roszczeń i to w przypadku prawdopodobnie najczęściej (ze względu na ich darmowość) używanych systemów.

Podział na części składowe i powiązane usługi stanowi przykład odejścia od ogólnej zasady, zgodnie z którą usługi nie są regulowane zakresem PLD. Decyzja o włączeniu tej kategorii w ramy Dyrektywy oceniana jest jednak w doktrynie pozytywnie, gdyż świadczy o tym, że Komisja trafnie zauważa zmianę w projektowaniu urządzeń²². W przypadku systemów AI jest to wręcz kluczowe, gdyż bardzo często sztuczna inteligencja, zwłaszcza bazująca na oprogramowaniu opartym na działaniu w chmurze oferowana jest konsumentom jako usługa, a nie jako produkt²³. Obecnie trudno jest zastosować klasyczne ujęcie tego tematu, w przypadku kiedy większość urządzeń zawiera w sobie elementy cyfrowe, które regulują prawidłowe działanie końcowego produktu. Dodatkowo po-

¹⁶ Argument ten dało się dostrzec również znacznie wcześniej, bo już w 2017 r., na Konferencji dotyczącej odpowiedzialności za produkt (*Product Liability Conference*, 20.10.2017 r., Bruksela) firma Intel wyraziła stanowisko, że kwestia 10-letniego okresu odpowiedzialności wyklucza możliwość traktowania oprogramowania jako produkt, a co za tym idzie – stosowania wobec oprogramowania reżimu PLD, ponieważ oprogramowanie jest nieustannie aktualizowane, a więc nie da się przewidzieć, od kiedy należy zacząć liczenie wspomnianego okresu, <https://ec.europa.eu/docsroom/documents/26661?locale=en> (dostęp z 8.7.2023 r.).

¹⁷ Ang. *Human-centric Approach*, podejście to podkreślane jest często przez organy Unii, a zapoczątkowane zostało w komunikacie Komisji z 25.4.2018 r. *Sztuczna inteligencja dla Europy*, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52018DC0237> (dostęp z 8.7.2023 r.).

¹⁸ J. De Bruyne, O. Dheu, Ch. Ducuing, *The European Commission's Approach To Extra Contractual Liability and AI – An Evaluation of the AI Liability Directive and the Revised Product Liability Directive*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4295676 (dostęp z 8.7.2023 r.).

¹⁹ P. Hacker, *The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future*, <https://arxiv.org/abs/2211.13960> (dostęp z 8.7.2023 r.).

²⁰ Zob. Motyw 13 Preambuly PLD, jak podkreślono w najnowszej wersji tekstu, jest to spowodowane faktem, że tego rodzaju produkty nie są, z samej swojej definicji, wypuszczane na rynek.

²¹ W.D. Heaven, *The open-source AI boom is built on Big Tech's handouts. How long will it last?*, MIT Technology Review, <https://www.technologyreview.com/2023/05/12/1072950/open-source-ai-google-openai-eleuther-meta/>, dostęp: 8.07.2023 r. – Heaven zauważa, że motywacja stojąca za tym zainteresowaniem różni się – największe firmy pokroju Mety czy OpenAI uważnie przyglądają się rozwojowi branży, jednak są oni w stanie ograniczyć działalność firm opracowujących systemy AI typu open-source z uwagi na swoją przewagę finansową i technologiczną.

²² P. Hacker, *op. cit.*

²³ T.S. Cabral, *Liability and artificial intelligence in the EU: Assessing the adequacy of the current Product Liability Directive*, Maastricht Journal of European and Comparative Law, vol. 27, nr 5, 2020, s. 615–635, <https://doi.org/10.1177/1023263X20948689> (dostęp z 8.7.2023 r.).

jedyncze urządzenia mogą się ze sobą łączyć i tworzyć zależne od siebie ekosystemy, np. w ramach IoT. Słusznie zauważono, że zarówno z punktu widzenia zasad odpowiedzialności, jak i z punktu widzenia politycznego, nie istnieją przesłanki dla traktowania w inny sposób oprogramowania sprzedawanego jako osobny produkt od oprogramowania będącego w pakiecie z nośnikiem fizycznym²⁴.

Dla systemów AI znaczenie ma także wprowadzenie definicji „kontroli producenta”, gdyż w praktyce istotne może okazać się wykazanie, czy dany podmiot był w stanie kontrolować działanie produktów obdarzonych wysoką autonomią. Zgodnie z art. 4 ust. 5 PLD, mowa tu o sytuacji, w której producent dokonuje lub w przypadku działania strony trzeciej zezwala bądź wpływa na integrację, wzajemne połączenie lub dostawę części składowej, w tym aktualizację lub modernizację oprogramowania, lub na modyfikację produktu, w tym istotną modyfikację, a także ma możliwość samodzielnego dokonywania lub zezwalania stronie trzeciej na dokonanie aktualizacji (*update*) lub zmiany wersji oprogramowania (*upgrade*). Termin modyfikacji istotnej, który nie pojawił się w początkowej propozycji KE, oznaczać ma taką modyfikację produktu wprowadzonego na rynek lub oddanego do użytku, która została uznana za istotną przez przepisy unijne lub krajowe albo nie została przez nie określona, jednak dotyczy zmiany pierwotnego działania, przeznaczenia, typu produktu, które nie zostało przewidziane przy pierwotnej ocenie ryzyka i zmienia charakter zagrożenia bądź stwarza go na nowo lub podnosi poziom ryzyka. W przypadku systemów AI w praktyce możemy spodziewać się wielu takich zmian, gdyż wprowadzone do algorytmu dane mogą z łatwością wpłynąć na zmianę zakresu ryzyka programu, który ma spory stopień autonomiczności.

