KOMISJA
EUROPEJSKA

Bruksela, dnia 19.2.2020 r.
COM(2020) 64 final

SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO, RADY I EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO

Sprawozdanie na temat wpływu sztucznej inteligencji, internetu rzeczy i robotyki na bezpieczeństwo i odpowiedzialność

SPRAWOZDANIE NA TEMAT WPŁYWU SZTUCZNEJ INTELIGENCJI, INTERNETU RZECZY I ROBOTYKI NA BEZPIECZEŃSTWO I ODPOWIEDZIALNOŚĆ

1. Wprowadzenie

Sztuczna inteligencja (AI)[1], internet rzeczy (IoT)[2] i robotyka stworzą nowe możliwości i przyniosą korzyści naszemu społeczeństwu. Komisja uznaje znaczenie i potencjał tych technologii oraz potrzebę znacznych inwestycji w tych dziedzinach[3]. Zależy jej na tym, aby uczynić z Europy światowego lidera w dziedzinie AI, IoT i robotyki. Do osiągnięcia tego celu potrzebne są jasne i przewidywalne ramy prawne pozwalające sprostać wyzwaniom technologicznym.

1.1. Istniejące ramy bezpieczeństwa i odpowiedzialności

Ogólnym celem ram prawnych w zakresie bezpieczeństwa i odpowiedzialności jest zapewnienie, aby wszystkie produkty i usługi, w tym te łączące w sobie pojawiające się technologie cyfrowe, działały w sposób bezpieczny, niezawodny i spójny, a powstałe szkody były skutecznie naprawiane. Wysoki poziom bezpieczeństwa produktów i systemów łączących w sobie nowe technologie cyfrowe oraz solidne mechanizmy naprawy występujących szkód (tj. ramy odpowiedzialności) sprawiają, że konsumenci są lepiej chronieni. Przyczyniają się one również do budowania zaufania do tych technologii, co jest warunkiem wstępnym korzystania z nich przez przemysł i użytkowników. To z kolei wpłynie na zwiększenie konkurencyjności naszego przemysłu i przyczyni się do realizacji celów Unii[4]. Jasne ramy bezpieczeństwa i odpowiedzialności są szczególnie ważne w kontekście pojawiania się nowych technologii, takich jak AI, IoT i robotyka, dlatego że zapewnią ochronę konsumentów i pewność prawa dla przedsiębiorstw.

Unia posiada solidne i wiarygodne ramy regulacyjne w zakresie bezpieczeństwa i odpowiedzialności za produkt oraz solidny zestaw norm bezpieczeństwa. Uzupełnieniem tych ram regulacyjnych i norm są krajowe i niezharmonizowane przepisy w zakresie odpowiedzialności. Wszystkie one zapewniają dobrostan naszych obywateli w ramach jednolitego rynku i zachęcają do innowacji i rozwoju technologicznego. AI, IoT i robotyka zmieniają jednak właściwości wielu produktów i usług.

W komunikacie w sprawie sztucznej inteligencji dla Europy[5], przyjętym w dniu 25 kwietnia 2018 r., Komisja zapowiedziała, że przedstawi sprawozdanie, w którym oceni wpływ pojawiających się technologii cyfrowych na istniejące ramy bezpieczeństwa i odpowiedzialności. Celem niniejszego sprawozdania jest ustalenie i analiza szerszego

---

[1] Definicja sztucznej inteligencji grupy ekspertów wysokiego szczebla ds. AI znajduje się na stronie https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

[2] Definicja internetu rzeczy przedstawiona w zaleceniu Y.2060 Międzynarodowej Unii Telekomunikacyjnej, Biura Specyfikacji Telekomunikacyjnych znajduje się na stronie: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

[3] SWD(2016) 110, COM(2017) 9, COM(2018) 237 i COM(2018) 795.

[4] http://ec.europa.eu/growth/industry/policy_pl

[5] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM%3A2018%3A237%3AFIN.
W dokumencie roboczym służb Komisji towarzyszącym temu komunikatowi SWD(2018) 137 (https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137) wstępnie zidentyfikowano wyzwania dotyczące odpowiedzialności, powstające w kontekście pojawiających się technologii cyfrowych.

wpływu ram odpowiedzialności i bezpieczeństwa w odniesieniu do AI, IoT i robotyki oraz potencjalnych luk w tych ramach. Wytyczne przedstawione w niniejszym sprawozdaniu towarzyszące białej księdze w sprawie sztucznej inteligencji są przedmiotem dyskusji i stanowią część szerszych konsultacji z zainteresowanymi stronami. Sekcja dotycząca bezpieczeństwa opiera się na ocenie[6] dyrektywy w sprawie maszyn[7] oraz na współpracy z odpowiednimi grupami ekspertów[8]. Sekcja dotycząca odpowiedzialności opiera się na ocenie[9] dyrektywy w sprawie odpowiedzialności za produkt[10], wkładzie odpowiednich grup ekspertów[11] i kontaktach z zainteresowanymi stronami. Celem niniejszego sprawozdania nie jest przedstawienie dogłębnego przeglądu istniejących przepisów dotyczących bezpieczeństwa i odpowiedzialności. Skupia się ono na kluczowych kwestiach, które dotychczas określono.

1.2. Cechy AI, IoT i robotyki

AI, IoT i robotyka mają wiele cech wspólnych. Mogą one łączyć w sobie **łączność z internetem**, **autonomię** i **zależność od danych**, aby wykonywać zadania przy niewielkim poziomie kontroli lub nadzoru przez człowieka lub bez tego typu kontroli i nadzoru. Systemy wyposażone w AI posiadają również zdolność poprawy swoich osiągnięć, gdyż uczą się na podstawie zdobytego doświadczenia. Ich **złożoność** widać zarówno na przykładzie różnorodności podmiotów gospodarczych uczestniczących w **łańcuchu dostaw**, jak i wielorakości komponentów, części, oprogramowania, systemów lub usług tworzących razem nowe ekosystemy technologiczne. Do tego dochodzi ich **otwartość** na aktualizację i modernizację po wprowadzeniu do obrotu. Ogromne ilości wykorzystywanych danych, poleganie na algorytmach i **nieprzejrzystość** procesów podejmowania decyzji w zakresie AI utrudniają przewidywalność zachowania produktu opartego na AI i zrozumienie ewentualnych przyczyn szkód. Wreszcie łączność z internetem i otwartość mogą również być powodem narażenia produktów opartych na AI i IoT na **cyberzagrożenia**.

1.3. Możliwości stwarzane przez AI, IoT i robotykę

Zwiększenie zaufania użytkowników do pojawiających się technologii i ich akceptacji społecznej, udoskonalanie produktów, procesów i modeli biznesowych oraz pomaganie

---

6 SWD(2018) 161 final

7 Dyrektywa 2006/42/WE

8 Sieć na rzecz bezpieczeństwa konsumentów ustanowiona w dyrektywie 2001/95/WE w sprawie ogólnego bezpieczeństwa produktów, dyrektywie 2006/42/WE w sprawie maszyn oraz dyrektywie 2014/53/UE w sprawie urządzeń radiowych, grupy ekspertów złożone z przedstawicieli państw członkowskich, przemysłu i innych zainteresowanych stron, takich jak organizacje konsumenckie.