Szkoda

Projektodawcy PLD zdecydowali się na podtrzymanie dość wąskiego zakresu szkód. Tak jak w oryginalnej Dyrektywie, ograniczono się wyłącznie do strat materialnych. Jedną z głównych zmian było zrezygnowanie z dotychczasowego progu wartości szkody. Poza zakresem regulacji zostały jednak tak istotne kwestie, jak np. szkody związane z przetwarzaniem danych, co Komisja kontrargumentuje istnieniem odpowiednich rozwiązań, w szczególności na bazie RODO, czy też szkody wywołujące stratę ekonomiczną²⁵. Co prawda w dodanym w trakcie prac legislacyjnych art. 5a ust. 2 podkreślono – co należy ocenić pozytywnie – że powyższe ograniczenia nie wyłączają zastosowania krajowych przepisów dotyczących odszkodowania za szkody niematerialne, jednak takie podejście może negatywnie wpłynąć na harmonizację przepisów wspólnotowych i równe szanse dochodzenia roszczeń w przypadku popularnych przecież w świecie cyfrowym spraw ponadnarodowych.

Takie rozwiązanie może wyłączać możliwość ochrony i kompensacji na gruncie PLD w dużej liczbie przypadków. Przykładowo wskazywano, że w przypadku użycia systemu AI w celu scoringu kredytowego czy oceny sytuacji finansowej, w momencie kiedy zostanie wyrządzona szkoda, można się spodziewać, że będzie to typowa szkoda finansowa, a nie materialna²⁶. Jak trafnie zwróciła uwagę *U. Pach*, zastępca dyrektora BEUC²⁷, w takim przypadku osoba domagająca się kompensacji szkody będzie mogła skorzystać jedynie z przepisów AILD, które opierają się na zasadzie winy. To rozwiązanie utrudnia efektywne dochodzenie roszczeń, przede wszystkim z uwagi na złożoność systemów AI wykorzystywanych m.in. przez banki, co przekłada się bezpośrednio na trudność i kosztowność wykazania winy²⁸. Podejście UE do terminu szkody należy uznać za błąd, zwłaszcza mając na uwadze sytuację strony słabszej, czyli poszkodowanego. Z pewnością są one korzystne dla strony producentów, jednak prawodawcy nie powinni zapominać, że celem wprowadzanych przepisów powinno być, przy zachowaniu odpowiedniego balansu, wzmocnienie pozycji potencjalnych poszkodowanych będących obywatelami Unii, którym do tej pory trudno było jakkolwiek konkurować w przestrzeni procesowej z posiadającymi zarówno zaplecze wiedzy informatycznej, jak i prawnej przedsiębiorstwami z branży nowoczesnych technologii²⁹.

Wadliwość

Zmodyfikowano także zakres wadliwości, a w szczególności zakres okoliczności, których ogół społeczeństwa ma prawo oczekiwać od produktu bezpiecznego. Możemy mówić o ich znacznym poszerzeniu, gdyż w miejsce dotychczasowych trzech zaproponowano aż 9 przesłanek. Dla systemów AI szczególne znaczenie mają przede wszystkim:

- zastosowanie produktu i jego niewłaściwe użycie;
- możliwość jego dalszego uczenia się po wprowadzeniu go na rynek lub do użytku;
- wpływ na produkt innych produktów stosowanych razem z produktem;

²⁴ *Ibidem*.

²⁵ *S. De Luca*, New Product Liability Directive. Briefing, [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2023\)739341](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)739341) (dostęp z 8.7.2023 r.).

²⁶ *S. Nawaz*, The Proposed EU AI Liability Rules: Ease or Burden?, <https://europeanlawblog.eu/2022/11/07/the-proposed-eu-ai-liability-rules-ease-or-burden/> (dostęp z 8.7.2023 r.) oraz *P. Hacker*, *op. cit.*, s. 44.

²⁷ Europejska Organizacja Konsumentów.

²⁸ *L. Bertuzzi*, The new liability rules for AI, <https://www.euractiv.com/section/digital/podcast/the-new-liability-rules-for-ai/> (dostęp z 8.7.2023 r.).

²⁹ Niektórzy przedstawiciele producentów wyrazili tożsame do powyższego stanowisko w trakcie konsultacji społecznych, przykładowo <https://ccianet.org/library/ccia-europe-position-paper-pld-revision/>, czy też w ramach wspólnego listu <https://ccianet.org/library/joint-industry-letter-on-the-pld-and-ai-directive/>.

- moment wprowadzenia do obrotu, oddania do użytku lub moment, w którym produkt przestał podlegać kontroli producenta;
- wymogi dotyczące bezpieczeństwa produktów, w tym wymogi w zakresie cyberbezpieczeństwa³⁰.

Jedną z podstawowych trudności z identyfikacją wadliwości w przypadku systemów AI jest ich możliwość nauki już po wprowadzeniu produktu na rynek. Do tej pory w przypadku powstania wady już po wprowadzeniu produktu do obrotu producent mógł bronić się na podstawie art. 7 lit. B, który wyłączał odpowiedzialność, w przypadku kiedy wada powodująca szkodę powstała po wprowadzeniu produktu do obrotu. Obecna koncepcja wymusza na każdej ze stron ocenę potencjalnych możliwości dalszego rozwoju urządzenia. Jest to znacząca zmiana, zwłaszcza pod kątem unikania przez programistów ewentualnej odpowiedzialności spowodowanej przez dalsze uczenie się algorytmu³¹. Kwestia nauki po wprowadzeniu do obrotu i przypisania odpowiedzialności jest sprawą o tyle praktyczną, że co jakiś czas pojawiają się w świadomości opinii publicznej sytuacje wpisujące się w zakres tego artykułu. Za przykład wskazywano chatbota Tay wyprodukowanego przez Microsoft, który w wyniku nauczania się zachowań innych użytkowników portalu Twitter zaczął publikować dyskryminujące posty³². W takim przypadku, na gruncie proponowanych zmian, podmiot gospodarczy musiałby wykazać, że posiada on możliwość reagowania na potencjalne zagrożenie, czy to maszynowo, czy też ręcznie³³.

Kolejnym znaczącym dla kwestii AI aspektem jest sytuacja, w której producent zachowuje kontrolę nad produktem już po wprowadzeniu go do obrotu lub oddaniu do użytku. W tym przypadku nie ma znaczenia, czy dany produkt będzie samodzielnie się rozwijał albo czy będą na niego wpływać inne urządzenia. Rola podmiotu gospodarczego przy takich okolicznościach rośnie, ponieważ jest on w stanie wpływać na sposób i kierunek działania swojego produktu. Jednocześnie zwraca się uwagę, że wraz ze wzrostem kontroli nad urządzeniem producent zyskuje także znaczący wpływ na rozwój ryzyka lub powstanie wady, dlatego dodanie tej okoliczności wydaje się prawidłowym rozwiązaniem³⁴.