9 COM(2018) 246 final

10 Dyrektywa 85/374/EWG

11 Grupę ekspertów ds. odpowiedzialności i nowych technologii utworzono, aby zapewnić Komisji wiedzę fachową na temat stosowania dyrektywy w sprawie odpowiedzialności za produkty oraz krajowych przepisów dotyczących odpowiedzialności cywilnej oraz aby wspierać ją w opracowaniu wytycznych dotyczących ewentualnego dostosowania obowiązujących przepisów w odniesieniu do nowych technologii. Grupa ekspertów dzieli się z kolei na dwie podgrupy odpowiedzialne za tworzenie dyrektywy w sprawie odpowiedzialności za produkty i tworzenie nowych technologii, zob. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1.
Sprawozdanie podgrupy odpowiedzialnej za tworzenie nowych technologii na temat odpowiedzialności w zakresie sztucznej inteligencji i innych nowych technologii znajduje się na stronie: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

europejskim producentom w zwiększeniu wydajności to tylko niektóre z możliwości, jakie stwarza AI, IoT i robotyka.

Poza wzrostem produktywności i wydajności AI niesie także obietnicę umożliwienia ludziom rozwoju inteligencji, jaka do tej pory nie istniała, co utoruje drogę dla nowych odkryć i pomoże rozwiązać niektóre z największych współczesnych wyzwań: od leczenia chorób przewlekłych, przewidywania wystąpienia choroby lub zmniejszenia liczby ofiar śmiertelnych w wypadkach drogowych po przeciwdziałanie zmianie klimatu lub przewidywanie zagrożeń dla cyberbezpieczeństwa.

Technologie te mogą przynieść wiele korzyści, ponieważ poprawią bezpieczeństwo produktów, sprawiając, że będą one mniej podatne na pewne zagrożenia. Na przykład podłączone do internetu i zautomatyzowane pojazdy mogłyby poprawić bezpieczeństwo ruchu drogowego, ponieważ większość wypadków drogowych spowodowanych jest obecnie błędami ludzkimi[12]. Ponadto systemy IoT są zaprojektowane w taki sposób, aby odbierać i przetwarzać ogromne ilości danych z różnych źródeł. Zwiększony poziom informacji może służyć temu, aby produkty mogły samodzielnie dostosowywać się i w związku z tym stawać się bezpieczniejsze. Nowe technologie mogą przyczynić się do bardziej skutecznego wycofywania produktu od konsumentów, na przykład mogą ostrzegać użytkowników przed problemem związanym z bezpieczeństwem[13]. Jeżeli problem związany z bezpieczeństwem powstaje w trakcie korzystania z produktu podłączonego do internetu, producenci mogą bezpośrednio kontaktować się z użytkownikami, aby, z jednej strony, ostrzec użytkowników przed zagrożeniami, a z drugiej strony, aby w miarę możliwości bezpośrednio rozwiązywać problem, dostarczając na przykład aktualizację dotyczącą bezpieczeństwa. Na przykład podczas wycofywania jednego ze swoich urządzeń w 2017 r. producent smartfonów przeprowadził aktualizację oprogramowania polegającą na zredukowaniu do zera pojemności baterii wycofywanych telefonów[14], aby użytkownicy przestali korzystać z niebezpiecznych urządzeń.

Nowe technologie mogą ponadto przyczynić się do poprawy identyfikowalności produktów. Na przykład cechy łączności z internetem charakteryzujące IoT mogą umożliwić przedsiębiorstwom i organom nadzoru rynku śledzenie niebezpiecznych produktów oraz identyfikację ryzyka w łańcuchach dostaw[15].

Oprócz możliwości, jakie AI, IoT i robotyka mogą przynieść gospodarce i naszym społeczeństwom, mogą one również stwarzać ryzyko naruszenia chronionych prawem interesów, zarówno materialnych, jak i niematerialnych. W miarę poszerzania się zakresu stosowania ryzyko wystąpienia takiej szkody będzie się zwiększać. W tym kontekście istotne jest zbadanie, czy i w jakim stopniu obecne ramy prawne dotyczące bezpieczeństwa i odpowiedzialności nadal spełniają swój cel, jakim jest ochrona użytkowników.

---

[12] Szacuje się, że około 90 % wypadków drogowych spowodowanych jest błędami ludzkimi. Zob. sprawozdanie Komisji „Ratowanie życia: zwiększanie bezpieczeństwa samochodowego w UE” (COM(2016) 0787 final).

[13] Na przykład kierowca samochodu może zostać ostrzeżony, że powinien zwolnić, gdyby zbliżał się do miejsca wypadku.

[14] OECD (2018), „Measuring and maximising the impact of product recalls globally: OECD workshop report” (Pomiary i maksymalizacja wpływu wycofywania produktów z rynku w skali globalnej: sprawozdanie OECD z warsztatów), *OECD Science, Technology and Industry Policy Papers*, No. 56, OECD Publishing, Paryż, https://doi.org/10.1787/ab757416-en.

[15] OECD (2018), „Enhancing product recall effectiveness globally: OECD workshop report” (Poprawa skuteczności wycofywania produktów z rynku w skali globalnej: sprawozdanie OECD z warsztatów), *OECD Science, Technology and Industry Policy Papers*, No. 58, OECD Publishing, Paryż, https://doi.org/10.1787/ef71935c-en.

2. Bezpieczeństwo

W komunikacie Komisji na temat „Budowania zaufania do sztucznej inteligencji ukierunkowanej na człowieka" stwierdzono, że ***systemy SI powinny być bezpieczne z założenia, a bezpieczeństwo należy uwzględniać na etapie ich projektowania, aby zagwarantować, że są one bezpieczne w sposób możliwy do sprawdzenia na każdym etapie,*** *z uwzględnieniem* ***bezpieczeństwa fizycznego i psychicznego*** *wszystkich zainteresowanych*[16].

Celem oceny przedstawionych w niniejszej sekcji unijnych przepisów dotyczących bezpieczeństwa produktów jest analiza, czy obecne unijne ramy prawne zawierają odpowiednie elementy w celu zapewnienia, by w szczególności pojawiające się technologie i systemy oparte na AI były bezpieczne z założenia, a bezpieczeństwo było uwzględniane na etapie ich projektowania.

Niniejsze sprawozdanie dotyczy głównie dyrektywy w sprawie ogólnego bezpieczeństwa produktów[17] oraz zharmonizowanych przepisów dotyczących produktów, które są zgodne z zasadami horyzontalnymi „nowego podejścia"[18] lub „nowych ram prawnych" (dalej „unijne przepisy lub ramy dotyczące bezpieczeństwa produktów")[19]. Przepisy horyzontalne zapewniają spójność zasad sektorowych dotyczących bezpieczeństwa produktów.

Celem unijnych przepisów dotyczących bezpieczeństwa produktów jest zapewnienie, aby produkty wprowadzane na unijny rynek spełniały wysokie wymagania w zakresie zdrowia, bezpieczeństwa i ochrony środowiska oraz aby takie produkty mogły być przedmiotem swobodnego obrotu w całej Unii. Uzupełnieniem przepisów sektorowych[20] jest dyrektywa w sprawie ogólnego bezpieczeństwa produktów[21], zgodnie z którą wszystkie produkty konsumpcyjne, nawet jeśli nie zostały uregulowane unijnymi przepisami sektorowymi, mają być bezpieczne. Zasady bezpieczeństwa są uzupełnione o nadzór rynku i uprawnienia przyznane organom krajowym na mocy rozporządzenia w sprawie nadzoru rynku[22] oraz dyrektywy w sprawie ogólnego bezpieczeństwa produktów[23]. W sektorze transportu istnieją dodatkowe przepisy unijne i krajowe dotyczące dopuszczenia do eksploatacji pojazdu silnikowego[24], statku powietrznego lub statku wodnego, a także jasne zasady dotyczące

---

[16] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów na temat „Budowania zaufania do sztucznej inteligencji ukierunkowanej na człowieka", Bruksela, dnia 8.4.2019 r., COM(2019) 168 final.

[17] Dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 r. w sprawie ogólnego bezpieczeństwa produktów (Dz.U. L 11 z 15.1.2002, s. 4).

[18] Dz.U. C 136 z 4.6.1985, s. 1.

[19] Rozporządzenie (WE) nr 2008/765 i decyzja Komisji (WE) nr 2008/768.

[20] Zbiór ten nie obejmuje unijnych przepisów dotyczących transportu i samochodów.

[21] Dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 r. w sprawie ogólnego bezpieczeństwa produktów (Dz.U. L 11 z 15.1.2002, s. 4).

[22] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93, Dz.U. L 218 z 13.8.2008, s. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj, oraz, począwszy od 2021 r., rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011, Dz.U. L 169 z 25.6.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/1020/oj

[23] Art. 8 ust. 1 lit. b) i art. 8 ust. 3 dyrektywy w sprawie ogólnego bezpieczeństwa produktów

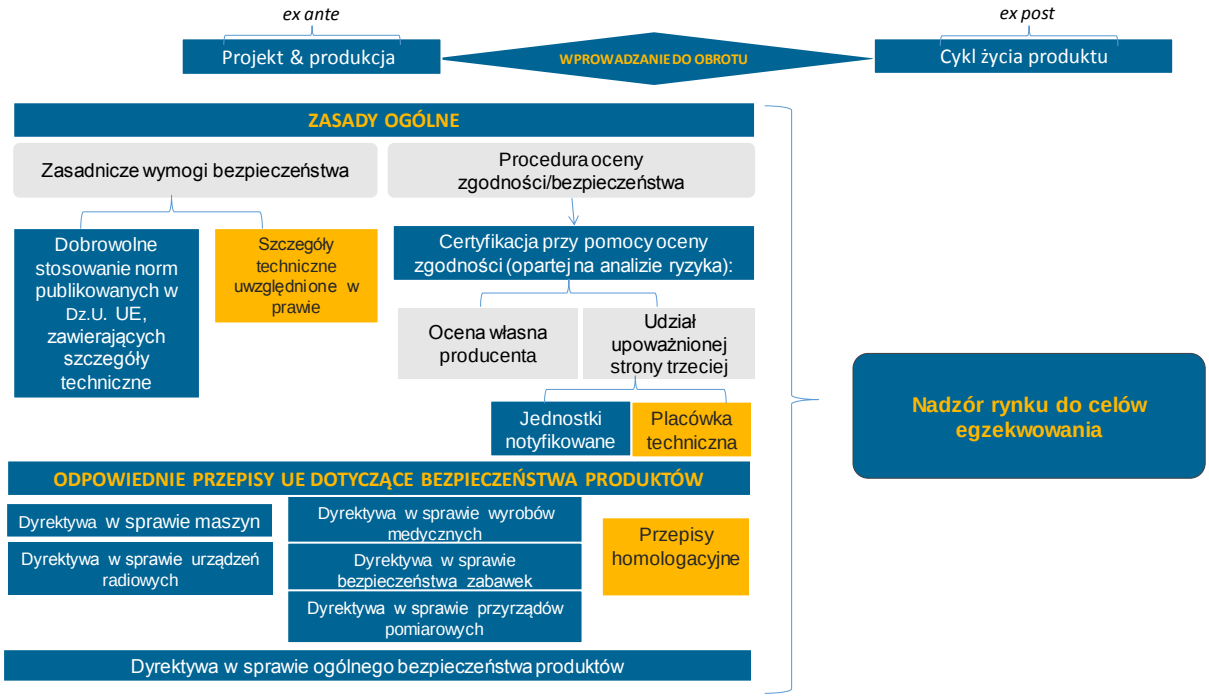
[24] Na przykład dyrektywa 2007/46/WE – homologacja pojazdów silnikowych i ich przyczep oraz układów, komponentów i oddzielnych zespołów technicznych przeznaczonych do tych pojazdów, oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/858 z dnia 30 maja 2018 r. w sprawie homologacji i nadzoru rynku pojazdów silnikowych i ich przyczep oraz układów, komponentów i oddzielnych zespołów

bezpieczeństwa podczas eksploatacji, obejmujące zadania dla operatorów oraz zadania dla organów w zakresie nadzoru.

Zasadniczym elementem unijnych przepisów dotyczących bezpieczeństwa produktów jest również normalizacja europejska. Ze względu na globalny charakter cyfryzacji i pojawiających się technologii cyfrowych współpraca międzynarodowa w zakresie normalizacji ma szczególne znaczenie dla konkurencyjności przemysłu europejskiego.

Dużą część unijnych ram dotyczących bezpieczeństwa produktów opracowano, zanim jeszcze pojawiły się technologie cyfrowe, takie jak AI, IoT czy robotyka. Dlatego też nie zawsze zawierają one przepisy wyraźnie odnoszące się do nowych wyzwań i zagrożeń związanych z pojawiającymi się technologiami. Zważywszy na fakt, że istniejące ramy dotyczące bezpieczeństwa produktów są neutralne pod względem technicznym, nie oznacza to jednak, że nie miałyby one zastosowania do produktów wykorzystujących te technologie. Późniejsze akty ustawodawcze, które wchodzą w zakres tych ram, na przykład w sektorze wyrobów medycznych lub samochodów osobowych, wyraźnie uwzględniają niektóre aspekty pojawienia się technologii cyfrowych, takich jak np. zautomatyzowane decyzje, oprogramowanie jako oddzielny produkt i łączność z internetem.

Przesłanki leżące u podstaw obecnych unijnych przepisów dotyczących bezpieczeństwa produktów[25]



Poniżej przedstawiono wyzwania związane z pojawiającymi się technologiami, na jakie wystawione są unijne ramy bezpieczeństwa produktów.

Łączność z internetem jest podstawową cechą stale rosnącej liczby produktów i usług. Ta cecha stanowi wyzwanie dla tradycyjnie pojmowanego bezpieczeństwa, ponieważ łączność

technicznych przeznaczonych do tych pojazdów, zmieniające rozporządzenie (WE) nr 715/2007 i (WE) nr 595/2009 oraz uchylające dyrektywę 2007/46/WE

[25] Grafika nie obejmuje wymogów w zakresie przepisów dotyczących cyklu życia produktu, tj. użytkowania i konserwacji i przedstawiono ją wyłącznie celem ilustracji.

z internetem może bezpośrednio zagrażać bezpieczeństwu samego produktu oraz pośrednio, w przypadku ataku hakerskiego, prowadząc do zagrożeń dla bezpieczeństwa i wpływając na bezpieczeństwo użytkowników.

Dobrym przykładem jest tutaj zgłoszenie w unijnym systemie wczesnego ostrzegania dokonane przez Islandię dotyczące inteligentnego zegarka dla dzieci[26]. Produkt ten nie wyrządziłby bezpośredniej szkody dziecku noszącemu ten zegarek, ale ponieważ nie posiada on minimalnego poziomu bezpieczeństwa, może być łatwo wykorzystany jako narzędzie umożliwiające dostęp do dziecka. Ponieważ jedną z zamierzonych funkcji tego produktu jest zapewnienie bezpieczeństwa dzieciom dzięki lokalizacji, konsument oczekuje, że produkt ten nie będzie stanowił zagrożenia dla bezpieczeństwa dzieci, gdyż każdy może je namierzyć albo się z nimi skontaktować.