Ostatnią z wprowadzonych okoliczności, która wpływa na dostosowanie ram odpowiedzialności do specyfiki systemów AI, jest wymóg zachowania bezpieczeństwa produktów, w tym cyberbezpieczeństwa. Przesłanka ta została wprowadzona głównie w celu ujednolicenia materii PLD z pozostałymi aktami i działaniami unijnymi, co należy ocenić pozytywnie, zwłaszcza pod kątem pewności prawa i zaufania dla unijnego prawodawstwa. W tym samym czasie co modyfikacja PLD procedowany jest bowiem wniosek dotyczący rozporządzenia w sprawie produktów maszynowych³⁵. Jednocześnie kwestia bezpieczeństwa, i fizycznego, i cyfrowego,

poruszona jest w ramach art. 32 RODO³⁶, art. 15 AI Act³⁷ oraz proponowana w rozporządzeniu Cyber Resilience Act (CRA)³⁸.

Da się zauważyć głosy, że PLD w swojej zmodernizowanej wersji nie odnosi się do jednej podstawowej kwestii. Z uwagi na specyficzny sposób podejmowania decyzji oraz oparcie się na dostarczonych danych systemy AI mogą popełniać błędy, których człowiek by nie popełnił³⁹. I analogicznie, mogą również unikać błędów typowych dla ludzi, co pozostaje w sprzeczności z zawartą w art. 6 ust. 1 PLD przesłanką wadliwości, czyli oczekiwaniami ogółu społeczeństwa⁴⁰. Wraz z narażeniem na niedostatecznie dostępne do analizy wady konstrukcyjne te dwie przesłanki mogą stanowić słaby punkt efektywnego przypisania wadliwości. Mimo tego zagrożenia można odnieść wrażenie, że kwestia prawidłowego określenia wadliwości systemu AI na gruncie treści PLD będzie w najbliższych latach obiektem zainteresowania doktryny⁴¹.

³⁰ Zob. art. 6 ust. 1 PLD

³¹ P. Hacker, *op. cit.*, s. 20.

³² A. Tenner, G. Chelous, Microsoft's AI Twitter bot goes dark after racist, sexist tweets. <https://www.reuters.com/article/us-microsoft-twitter-bot-idUSKCN0WQ2LA>; E. Hunt, Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter, The Guardian, 24.3.2016 r., www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter (dostęp z 8.7.2023 r.).

³³ P. Hacker, *op. cit.*, s. 20.

³⁴ P. Hacker, *op. cit.*, s. 20.

³⁵ Dz.Urz. UE L Nr 165, 29.6.2023 r., s. 1.

³⁶ Dz.Urz. UE L Nr 119, 4 maja 2016 r., s.1, dalej jako: RODO.

³⁷ Wniosek rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji COM/2021/206 (Akt w sprawie sztucznej inteligencji, AI Act).

³⁸ Wniosek rozporządzenie Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020.

³⁹ Za przykład wskazywany jest tu wypadek autonomicznego samochodu Tesla z maja 2016 r., który przy włączonym autopilocie uderzył w ciężarówkę w wyniku omyłkowego uznania jej za most. W wyniku tego wypadku zginął pasażer Tesli. W tym kontekście wypadek ten jest kluczowy, gdyż kierowca-człowiek nie jest w stanie pomylić ciężarówkę z mostem, a bazująca na niezinterpretowanych danych AI już tak. D. Shephardson, Tesla driver in fatal „Autopilot” crash got numerous warnings: U.S. government, <https://www.reuters.com/article/us-tesla-crash-idUSKBN19A2XC> (dostęp z 8.7.2023 r.).

⁴⁰ P. Hacker, *op. cit.*, s. 21.

⁴¹ P. Hacker opowiada się, a z czym należy się zgodzić – po przeanalizowaniu zarówno podejścia antropomorficznego, jak i nastawionego na AI – że optymalnym rozwiązaniem byłoby powiązanie systemów AI nie z oczekiwaniami konsumentów, lecz ze standardem technicznym, jaki wymagany jest dla danego sektora produktów. Dopiero w przypadku braku takich standardów proponuje on inne podejście – odnośnie do AI działającej na kształt człowieka (*infrahuman AI*) miałyby być to wzruszalne domniemanie wadliwości, natomiast w przypadku AI lepszej od ludzi (*suprahuman AI*) nie jest obecnie możliwe wskazanie optymalnego rozwiązania. W całości postuluje on jednak odejście od typowego dla aktualnej regulacji podejścia antropomorficznego, z uwagi na znaczne rozbieżności między sposobem działania ludzi i sztucznej inteligencji.

Zmiana podmiotowa – nowa kategoria podmiotu gospodarczego

Projektodawcy w ramach dostosowywania przepisów do realiów obecnej gospodarki zdecydowali się na rozszerzenie kategorii podmiotów, które mogą być pociągnięte do odpowiedzialności. Dotychczasowy termin producenta został zastąpiony obszerniejszym znaczeniowo terminem podmiotu gospodarczego, w ramach którego mieści się cały szereg podmiotów. Są to przede wszystkim producenci, ale także producenci części składowych, importer, dystrybutor, upoważniony przedstawiciel producenta czy dostawca usług realizacji zamówień⁴². Odpowiedzialność producenta (a nie producenta części składowej) rozciąga się także na takie szkody, które zostały wyrządzone w wyniku działania wadliwej części składowej, która została zintegrowana lub połączona z produktem pod jego kontrolą. W przypadku kiedy jakiś podmiot – czy to osoba fizyczna, czy prawna – dokona znaczącej modyfikacji poza kontrolą producenta, a następnie produkt ten zostanie wprowadzony na rynek lub oddany do użytku, to modyfikator będzie uznany za producenta, a co za tym idzie, będzie odpowiadał na tych samych zasadach. Dodanie kategorii modyfikatorów można odczytać jako wsłuchanie się w opinie przedstawione w trakcie konsultacji społecznych, co niewątpliwie jest dobrą praktyką.