Innym przykładem jest zgłoszenie dokonane przez Niemcy w odniesieniu do samochodu osobowego[27]. Radio znajdujące się w pojeździe może mieć pewne luki w zabezpieczeniach oprogramowania umożliwiające osobom trzecim nieuprawniony dostęp do wzajemnie połączonych systemów sterowania w takim pojeździe. Gdyby luki w zabezpieczeniach oprogramowania zostały wykorzystane w złej wierze przez osobę trzecią, mogłoby dojść do wypadku drogowego.

Zastosowania przemysłowe mogą być również narażone na cyberzagrożenia mające wpływ na bezpieczeństwo osób na większą skalę, jeżeli takie zastosowania nie posiadają wymaganego poziomu bezpieczeństwa. Przykładem mogą być cyberataki na krytyczne systemy sterowania zakładu przemysłowego w celu spowodowania wybuchu, który może spowodować ofiary śmiertelne.

Unijne przepisy dotyczące bezpieczeństwa produktów nie przewidują z zasady obowiązkowych zasadniczych wymogów szczegółowo ujętych w kontekście cyberzagrożeń mających wpływ na bezpieczeństwo użytkowników. Istnieją jednak przepisy dotyczące aspektów bezpieczeństwa w rozporządzeniu w sprawie wyrobów medycznych[28], dyrektywie w sprawie przyrządów pomiarowych[29], dyrektywie w sprawie urządzeń radiowych[30] lub w przepisach dotyczących homologacji typu całego pojazdu[31]. Akt o cyberbezpieczeństwie[32] ustanawia dobrowolne ramy certyfikacji cyberbezpieczeństwa dla produktów, usług i procesów w zakresie technologii informacyjno-komunikacyjnych (ICT), a odpowiednie unijne przepisy dotyczące bezpieczeństwa produktów ustanawiają obowiązkowe wymogi.

Ryzyko utraty łączności z internetem, jakie stwarzają nowe technologie cyfrowe, może ponadto pociągać za sobą ryzyko związane z bezpieczeństwem. Na przykład jeżeli

[26] Zgłoszenie w systemie RAPEX dokonane przez Islandię opublikowane na unijnej stronie internetowej „Safety Gate" (A12/0157/19)

[27] Zgłoszenie w systemie RAPEX dokonane przez Niemcy opublikowane na unijnej stronie „Safety Gate" (A12/1671/15)

[28] Rozporządzenie (UE) 2017/745 w sprawie wyrobów medycznych

[29] Dyrektywa 2014/32/UE odnosząca się do udostępniania na rynku przyrządów pomiarowych

[30] Dyrektywa 2014/53/UE w sprawie urządzeń radiowych

[31] Dyrektywa 2007/46/WE — homologacja pojazdów silnikowych i ich przyczep oraz układów, części i oddzielnych zespołów technicznych przeznaczonych do tych pojazdów. Ze skutkiem od dnia 1 września 2020 r. dyrektywa ta zostanie uchylona i zastąpiona rozporządzeniem (UE) 2018/858 w sprawie homologacji i nadzoru rynku pojazdów silnikowych i ich przyczep oraz układów, komponentów i oddzielnych zespołów technicznych przeznaczonych do tych pojazdów, zmieniającym rozporządzenie (WE) nr 715/2007 i (WE) nr 595/2009 oraz uchylającym dyrektywę 2007/46/WE.

[32] Rozporządzenie (UE) 2019/881

podłączony do internetu alarm pożarowy traci łączność, może nie ostrzec użytkownika w razie pożaru.

Kwestia bezpieczeństwa podnoszona w obecnych unijnych przepisach dotyczących bezpieczeństwa produktów jest celem polityki publicznej. Koncepcja bezpieczeństwa wiąże się ze stosowaniem produktu i ryzykiem, np. mechanicznym, elektrycznym itp., któremu należy zaradzić, aby zapewnić bezpieczeństwo produktu. Należy zauważyć, że w zależności od aktu prawnego w ramach unijnych przepisów dotyczących bezpieczeństwa produktów pojęcie zastosowania produktu obejmuje nie tylko przeznaczenie, ale również przewidywalne zastosowanie, a w niektórych przypadkach, np. w dyrektywie w sprawie maszyn33, nawet racjonalnie przewidywalne niewłaściwe zastosowanie.

Pojęcie bezpieczeństwa w obecnych unijnych przepisach dotyczących bezpieczeństwa produktów jest zgodne z rozszerzonym pojęciem bezpieczeństwa dotyczącym ochrony konsumentów i użytkowników. Dlatego pojęcie bezpieczeństwa produktów obejmuje ochronę przed wszelkimi rodzajami ryzyka stwarzanego przez produkt, obejmującymi nie tylko ryzyko mechaniczne, chemiczne, elektryczne, ale również cyberryzyko oraz ryzyko związane z utratą przez urządzenia łączności z internetem.

Można rozważyć jednoznaczne przepisy w tej kwestii jeżeli chodzi o zakres odpowiednich aktów prawnych Unii, aby zapewnić lepszą ochronę użytkowników i większą pewność prawa.

Autonomia[34] jest jedną z głównych cech AI. Niezamierzone rezultaty będące skutkiem AI mogą wyrządzić szkodę użytkownikom i osobom narażonym.

W zakresie, w jakim przyszłe „zachowanie" produktów opartych na AI może zostać z góry określone w drodze oceny ryzyka przeprowadzonej przez producenta przed wprowadzeniem produktów do obrotu, unijne ramy dotyczące bezpieczeństwa produktów nakładają już na producentów obowiązek uwzględniania w ocenie ryzyka „zastosowania"[35] produktów przez cały okres ich użytkowania. Przewidują one również, że producenci muszą dostarczać użytkownikom instrukcje i informacje na temat bezpieczeństwa lub ostrzeżenia[36]. W tym kontekście dyrektywa w sprawie urządzeń radiowych[37] nakłada na przykład na producenta obowiązek umieszczania instrukcji zawierających informacje na temat sposobu korzystania z urządzenia radiowego zgodnie z jego przeznaczeniem.

W przyszłości mogą wystąpić również sytuacje, kiedy nie będzie można z wyprzedzeniem określić wszystkich rezultatów działania systemów opartych na AI. W takiej sytuacji ocena

33 Dyrektywa 2006/42/WE w sprawie maszyn

34 Produkty oparte na AI mogą wprawdzie działać autonomicznie przez postrzeganie środowiska i bez konieczności stosowania z góry określonych instrukcji, ich zachowanie jest jednak ograniczone celem, jakiemu mają one służyć, i innymi istotnymi decyzjami w zakresie projektu podjętymi przez ich projektantów.

35 W unijnych przepisach dotyczących bezpieczeństwa produktów producenci przeprowadzają ocenę ryzyka na podstawie przeznaczenia produktu, przewidywalnego zastosowania lub racjonalnie przewidywalnego niewłaściwego zastosowania.

36 Decyzja Parlamentu Europejskiego i Rady 768/2008/WE z dnia 9 lipca 2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylająca decyzję Rady 93/465/EWG, Dz.U. L 218 z 13.8.2008, s. 82. Art. R2.7 załącznika I brzmi: „Producenci zapewniają dołączenie do produktu instrukcji obsługi oraz dostarczenie informacji na temat bezpieczeństwa w języku łatwo zrozumiałym dla konsumentów i innych użytkowników końcowych, wskazanym przez zainteresowane państwo członkowskie."