Przewidziana została także sytuacja alternatywna, w której podmiot gospodarczy mający siedzibę w UE nie może być zidentyfikowany. W tej sytuacji możliwe jest dochodzenie roszczeń od każdego dystrybutora, ale po spełnieniu dwóch warunków. Po pierwsze, poszkodowany musi najpierw zwrócić się do tego dystrybutora z wnioskiem o udzielenie informacji na temat podmiotu gospodarczego lub własnego dystrybutora, a po drugie, dystrybutor w następstwie tego wniosku albo nie wskaże żadnego podmiotu gospodarczego, albo nie udzieli odpowiedzi w przeciągu miesiąca od jego otrzymania. Komisja trafnie zidentyfikowała zmianę okoliczności rynkowych i propozycję wielopoziomowej odpowiedzialności należałoby zaaprobować.

Proponowana dyrektywa zawiera w sobie kontynuację dotychczasowego podejścia dotyczącego sytuacji, kiedy za szkodę odpowiada więcej niż jedna osoba. Przedstawiciele doktryny zwrócili uwagę, że w praktyce systemy sztucznej inteligencji czy nawet poszczególne kody są przygotowywane i rozwijane przez jeden podmiot, a następnie implementowane do urządzenia i tam integrowane z oprogramowaniem z innego źródła⁴³. W takiej sytuacji każdy z podmiotów gospodarczych zaangażowanych w proces produkcyjny odpowiada solidarnie, jeśli ich działanie przyczyniło się do szkody. Kwestia ta została także poruszona w preambule do Dyrektywy w motywie 26 oraz motywie 40, gdzie podkreślano, że istotna jest możliwość wyegzekwowa-

nia odpowiedzialności od każdego z producentów danego przedmiotu. W przypadku kiedy producent zdecyduje się na włączenie do swojego produktu części, która pochodzi od innego producenta, poszkodowany powinien móc dochodzić odszkodowania albo od producenta końcowego, albo producenta części wadliwej. Decyzja o kontynuowaniu kształtowania relacji między podmiotami zaangażowanymi w proces w oparciu o zasadę odpowiedzialności solidarnej wydaje się korzystna, zwłaszcza – co silnie akcentowali twórcy – w świetle ochrony konsumenta⁴⁴. Potencjalny poszkodowany nie musi się bowiem zastanawiać na temat tego, w kierunku którego z producentów powinien kierować roszczenia, co w świetle złożoności i zaawansowania systemów AI wykorzystujących wiele części składowych może być szczególnie problematyczne.

Użytkownicy systemów AI mogą więc uzyskać dużo lepszą ochronę z uwagi na mnogość podmiotów, które mogą być pociągnięte do odpowiedzialności. Wątpliwości może jednak budzić kwestia efektywności tego rozwiązania, zwłaszcza mając na uwadze znaczne rozproszenie cyfrowego świata. W celu ułatwienia dochodzenia swoich roszczeń przewidziano wiele domniemań, które mają usprawnić cały ten proces.

Ujawnianie dowodów, czyli poprawa pozycji poszkodowanego

Znowelizowana PLD ma znacząco odbiegać pod względem formalnym od swojej poprzedniczki. Założenia te mają dotyczyć w szczególności trzech kwestii – ujawnienia dowodu, ciężaru dowodu i zwolnienia z odpowiedzialności.

Problem dostępności do dowodów wynika w znacznej mierze ze specyfiki produktów, w szczególności tych wykorzystujących sztuczną inteligencję. Takie cechy sztucznej inteligencji jak nieprzejrzyistość i złożoność sprawiają bowiem, że konsument, który nie ma profesjonalnej wiedzy z tej dziedziny (a czasami nawet to może być niewystarczające, jeśli produkt ma np. bardzo niszowy zakres zastosowania), nie jest w stanie dotrzeć samodzielnie do niezbędnych dla niego dowodów. Trudno bowiem stwierdzić, będąc przeciętnym konsumentem, w jaki sposób produkt opierający się na decyzjach algorytmów działa, a nawet gdyby poszkodowany był w posiadaniu takich informacji, to musiałby je jeszcze odpowiednio zinterpretować i zrozumieć. Taka dysproporcja narusza zasadę sprawiedliwego podziału ryzyka⁴⁵. Z tego powodu w art. 8 przewidziano, że państwa członkowskie mają zapewnić poszkodowanemu, który dochodzi roszczenia

⁴² Definicję tych terminów znajdziemy w art. 4 ust. 11–15.

⁴³ P. Hacker, *op.cit.*

⁴⁴ *Ibidem.*

⁴⁵ Zob. Motyw 30 Preambuły PLD.

przed sądem krajowym i który przedstawił fakty i dowody wystarczające do uzasadnienia wiarygodności roszczenia uzyskanie od powoda dowodów znajdujących się w jego posiadaniu.

Taka możliwość, dodatkowo zgodna z prawem krajowym, ma być ograniczona wyłącznie do tego co niezbędne i proporcjonalne. W trakcie oceny niezbędności i proporcjonalności powinno się brać pod uwagę interes wszystkich zainteresowanych stron, nie tylko bezpośrednio zaangażowanych w proces, ale także osób trzecich. Dodatkowo powinno się je ocenić pod kątem możliwości ujawnienia informacji poufnych i tajemnic przedsiębiorstwa, które zostały określone w art. 2 pkt 1 dyrektywy 2016/943⁴⁶.

Chociaż samo założenie wydaje się słuszne, gdyż z pewnością zapobiegnie nadmiernemu obciążeniu strony przeciwnej, to jednak w doktrynie dostrzeżono w nim błędy. Przede wszystkim – inaczej niż w przypadku AILD – uprawnienie to zostało przewidziane jedynie dla sytuacji, w których spór został już wszczęty przed sądem. Takie rozwiązanie może być problematyczne z praktycznego punktu widzenia, gdyż słusznie stwierdzono, że w wielu państwach członkowskich, w tym w Polsce, wniesienie sporu przed sąd wiąże się z uiszczeniem opłaty sądowej lub złożenia depozytu do sądu. Opłaty te zależne są od rodzaju sporu i rodzaju postępowania, zatem naturalne wydaje się przypuszczenie, że będą one wyższe w przypadku standardowego postępowania procesowego, w ramach którego miałoby nastąpić ujawnienie dowodów niż w przypadku postępowania przedprocesowego, którego głównym celem byłoby jedynie rozstrzygnięcie omawianej kwestii⁴⁷.