37 Art. 10 ust. 8 dotyczący instrukcji dla użytkownika końcowego i załącznika VI odnoszącego się do deklaracji zgodności UE

ryzyka przeprowadzona przed wprowadzeniem produktu do obrotu może już nie odzwierciedlać zastosowania, funkcjonowania lub zachowania produktu. W takich przypadkach, kiedy przeznaczenie, pierwotnie przewidziane przez producenta, zostało zmienione[38] w wyniku autonomicznego zachowania i naruszona została zgodność z wymogami bezpieczeństwa, można uznać, że konieczne jest poddanie produktu samouczącego się ponownej ocenie[39].

Zgodnie z obecnymi ramami, w przypadku gdy producenci zorientują się, że dany produkt stwarza w trakcie swojego cyklu życia zagrożenie dla bezpieczeństwa, są oni już teraz zobowiązani niezwłocznie poinformować o tym właściwe organy i podjąć działania zapobiegające zagrożeniu dla użytkowników[40].

Oprócz oceny ryzyka przeprowadzonej przed wprowadzeniem produktu do obrotu można by wprowadzić nową procedurę oceny ryzyka, w przypadku gdy produkt podlega istotnym zmianom w trakcie cyklu życia, np. gdy wprowadza się do niego nową funkcję, której producent nie przewidział we wstępnej ocenie ryzyka. Ocena ta powinna się koncentrować na tym, jak autonomiczne zachowanie produktu przez cały jego cykl życia wpływa na bezpieczeństwo. Ocenę ryzyka powinien przeprowadzać właściwy podmiot gospodarczy. Odpowiednie unijne akty prawne mogłyby ponadto wprowadzać wobec producentów zaostrzone wymogi dotyczące instrukcji i ostrzeżeń dla użytkowników.

Podobne oceny ryzyka są już wymagane w przepisach dotyczących transportu[41]; na przykład w przepisach dotyczących transportu kolejowego, w przypadku gdy pojazd kolejowy jest modyfikowany po jego certyfikacji, na autora zmiany nakłada się obowiązek przeprowadzenia szczególnej procedury, a także określone są jasne kryteria w celu ustalenia, czy konieczne jest informowanie właściwego organu.

Możliwość samodzielnego uczenia się przez produkty i systemy oparte na AI może umożliwić maszynie podejmowanie decyzji, które odbiegają od tego, co zostało pierwotnie zamierzone przez producentów, i w konsekwencji od tego, czego oczekują użytkownicy. Rodzi to pytania o kwestię kontroli przez człowieka, tak aby ludzie mogli decydować, w jaki sposób powierzać – o ile w ogóle – podejmowanie decyzji produktom i systemom opartym na

[38] Jak dotąd pojęcie „samouczenie się” w kontekście AI jest stosowane głównie po to, aby wskazać, że maszyny są zdolne do uczenia się podczas szkolenia ich; nie jest jednak wymagane, aby po ich uruchomieniu maszyny oparte na AI nadal się uczyły; przeciwnie, zwłaszcza w dziedzinie opieki zdrowotnej maszyny oparte na AI zwykle przestają się uczyć po pomyślnym zakończeniu szkolenia. W związku z tym na tym etapie autonomiczne zachowanie będące wynikiem systemów opartych na AI nie oznacza, że produkt wykonuje zadania nieprzewidziane przez projektantów.

[39] Jest to zgodne z sekcją 2.1 „Niebieskiego przewodnika – wdrażanie unijnych przepisów dotyczących produktów” z 2016 r.

[40] Art. 5 dyrektywy 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 r. w sprawie ogólnego bezpieczeństwa produktów.

[41] W przypadku jakiejkolwiek zmiany w systemie kolejowym, która może mieć wpływ na bezpieczeństwo (np. zmiany techniczne, operacyjne ale także zmiany organizacyjne, które mogą mieć wpływ na proces eksploatacji lub utrzymania), proces, który należy stosować, opisano w załączniku I do rozporządzenia wykonawczego Komisji (UE) 2015/1136 (Dz.U. L 185 z 14.7.2015, s. 6).
W przypadku „znaczącej zmiany” niezależna „jednostka oceniająca” powinna przedstawić wnioskodawcy takiej zmiany sprawozdanie w sprawie oceny bezpieczeństwa (jednostką oceniającą może być krajowy organ ds. bezpieczeństwa lub inny organ kompetentny pod względem technicznym).
Po przeprowadzeniu analizy ryzyka wnioskodawca będzie stosował odpowiednie środki w celu ograniczenia ryzyka (jeżeli wnioskodawca jest przedsiębiorstwem kolejowym lub zarządcą infrastruktury, stosowanie rozporządzenia jest częścią systemu zarządzania bezpieczeństwem, którego stosowanie nadzoruje krajowy organ ds. bezpieczeństwa).

AI, aby osiągnąć wybrane przez człowieka cele[42]. Istniejące unijne przepisy dotyczące bezpieczeństwa produktów nie odnoszą się wyraźnie do nadzoru przez człowieka w kontekście samouczących się produktów i systemów opartych na AI[43].

W odpowiednich aktach prawnych Unii można by przewidzieć, w charakterze zabezpieczenia, szczegółowe wymogi w zakresie nadzoru przez człowieka od etapu koncepcji produktu przez cały cykl życia produktów i systemów opartych na AI.

Przyszłe „zachowanie" zastosowań opartych na AI może stwarzać **ryzyko dla zdrowia psychicznego**[44] użytkowników, na przykład wskutek ich współpracy z robotami humanoidalnymi i systemami opartymi na AI w domu lub w środowisku pracy. W tym względzie obecnie pojęcie bezpieczeństwa stosuje się zasadniczo w odniesieniu do postrzeganego przez użytkownika zagrożenia powstania szkód materialnych, które może pochodzić ze strony nowej technologii cyfrowej. Jednocześnie bezpieczne produkty zdefiniowano w unijnych ramach prawnych jako produkty, które nie stwarzają żadnego zagrożenia lub jedynie minimalne zagrożenie dla zdrowia i bezpieczeństwa ludzi. Powszechnie uznaje się, że definicja zdrowia obejmuje zarówno pomyślność fizyczną, jak i umysłową. Zagrożenia dla zdrowia psychicznego należy jednak wyraźnie uwzględnić w pojęciu bezpieczeństwa produktów zawartym w ramach prawnych.

Autonomia nie powinna na przykład powodować nadmiernego stresu i poczucia dyskomfortu przez dłuższy okres ani szkodzić zdrowiu psychicznemu. W tym względzie za czynniki, które pozytywnie wpływają na poczucie bezpieczeństwa osób starszych[45], uważa się: utrzymywanie zapewniających poczucie bezpieczeństwa kontaktów z pracownikami służby zdrowia, poczucie kontroli nad codziennymi czynnościami oraz bycie informowanym o dotyczących ich aspektach życia. Producenci robotów, które wchodzą w interakcje ze starszymi osobami, powinni wziąć pod uwagę wspomniane czynniki, aby zapobiegać zagrożeniom dla zdrowia psychicznego.

Stosowne przepisy UE mogłyby jednoznacznie nakładać na producentów, między innymi, robotów humanoidalnych opartych na AI, jasny obowiązek uwzględniania niematerialnych szkód, jakie ich produkty mogą powodować u użytkowników, w szczególności użytkowników podatnych na zagrożenia, takich jak osoby starsze w systemie ochrony zdrowia.

Inną istotną cechą produktów i systemów opartych na AI jest **zależność od danych**. Dokładność i istotność danych są niezbędne, aby zapewnić, by decyzje podejmowane przez systemy i produkty oparte na AI były zgodne z zamierzeniem producenta.

Unijne przepisy dotyczące bezpieczeństwa produktów nie odnoszą się wyraźnie do zagrożeń dla bezpieczeństwa wynikających z błędnych danych. Zależnie jednak od „zastosowania"

---

[42] Zalecenia polityczne i inwestycyjne dotyczące wiarygodnej AI (ang. *Policy and Investment Recommendations for Trustworthy AI*), grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji, czerwiec 2019 r.

[43] Nie wyklucza to jednak, że w danej sytuacji konieczny może być nadzór ze względu na niektóre z istniejących bardziej ogólnych obowiązków dotyczących wprowadzania produktu do obrotu.

[44] Konstytucja WHO, pierwszy punktor: „Zdrowie jest stanem zupełnej pomyślności fizycznej, umysłowej i społecznej, a nie jedynie brakiem choroby lub ułomności." (https://www.who.int/about/who-we-are/constitution)

[45] Roboty społeczne: technologiczne, społeczne i etyczne aspekty interakcji między ludźmi a robotem humanoidalnym (ang. *Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction)*, s. 237–264, Neziha Akanalin, Annica Kristethersson i Amy Lutur, lipiec 2019 r.

produktu producenci powinni przewidzieć na etapie koncepcji i testowania dokładność danych i ich istotność dla funkcji bezpieczeństwa.

Na przykład system oparty na AI opracowany w celu wykrywania konkretnych przedmiotów może mieć trudności z rozpoznawaniem przedmiotów przy złym oświetleniu, dlatego też projektanci powinni uwzględnić dane pochodzące z badań produktu zarówno w warunkach odpowiedniego, jak i słabego oświetlenia.

Inny przykład dotyczy robotów rolniczych, takich jak roboty do zbierania owoców. Zadaniem takich robotów jest rozpoznawanie i lokacja dojrzałych owoców na drzewach lub na ziemi. Wprawdzie dzięki wykorzystywanym algorytmom już teraz poziom skuteczności klasyfikacji wynosi ponad 90 %, jednak braki w zbiorach danych wykorzystywanych przez algorytmy mogą spowodować, że roboty podejmą niewłaściwą decyzję, w wyniku której zwierzę lub osoba zostaną zranione.

Pojawia się pytanie, czy unijne przepisy dotyczące bezpieczeństwa produktów powinny zawierać szczegółowe wymogi w zakresie zapobiegania zagrożeniom dla bezpieczeństwa, jakie wiążą się z błędnymi danymi na etapie koncepcji, oraz mechanizmy zapewniające utrzymanie jakości danych w trakcie całego okresu stosowania produktów i systemów opartych na AI.

Inną podstawową cechą niektórych produktów i systemów opartych na AI jest **nieprzejrzystość**, jaka może wynikać ze zdolności do poprawy osiągnięć dzięki uczeniu się na podstawie zdobytego doświadczenia. W zależności od podejścia metodologicznego produkty i systemy oparte na AI mogą charakteryzować się różnym stopniem nieprzejrzystości. Może to sprawiać, że proces decyzyjny systemu może być trudny do prześledzenia („efekt czarnej skrzynki"). Ludzie nie muszą rozumieć każdego etapu procesu decyzyjnego, ale ponieważ algorytmy AI stają się coraz bardziej zaawansowane i są wprowadzane w kluczowych dziedzinach, konieczne jest, by człowiek był w stanie zrozumieć, jak doszło do tego, że system – za pomocą algorytmu – podjął takie a nie inne decyzje. Byłoby to szczególnie ważne w przypadku mechanizmu egzekwowania *ex post*, ponieważ umożliwiałoby organom egzekwowania prawa ustalanie odpowiedzialności za zachowanie i wybory systemów opartych na AI. Potwierdzono to również w komunikacie Komisji w sprawie budowania zaufania do sztucznej inteligencji ukierunkowanej na człowieka[46].

Unijne przepisy dotyczące bezpieczeństwa produktów nie odnoszą się wyraźnie do rosnących zagrożeń wynikających z nieprzejrzystości systemów opartych n algorytmach. Konieczne jest zatem rozważenie wymogów w zakresie przejrzystości algorytmów, a także solidności, odpowiedzialności oraz, w stosownych przypadkach, nadzoru przez człowieka i obiektywnych rezultatów[47], szczególnie ważnych w przypadku mechanizmu egzekwowania *ex post*, aby budować zaufanie do korzystania z tych technologii. Jednym ze sposobów poradzenia sobie z tym wyzwaniem może być nałożenie na twórców algorytmów obowiązku ujawnienia parametrów projektowych i metadanych zawartych w zbiorach danych, w razie gdyby miały miejsce wypadki.

[46] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

[47] Na podstawie kluczowych wymogów zaproponowanych przez grupę ekspertów wysokiego szczebla w wytycznych w zakresie etyki dotyczących godnej zaufania sztucznej inteligencji: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines

Dodatkowe zagrożenia, które mogą mieć wpływ na bezpieczeństwo, wynikają ze **złożoności produktów i systemów**, gdyż różne części, urządzenia i produkty mogą być ze sobą połączone i wzajemnie wpływać na funkcjonowanie każdego z nich (np. produkty będące częścią ekosystemu inteligentnego domu).

Kwestia złożoności została już uwzględniona w unijnych ramach prawnych w dziedzinie bezpieczeństwa, o których mowa na początku niniejszej sekcji[48]. Przy przeprowadzaniu oceny ryzyka produktu producent musi w szczególności wziąć pod uwagę przeznaczenie, przewidywalne zastosowanie oraz w stosownych przypadkach racjonalnie przewidywalne niewłaściwe zastosowanie.

W tym kontekście, **jeżeli producent przewiduje, że jego urządzenie zostanie wzajemnie połączone z innymi urządzeniami i będzie wchodzić z nimi w interakcje, należy to uwzględnić podczas oceny ryzyka**. Zastosowanie lub niewłaściwe zastosowanie określa się na przykład na podstawie doświadczeń z wcześniejszego zastosowania produktów tego samego typu, badania wypadków lub zachowania ludzkiego.

Złożoność systemów została również bardziej szczegółowo uregulowana przez sektorowe przepisy dotyczące bezpieczeństwa, takie jak rozporządzenie dotyczące wyrobów medycznych i do pewnego stopnia przez przepisy dotyczące ogólnego bezpieczeństwa produktów[49]. Na przykład producent urządzenia podłączonego do internetu, które ma być częścią ekosystemu inteligentnego domu, powinien być w stanie racjonalnie przewidzieć, że jego produkty będą miały wpływ na bezpieczeństwo innych produktów.

Ponadto przepisy dotyczące transportu uwzględniają tę złożoność na poziomie systemu. W przypadku samochodów, pociągów i samolotów przeprowadza się homologację typu i certyfikację w odniesieniu do każdego elementu, a także w odniesieniu do całego pojazdu lub statku powietrznego. Ocena zdatności do ruchu drogowego i do lotu oraz interoperacyjności kolei jest częścią oceny bezpieczeństwa. W transporcie „systemy" muszą być „zatwierdzone" przez organ na podstawie oceny zgodności przez stronę trzecią pod kątem jasnych wymogów technicznych lub po wykazaniu, w jaki sposób przeciwdziała się ryzyku. Rozwiązaniem jest zazwyczaj połączenie poziomu „produktu" i „systemu".