Co więcej, przepisy PLD przewidują jedynie ułatwienie dotyczące ujawnienia dowodów, natomiast nie została w żadnym stopniu poruszona kwestia późniejszej interpretacji zdobytych informacji⁴⁸. W takim przypadku na poszkodowanym spoczywa obowiązek znalezienia odpowiedniego podmiotu, który pomoże mu wykorzystać uzyskane dane do poparcia swojego roszczenia. Takie rozwiązanie nie dość, że może być problematyczne w sytuacji, w których dane pochodzą z zaawansowanych systemów AI, to dodatkowo może narazić występującego z roszczeniem na znaczne koszty ekspertyzy⁴⁹.

Ciężar dowodu i jego modyfikacja

W wypadku systemów AI ciężar dowodu może okazać się kluczowy, gdyż jego niewłaściwy rozkład spowoduje znaczną dysproporcję stron procesowych i w praktyce zablokuje możliwość udowodnienia swoich twierdzeń przez poszkodowanych. Dodatkowa trudność wynika z braku spójności przepisów poszczególnych państw członkowskich – raport Komisji wykazał, że różnice występują zarówno pomiędzy poszczególnymi państwami, jak i w ramach poszczególnych

państw w porządku wewnętrznym⁵⁰. To z kolei prowadzi do nierówności między poszkodowanymi, w zależności od ich obywatelstwa lub miejsca dochodzenia roszczenia. Dodatkowy rozwój IoT i AI spowodował, że aspekt wykazania dowodów zaczął być jeszcze bardziej istotny, a dla poszkodowanych – problematyczny. Jak zauważono, oprogramowanie może zawierać w sobie bardzo dużą, sięgającą kilku milionów linijek kodu, wśród których znalezienie szkody może być bardzo trudne, nawet z wykorzystaniem specjalistycznej wiedzy⁵¹. Do tego pojawia się problem łączenia się poszczególnych urządzeń w ekosystemy, wykorzystywania zewnętrznego oprogramowania oraz rozwoju algorytmu bazującego na samouczeniu⁵². Z powodu powyżej zasygnalizowanych problemów nie wzbudził zdziwienia fakt, że w treści modernizacji Dyrektywy zostały przewidziane nowe pomysły na regulację tej kwestii.

W przypadku nowelizacji PLD zdecydowano się na częściowe odwrócenie ciężaru dowodu. Dotychczasowe przepisy w znacznym stopniu obciążały poszkodowanego, na którym w całości spoczywał ciężar dowodów. Odbiór społeczny ta-

⁴⁶ Dz.Urz. UE L Nr 157, s. 1.

⁴⁷ P. Hacker, *op. cit.*, s. 27.

⁴⁸ Problem ten został poruszony w doktrynie w trakcie omawiania Rezolucji Parlamentu Europejskiego dotyczącego systemu odpowiedzialności cywilnej za sztuczną inteligencję (2020/2014(INL)), gdzie M. Świerczyński i Z. Więckowski rozważają pomysł powołania rzecznika AI, który, na wzór rzeczników patentowych, pomagałby poszkodowanym w efektywnym wykorzystaniu informacji dotyczących działania systemów AI, zob. M. Świerczyński, Z. Więckowski, *Sztuczna inteligencja w prawie międzynarodowym. Rekomendacje wybranych rozwiązań*, 2021.

⁴⁹ J. De Bruyne, O. Dheu, Ch. Ducuing, *op. cit.* – znaczne koszty zostały także dostrzeżone w czwartym raporcie dotyczącym PLD przez niektóre z władz krajowych, np. Bułgarii, Włoch, Maltę, Łotwy, Słowacji czy Szwecji https://www.eumonitor.eu/9353000/1/j4nvhdsc8bljza_j9vvik7m1c3gyxp/visw46u9zkzm (dostęp z 8.7.2023 r.).

⁵⁰ Czwarty raport dotyczący PLD, *op. cit.*, D. Fairgrieve, G. Howells, M. Pilgerstorfe, *The Product Liability Directive: Time to get Soft?*, *Journal of European Tort Law*, vol. 4, no. 1, 2013, s. 8-9 <https://doi.org/10.1515/jetl-2013-0001> oraz J. De Bruyne, O. Dheu, Ch. Ducuing, *The European Commission's Approach To Extra-Contractual Liability and AI – An Evaluation of the AI Liability Directive and the Revised Product Liability Directive*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4295676 (dostęp z 8.7.2023 r.) – dostrzeżono tam, że w przypadku niektórych państw, takich jak Francja, Włochy, Belgia czy Hiszpania wystarczające jest wykazanie, że produkt nie spełniał funkcji, do których był przeznaczony. W innych, np. w Niemczech czy Wielkiej Brytanii, należy precyzyjnie wskazać przeznaczenie rzeczy. D. Fairgrieve zwraca uwagę, że stan prawny w Wielkiej Brytanii bazował na przywołanych w Trzecim Raporcie Komisji wyrokach *Richardson v. London Rubber Company Products Limited* oraz *Foster v. Bosil*, w których sądy wymagały wykazania wady. Od tego czasu wydano jednak odmienne orzeczenie w sprawie *Alan Peter Ide v. ATB Sales Limited*, w którym Izba Cywilna Sądu Apelacyjnego wskazała, że nie jest wymagane wskazanie dokładnego mechanizmu powodującego wadę (wyrok ten nie został przez Komisję przywołany, jednak wniosek ten został wspomniany), D. Fairgrieve, G. Howells, M. Pilgerstorfe *op. cit.*

⁵¹ Ch. Wendehorst, Y. Duller, *Safety and Liability Related Aspects of Software*, <https://digital-strategy.ec.europa.eu/en/library/study-safety-and-liability-related-aspects-software> (dostęp z 8.7.2023 r.).