W unijnych przepisach dotyczących bezpieczeństwa produktów, w tym przepisach dotyczących transportu, do pewnego stopnia już uwzględniono złożoność produktów lub systemów, aby przeciwdziałać zagrożeniom, które mogą mieć wpływ na bezpieczeństwo użytkowników.

Złożone systemy często obejmują **oprogramowanie**, które jest zasadniczym elementem systemu opartego na AI. W ramach wstępnej oceny ryzyka producent produktu końcowego ma na ogół obowiązek przewidzieć ryzyko związane z oprogramowaniem stanowiącym część danego produktu w momencie jego wprowadzenia do obrotu.

Niektóre akty prawne w ramach unijnych przepisów dotyczące bezpieczeństwa produktów wyraźnie odnoszą się do oprogramowania stanowiącego część danego produktu. Na przykład

[48] Rozporządzenie (WE) nr 2008/765 i decyzja (WE) nr 2008/768 oraz zharmonizowane przepisy sektorowe dotyczące bezpieczeństwa produktów, np. w dyrektywie 2006/42/WE w sprawie maszyn.

[49] Art. 2 dyrektywy w sprawie ogólnego bezpieczeństwa produktów stanowi, że produkt bezpieczny uwzględnia „oddziaływanie na inne produkty, jeżeli można racjonalnie przewidzieć, że będzie on używany wraz z innymi produktami".

dyrektywa w sprawie maszyn wymaga[50], aby awaria oprogramowania systemu kontroli nie prowadziła do niebezpiecznych sytuacji.

W unijnych przepisach dotyczących bezpieczeństwa produktów aktualizacje oprogramowania można porównać z obsługą techniczną ze względów bezpieczeństwa, pod warunkiem że nie zmieniają one znacząco produktu już wprowadzonego do obrotu ani nie wprowadzają nowych rodzajów ryzyka, których nie przewidziano w początkowej ocenie ryzyka. Jeżeli jednak aktualizacja oprogramowania znacznie zmienia produkt, do którego została ona pobrana, cały produkt można uznać za nowy produkt, a zgodność z odpowiednimi przepisami dotyczącymi bezpieczeństwa produktów należy w momencie dokonywania modyfikacji poddać ponownej ocenie[51].

Unijne zharmonizowane przepisy sektorowe dotyczące bezpieczeństwa produktów zasadniczo nie zawierają szczegółowych przepisów, jeżeli chodzi o samodzielne oprogramowanie, wprowadzane do obrotu bezpośrednio lub wysyłane po wprowadzeniu produktu do obrotu. Niektóre akty prawne w ramach unijnych przepisów odnoszą się jednak do samodzielnego oprogramowania, na przykład rozporządzenie w sprawie wyrobów medycznych. Dyrektywa w sprawie urządzeń radiowych może ponadto regulować, w drodze aktów delegowanych, również samodzielne oprogramowanie wysyłane do produktów podłączonych do internetu, które komunikują się między sobą za pośrednictwem określonych modułów radiowych[52]. Zgodnie z tą dyrektywą określone klasy lub kategorie urządzeń radiowych mają być wyposażone w funkcje zapewniające, by wysyłanie oprogramowania nie powodowało naruszenia zgodności tych urządzeń[53].

Podczas gdy unijne przepisy dotyczące bezpieczeństwa produktów uwzględniają zagrożenia dla bezpieczeństwa wynikające z oprogramowania będącego częścią produktu w momencie jego wprowadzania do obrotu i potencjalnie kolejnych aktualizacji przewidzianych przez producenta, potrzebne mogą być szczegółowe lub wyraźne wymogi dotyczące samodzielnego oprogramowania (np. „aplikacji", którą można pobrać). Szczególną uwagę należy zwrócić na samodzielne oprogramowanie odpowiedzialne za funkcje bezpieczeństwa w produktach i systemach opartych na AI.

Konieczne może być nałożenie na producentów dodatkowych obowiązków polegających na zapewnieniu funkcji zapobiegających wysyłaniu oprogramowania, które ma wpływ na bezpieczeństwo, w trakcie cyklu życia produktów opartych na AI.

Wreszcie na pojawiające się technologie cyfrowe mają wpływ **złożone łańcuchy wartości**. Złożoność ta nie jest jednak niczym nowym ani nie jest wyłącznie problemem, który pojawia się w związku z nowymi technologiami cyfrowymi, takimi jak AI czy IoT. Dotyczy to na przykład takich produktów jak komputery, roboty usługowe lub systemy transportu.

Zgodnie z unijnymi ramami bezpieczeństwa produktów bez względu na to, jak skomplikowany jest łańcuch wartości, odpowiedzialność za bezpieczeństwo produktu spoczywa na producencie, który wprowadza produkt do obrotu. Producenci są odpowiedzialni za bezpieczeństwo produktu końcowego, w tym za części stanowiące integralną część danego produktu, np. oprogramowanie komputera.

---

50 Sekcja 1.2.1 załącznika I do dyrektywy w sprawie maszyn

51 „Niebieski przewodnik – wdrażanie przepisów UE dotyczących produktów", 2016 r.

52 Moduły radiowe są urządzeniami elektronicznymi, które przekazują lub odbierają sygnały radiowe (WIFI, Bluetooth) między dwoma urządzeniami

53 Art. 3 ust. 3 lit. i) dyrektywy w sprawie urządzeń radiowych,

Niektóre akty prawne w ramach unijnych przepisów dotyczące bezpieczeństwa produktów zawierają już przepisy, które wyraźnie odnoszą się do sytuacji, w których kilka podmiotów gospodarczych dokonuje czynności? na danym produkcie, zanim zostanie on wprowadzony do obrotu. Na przykład zgodnie z dyrektywą w sprawie dźwigów[54] podmiot gospodarczy, który projektuje i produkuje dźwig, ma dostarczyć instalatorowi[55] „wszystkie konieczne dokumenty i informacje, aby umożliwić mu zapewnienie właściwej i bezpiecznej instalacji i testów dźwigu". Dyrektywa w sprawie maszyn nakłada na producentów sprzętu obowiązek dostarczania operatorowi informacji na temat sposobu montażu tego urządzenia z inną maszyną[56].

W unijnych przepisach dotyczących bezpieczeństwa produktów uwzględnia się złożoność łańcuchów wartości i nakłada obowiązki na kilka podmiotów gospodarczych zgodnie z zasadą „wspólnej odpowiedzialności".

Uregulowania dotyczące odpowiedzialności producenta za bezpieczeństwo produktu końcowego okazały się odpowiednie w odniesieniu do obecnych złożonych łańcuchów wartości, jednak w przypadku być może jeszcze bardziej złożonych łańcuchów wartości jednoznaczne przepisy wymagające w szczególności współpracy między podmiotami gospodarczymi w łańcuchu dostaw a użytkownikami zapewniłyby pewność prawa. W szczególności każdy podmiot w łańcuchu wartości mający wpływ na bezpieczeństwo produktu (np. producenci oprogramowania) i użytkownicy (modyfikując produkt) przyjmowaliby odpowiedzialność i dostarczaliby kolejnym podmiotom w łańcuchu niezbędne informacje i środki.