⁵² *Ibidem*.

kiego rozwiązania był jednak negatywny⁵³. Obecnie obowiązek „udowodnienia wadliwości produktu, poniesionej szkody oraz związku przyczynowego między wadliwością a szkodą” ma w dalszym stopniu spoczywać na osobie występującej z roszczeniem⁵⁴. W celu złagodzenia tych wymagań wprowadzono wiele domniemań.

Warto nadmienić, że projektodawcy zauważyli znaczną dysproporcję między poziomem wiedzy eksperckiej stron. Z tego powodu uznano, że sama złożoność techniczna lub naukowa powinna być określona przez sądy krajowe na podstawie indywidualnych przypadków, biorąc pod uwagę różne czynniki, np. charakter wykorzystywanej technologii, uczenie maszynowe czy złożony charakter przyczyny, którego udowodnienie wymagałoby wyjaśnienia przez wnioskodawcę wewnętrznego działania systemu AI. Powód w pozwie dotyczącym systemu sztucznej inteligencji powinien wnioskować, aby sąd rozstrzygnął o tym, że istnieją nadmierne trudności. W ten sposób od powoda nie wymaga się wyjaśnienia specyfiki systemu sztucznej inteligencji ani tego, w jaki sposób cechy te utrudniają ustalenie związku przyczynowego. Pozwany powinien mieć natomiast możliwość zakwestionowania wszystkich tych twierdzeń⁵⁵.

Wadliwość winy jest domniemana, jeśli wystąpi jedna z trzech przesłanek, przy czym nie muszą być one spełnione łącznie. Są to: brak dopełnienia obowiązku ujawnienia istotnych dowodów, jeśli wystąpi sytuacja z art. 8 ust. 1 PLD; stwierdzenie braku spełniania przez produkt obowiązkowych wymogów bezpieczeństwa oraz stwierdzenie, że szkoda wynika z „oczywistego nieprawidłowego działania produktu w trakcie użytkowania, którego można racjonalnie oczekiwać lub w zwykłych okolicznościach”⁵⁶.

Drugi z wymienionych warunków, a więc stwierdzenie niespełniania wymogów bezpieczeństwa oceniany jest w doktrynie pozytywnie, jako przykład zbliżania do siebie i integracji między sobą dwóch głównych filarów unijnej regulacji dotyczącej produktów, tj. przepisów dotyczących bezpieczeństwa i przepisów dotyczących odpowiedzialności⁵⁷.

Kolejnym krokiem jest domniemanie istnienia „związku przyczynowego między wadliwością produktu, a szkodą, w przypadku kiedy zostanie stwierdzone, że produkt jest wadliwy, a spowodowana szkoda zazwyczaj współwystępuje z tą wadą”. Problematyczne w tej sytuacji wydają się dwie kwestie. Po pierwsze, może dojść do sytuacji, w której poszkodowany będzie musiał wykorzystać wcześniej opisane domniemania. Domniemanie winy jest bowiem niezbędne do dokonania oceny wystąpienia związku przyczynowego. W przypadku kiedy występujący z roszczeniem nie będzie mógł skorzystać z pierwszego z domniemań do wykazania drugiego, zostanie on *de facto* pozbawiony możliwości obrony. Po drugie, przepisy nie wyjaśniają, co oznacza termin „zazwyczaj współwystępuje z daną wadą”. Proponuje się jednak, że określenie to odnosi się do wad, które przy zwykłym biegu wydarzeń mogą

doprowadzić do konkretnej szkody⁵⁸. Za takim stanowiskiem przemawia także treść motywu 33a Preambuły, w którym mowa jest o tym, że jeżeli szkoda oparta jest na znanych, istniejących już przypadkach, to powód powinien zostać zwolniony z obowiązku pełnego udowodnienia wystąpienia związku przyczynowego⁵⁹.

Zwolnienie z odpowiedzialności

W PLD przewidziano także pewne rozwiązania, które adresowane są do pozwanych. Tak samo jak oryginalna Dyrektywa, jej zmodernizowana wersja zawiera kilka okoliczności, które pozwalają podmiotom odpowiedzialnym zwolnić się od odpowiedzialności. Większość z nich została zasadniczo powtórzona, dlatego skupimy się na tych przesłankach, które mogą mieć szczególne znaczenie dla systemów AI.

Pierwszą z nich jest znana z oryginalnej wersji dyrektywy przesłanka późniejszego powstania wady, tzw. *later-defect defence*, zgodnie z którą podmioty gospodarcze nie ponoszą odpowiedzialności, jeśli wada nie istniała w momencie wprowadzenia produktu do obrotu lub udostępnienia do użytku albo powstała po tym momencie. Dotychczas kwestią bezsporną było założenie, że producenci są odpowiedzialni za te wady, które wynikają z tych działań, które można nazwać ich „sferą wpływów”⁶⁰. W doktrynie podnoszone były jednak głosy, że to zwolnienie staje się trudne do wyegzekwowania w przypadku szkód stworzonych przez systemy AI, które posiadają

⁵³ Badanie dokonane w trakcie ewaluacji PLD wykazało, że 53% nieudanych prób wystąpienia z roszczeniem wynikało z braku możliwości udowodnienia wadliwości lub związku przyczynowego między wadliwością a szkodą. Była to najczęstsza taka przyczyna. Komisja Europejska, Dyrekcja Generalna ds. Rynku Wewnętrznego, Przemysłu, Przedsiębiorczości i MSP, Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products: final report, <https://data.europa.eu/doi/10.2873/477640>. Również w trakcie konsultacji społecznych 95% przedstawicieli konsumentów i obywateli opowiedziało się za stanowiskiem, że ciężar dowodu ciążyący na poszkodowanym jest zbyt wysoki (wśród przedstawicieli branży było to jedynie 38%) – Uzasadnienie wniosku, s. 10.

⁵⁴ Obecnie takie rozwiązanie jest przewidziane na gruncie art. 4 PLD, chociaż ostatnimi laty jest ono uszczegółowiane przez orzecznictwo – np. w sprawie C-621/15 Sanofi Pasteur, ECLI:EU:C:2017:484.

⁵⁵ Zob. Motyw 34 Preambuły.

⁵⁶ W motywie 33 Preambuły PLD wskazano przykład ostatniej z wypisanych przesłanek – domniemanie to można porównać do sytuacji, w której w trakcie normalnego użytkowania wybuch szklana butelka. W takim wypadku nie miałoby sensu wykazywanie wadliwości, skoro nie budzi to żadnych wątpliwości.

⁵⁷ P. Hacker, *op. cit.*, s. 39; o wzmocnieniu tego związku świadczy także treść motywu 33 Preambuły PLD.

⁵⁸ Zdaniem P. Hackera takie stanowisko wynika z domniemań faktycznych charakterystycznych dla prawa cywilnego obecnie. Dodatkowo twierdzi on, że domniemanie to nie może zostać zastosowane, jeśli przeciętna osoba posiadająca wiedzę na temat konkretnej szkody nie spodziewała się tego konkretnego rodzaju szkody – *op. cit.*, s. 40.

⁵⁹ Zob. Motyw 33a Preambuły.

⁶⁰ J. Luzak, A Broken Notion: Impact of Modern Technologies on Product Liability, European Journal of Risk Regulation, Volume 11, Issue 3, s. 630–649, <https://doi.org/10.1017/err.2020.13> (dostęp z 8.7.2023 r.).

zdolność do późniejszego uczenia się⁶¹. Producenci mają jednak cały czas możliwość kontrolowania sprzętu i w razie potrzeby zmodyfikować lub nawet wyłączyć tę funkcję.

Projektodawcy również dostrzegli fakt, że producenci produktów cyfrowych są w stanie w zupełnie inny sposób i przez znacznie dłuższy czas kontrolować swój produkt, niż było to możliwe w przypadku producentów klasycznych, fizycznych produktów⁶². Uznali oni jednak, że taka kontrola następuje, jeżeli oprogramowanie czy powiązane usługi są dostarczane przez producenta lub za jego zgodą, bądź ma on wpływ na proces dostarczenia⁶³. Dlatego też zgodnie z art. 10 ust. 2, możliwość zastosowania zwolnienia z art. 10 ust. 1 lit. c jest wyłączona, w przypadku kiedy za wadę odpowiada: „powiązana usługa, oprogramowanie w tym aktualizacja lub modernizacja oraz brak aktualizacji lub modernizacji niezbędny do utrzymania bezpieczeństwa, a także znaczna modyfikacja”. Takie rozwiązanie, chociaż pozostawiające pole do dyskusji, może być ocenione pozytywnie, może ono w rezultacie zmusić producenta oprogramowania do dbania o to, by do produktów było dostarczone najnowsze i najbardziej bezpieczne oprogramowanie⁶⁴.

Dodatkowo ma to zapewnić odpowiedni poziom ochrony dla ewentualnych poszkodowanych, gdyż zakres przedmioty tego przepisu jest szeroki. Określenie „oprogramowanie i powiązane usługi” odnosi się także do tych algorytmów, które korzystają z samouczenia się lub uczenia maszynowego, a więc stanowią bazę dla systemów AI⁶⁵. Po raz kolejny zauważyć można powiązanie PLD z drugim filarem regulacji dotyczących produktów, a więc bezpieczeństwem. Świadczy o tym warunek wymieniony w lit. C – brak aktualizacji lub modernizacji niezbędny do utrzymania bezpieczeństwa. Wzajemna relacja tych dwóch aspektów jest bowiem pożądana ze względu na potrzebę harmonizacji przepisów dotyczących nowych technologii⁶⁶.

Ostatnią z przesłanek odnosi się do sytuacji, w której aktualny stan wiedzy naukowej lub technicznej w momencie wprowadzania produktu na rynek nie pozwala na wykrycie wadliwości (tzw. *development-defect defence* lub *state of the art defence*). Ważne jednak jest, co wywiedziono z judykatury, by oceny takiej dokonać w sposób obiektywny, uwzględniający wszelkie możliwe i dostępne źródła wiedzy, a nie oceniać tej kwestii przez pryzmat subiektywnych zdolności czy wiedzy danego podmiotu⁶⁷. Najwięcej kontrowersji wzbudzają systemy korzystające z samouczenia. Z powodu możliwości płynnej i ciągłej zmiany swych cech w zależności od dostarczonych do nich danych, w doktrynie podnosi się, że może powstać sytuacja, w której wada co prawda byłaby zawarta w produkcie od samego początku, jednak była ukryta i uaktywniła się dopiero po wprowadzeniu go do obrotu⁶⁸.

W stosunku do aktualnej wersji Dyrektywy zachodzi także zmiana, która niestety nie może zostać zaaprobowana i dotyczy możliwości wyłączenia tej przesłanki przez państwa

członkowskie⁶⁹. Niektóre państwa skorzystały z tego uprawnienia w całości, np. Finlandia i Luksemburg. Inne, takie jak Hiszpania i Francja wyłączyły zastosowanie tej przesłanki w stosunku do systemów wysokiego ryzyka⁷⁰. Takie działanie co prawda negatywnie wpływa na harmonizację przepisów pomiędzy poszczególnymi porządkami krajowymi, jednak jest ono wprowadzone w celu polepszenia sytuacji potencjalnego poszkodowanego⁷¹.

Podsumowanie

Powyższa analiza pokazuje, że w przypadku PLD wsłuchano się w głosy doktryny, która wyraźnie domagała się dostosowania przepisów tej dyrektywy do realiów obecnie funkcjonującego rynku. Zmiany te nie są jednak rewolucyjne. W głównej mierze oparto się na sprawdzonych już rozwiązaniach, a dodatkowo dodano i usunięto najbardziej problematyczne kwestie. Zmiany te są jednak wystarczające do objęcia zasięgiem PLD systemów sztucznej inteligencji.

Domniemania procesowe PLD oceniane są pozytywnie, gdyż wydają się niezbędne przy niejednokrotnie bardzo skomplikowanych systemach AI. Wśród podstawowego zarzutu, jaki można skierować do ujawniania dowodów, jest jego ograniczenie wyłącznie do etapu sądowego, w przeciwieństwie do AILD, która takie rozwiązanie przewiduje również dla „potencjalnych poszkodowanych”. Może to prowadzić do problemów z wyważeniem między efektywnością postępowania a ochroną poszkodowanych i to poprzez przechylenie się szali na niekorzyść strony powodowej. Brakuje też poruszenia kwestii wykorzystania ujawnionych danych na przykład poprzez stworzenie jakiegoś rodzaju organów pomagających poszkodowanym w efektywnym użyciu uży-

⁶¹ P. Hacker, *op. cit.*, s. 44.

⁶² Zob. Motyw 37 Preambuły PLD.

⁶³ *Ibidem*.

⁶⁴ P. Hacker zauważa jednak, że rozwiązanie ustanawiające pozakontraktowy obowiązek dostarczania aktualizacji, chociaż w przypadku PLD opiera się na odpowiednim balansie między zachętą do rozwoju a wymuszeniem rozwoju w wyniku przepisów prawa, to jednak nie powinno dotyczyć innych rodzajów aktualizacji niż te, które odnoszą się do bezpieczeństwa produktu. Uważa on bowiem, że to rynek najlepiej wymusza na producentach działanie w celu rozwoju swojego produktu. Wydaje się jednak, że jest to stanowisko błędne, gdyż nie można mieć żadnej pewności, że rynek i nacisk gospodarczy sprawi, że taka sytuacja zajdzie, w przeciwieństwie do regulacji prawnych, które znacznie ograniczają ewentualny brak działania producentów.

Także zob. J. De Bruyne, O. Dheu, Ch. Ducuing, *op. cit.*

⁶⁵ J. De Bruyne, O. Dheu, Ch. Ducuing, *op. cit.*

⁶⁶ *Ibidem*.

⁶⁷ Wyrok Trybunału z 29.5.1977 r. w sprawie C-300/95, Komisja Wspólnot Europejskich przeciwko Zjednoczonemu Królestwu Wielkiej Brytanii i Irlandii Północnej, ECLI:EU:C:1997:255.

⁶⁸ *Ibidem*.

⁶⁹ P. Hacker, *op. cit.*, s. 45; art. 15 ust. 1 lit. b dyrektywy 85/374/EWG.

⁷⁰ D. Fairgrieve, G. Howells, M. Pilgerstorfe, *op. cit.*

⁷¹ *Ibidem*.

skanych danych technicznych. Również sam zakres zastosowania, chociaż projektodawcy podkreślają, że tak nie będzie, może nakładać się z AILD, co może prowadzić do problemów dla poszkodowanych – zwłaszcza że AILD opiera się na zasadzie winy, więc jej użycie może być mniej korzystne⁷².

Najbliższe miesiące czy lata mogą okazać się kluczowe dla przyszłości sztucznej inteligencji w Europie, a znaczne przyspieszenie, głównie ilościowe, działania organów unijnych zdaje się tylko to potwierdzać. Nie zmienia to faktu, że jeszcze dużo czasu upłynie, zanim proponowane przepisy (w jakiegokolwiek formie) wejdą w życie – zwłaszcza że w najnowszej wersji zaproponowano wydłużenie terminu implementacji do 24 miesięcy. Upływ czasu ma bowiem duże znaczenie dla całego procesu legislacyjnego, gdyż na przestrzeni ostatnich kilku lat rzeczywistość diametralnie się zmieniła⁷³. Musimy także pamiętać, że rynek systemów AI zdaje się nie zwalniać tempa i obecnie trudno przewidzieć wszystkie kierunki jego rozwoju. Poprawnie skonstruowane przepisy odnośnie do tak

młodej i przyszłościowej branży, jaką jest sztuczna inteligencja, mogą mieć przecież wpływ nie tylko na realia europejskie, ale także – na co z pewnością liczą Projektodawcy – za pomocą tzw. efektu brukselskiego, na inne kontynenty⁷⁴. Pozostaje mieć jedynie nadzieję, że wypracowywane zmiany okażą się na tyle uniwersalne i skuteczne w praktyce, że będą mogły być powszechnie stosowane.

⁷² L. Bertuzzi, The new liability rules..., *op. cit.*

⁷³ Ch. Wendehorst, AI Liability in Europe: anticipating the EU AI Liability Directive, <https://www.adalovelaceinstitute.org/resource/ai-liability-in-europe/> (dostęp z 8.7.2023 r.).

⁷⁴ Termin ten, zaproponowany przez Anu Bradford oznacza wpływ, jaki unijna biurokracja może odegrać w świecie. W szczególności chodzi tu o wiodącą rolę i pokazanie kierunku, zwłaszcza odnośnie do wartości, w którą mogą podążać inne kraje. A. Bradford, The Brussels effect, Northwestern University Law Review, vol. 107, Nr 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770634# (dostęp z 8.7.2023 r.).

Słowa kluczowe: sztuczna inteligencja, odpowiedzialność cywilna, prawo cywilne, regulacje prawne sztucznej inteligencji, dyrektywa w sprawie odpowiedzialności za produkty wadliwe.

Proposal of modernisation for a Product Liability Directive and civil liability for artificial intelligence systems

This article aims to discuss the changes proposed by the European Union within the new project on the Product Liability Directive in the context of their use to claim civil liability for artificial intelligence. The author discusses issues relating to the initial stage of work on the proposal, i.e. the scope raised within public consultations. Subsequently, the author analyses crucial changes regarding the content of the Directive itself, including such points as the material scope of the act, personal applicability and procedural matters. Discussed changes mainly revolve around the expansion of the definitional framework and the use of appropriate legal constructions in order to adapt the regulations of the Directive to the specificity of claims related to the activity of artificial intelligence systems.

Key words: artificial intelligence, civil liability, civil law, artificial intelligence regulations, Product Liability Directive.

beckakademia SZKOLENIA ONLINE

Zarząd a nowoczesne technologie – praktyczne wskazówki dla managerów najwyższego szczebla

23 kwietnia 2024 r. • Prelegenci: Anna Matusiak-Wekiera, Ewa Mońdział



ZAPISY I SZCZEGÓŁY: akademia.beck.pl • 81 / 46 13 305