3. Odpowiedzialność

Na poziomie Unii przepisy dotyczące bezpieczeństwa produktów i odpowiedzialności za produkt stanowią dwa uzupełniające się mechanizmy służące realizacji tego samego celu polityki, jakim jest funkcjonowanie jednolitego rynku towarów, który zapewnia wysoki poziom bezpieczeństwa, tj. minimalizuje ryzyko szkody po stronie użytkowników i przewiduje odszkodowanie z tytułu szkód związanych z wadliwymi towarami.

Uzupełnieniem tych przepisów Unii są na poziomie krajowym niezharmonizowane ramy odpowiedzialności cywilnej, które zapewniają odszkodowanie z tytułu szkód z różnych przyczyn (takich jak produkty i usługi) oraz regulują kwestię różnych odpowiedzialnych osób (takich jak właściciele, operatorzy lub usługodawcy).

Optymalizacja unijnych przepisów w zakresie bezpieczeństwa w odniesieniu do AI może pomóc unikać wypadków, jednak mimo to może do nich dochodzić. Kwestia ta wchodzi w zakres odpowiedzialności cywilnej. Zasady odpowiedzialności cywilnej odgrywają w naszym społeczeństwie podwójną rolę: z jednej strony gwarantują, że osoby, które poniosły szkodę spowodowaną przez inne osoby, otrzymują odszkodowanie, z drugiej strony zapewniają zachęty gospodarcze dla strony odpowiedzialnej, by nie powodować takich

[54] Zgodnie z art. 16 ust. 2 dyrektywy 2014/33/UE

[55] W dyrektywie 2014/33/UE w sprawie dźwigów instalator jest równoważny producentowi i musi ponosić odpowiedzialność za zaprojektowanie, wykonanie, zainstalowanie dźwigu oraz wprowadzenie go do obrotu.

[56] Art. 1.7.4.2 załącznika I do dyrektywy w sprawie maszyn stanowi, że „każda instrukcja obsługi musi zawierać przynajmniej następujące informacje, jeżeli mają one zastosowanie:" i) „instrukcje montażu, instalacji i łączenia, zawierające rysunki, schematy i sposoby mocowania oraz określenie podwozia lub instalacji, na jakim maszyna ma być zamontowana;".

szkód. Zasady odpowiedzialności muszą zawsze zapewniać równowagę między ochroną obywateli przed szkodą oraz możliwością wprowadzania przez przedsiębiorstwa innowacji.

Unijne ramy odpowiedzialności działają dobrze. Opierają się one na równoległym stosowaniu dyrektywy w sprawie odpowiedzialności za produkty (dyrektywa 85/374/EWG), w której zharmonizowano odpowiedzialność producenta wadliwych produktów i inne niezharmonizowane krajowe systemy odpowiedzialności.

Dyrektywa w sprawie odpowiedzialności za produkty zapewnia warstwę ochrony, której sama krajowa odpowiedzialność na zasadzie winy nie zapewnia. Wprowadza ona system odpowiedzialności producenta na zasadzie ryzyka za wady w jego produktach. W przypadku szkody fizycznej lub materialnej osoba poszkodowana ma prawo do odszkodowania, jeżeli udowodni szkodę, wadę w produkcie (tj. brak zapewnienia bezpieczeństwa, jakiego społeczeństwo ma prawo oczekiwać) oraz związek przyczynowy między produktem wadliwym a szkodą.

Niezharmonizowane przepisy krajowe przewidują systemy odpowiedzialności na zasadzie winy, zgodnie z którymi, aby roszczenie z tytułu odpowiedzialności zostało uznane, osoby poszkodowane muszą dowieść winy osoby odpowiedzialnej, szkody i związku przyczynowego między wadą a szkodą. Przewidują one również systemy odpowiedzialności na zasadzie ryzyka, w przypadku gdy ustawodawca krajowy przypisuje odpowiedzialność za ryzyko konkretnej osobie, bez konieczności wykazania przez poszkodowanego błędu lub wady lub związku przyczynowego między błędem lub wadą a szkodą.

Krajowe systemy odpowiedzialności zapewniają osobom, które poniosły szkodę spowodowaną przez produkty i usługi, kilka równoległych sposobów ubiegania się o odszkodowanie, opartych na odpowiedzialności na zasadzie winy lub na zasadzie ryzyka. Roszczenia te kierowane są często przeciwko różnym osobom odpowiedzialnym i obwarowane są różnymi warunkami.

Na przykład poszkodowany uczestniczący w wypadku samochodowym wysuwa zwykle roszczenie z tytułu odpowiedzialności na zasadzie ryzyka wobec właściciela samochodu (tj. osoby, która wykupuje ubezpieczenie od odpowiedzialności cywilnej z tytułu użytkowania pojazdów mechanicznych) oraz roszczenie z tytułu odpowiedzialności na zasadzie winy wobec kierowcy (oba roszczenia na podstawie krajowego prawa cywilnego), a także – jeżeli pojazd był wadliwy – roszczenie na podstawie dyrektywy w sprawie odpowiedzialności za produkty wobec producenta.

Zgodnie ze zharmonizowanymi przepisami dotyczącymi ubezpieczenia pojazdów silnikowych korzystanie z pojazdu musi być ubezpieczone[57] i w praktyce to do ubezpieczyciela kierowane jest w pierwszej kolejności roszczenie o odszkodowanie z tytułu szkody osobowej lub szkody materialnej. Zgodnie z tymi przepisami w ramach obowiązkowego ubezpieczenia wypłacane jest odszkodowanie poszkodowanemu i zapewnia się ochronę ubezpieczonemu, który na podstawie krajowego prawa cywilnego[58] jest odpowiedzialny za pokrycie strat finansowych z tytułu wypadku z udziałem pojazdu silnikowego. Producenci nie podlegają obowiązkowemu ubezpieczeniu na mocy dyrektywy w sprawie odpowiedzialności za produkty. Jeżeli chodzi o ubezpieczenie pojazdów, unijne

[57] Zharmonizowane w odniesieniu do pojazdów silnikowych dyrektywą 2009/103/WE w sprawie ubezpieczenia od odpowiedzialności cywilnej za szkody powstałe w związku z ruchem pojazdów mechanicznych i egzekwowania obowiązku ubezpieczania od takiej odpowiedzialności.

[58] W większości państw członkowskich zasadę odpowiedzialności na zasadzie ryzyka stosuje się w odniesieniu do osoby, na którą zarejestrowany jest pojazd silnikowy.

przepisy nie traktują pojazdów autonomicznych inaczej niż pojazdów nieautonomicznych. Pojazdy takie, podobnie jak wszystkie inne pojazdy, muszą być objęte ubezpieczeniem od odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych, co jest najprostszym sposobem uzyskania odszkodowania przez stronę poszkodowaną.

Odpowiednie ubezpieczenie może złagodzić negatywne skutki wypadków, zapewniając poszkodowanemu sprawną wypłatę odszkodowania. Jasne zasady odpowiedzialności pomagają towarzystwom ubezpieczeniowym w obliczaniu ryzyka i żądaniu zwrotu kosztów od strony ostatecznie odpowiedzialnej za szkodę. Jeżeli wypadek jest spowodowany na przykład wadą, ubezpieczyciel pojazdu, po wypłaceniu odszkodowania poszkodowanemu, może zwrócić się o zwrot kosztów do producenta.

Jednak cechy nowych technologii cyfrowych, takich jak AI, IoT czy robotyka, podważają pewne aspekty unijnych i krajowych ram odpowiedzialności i mogą ograniczyć ich skuteczność. Niektóre z tych cech mogą utrudnić ustalenie, czy szkoda powstała w wyniku ludzkiego zachowania, które może być podstawą roszczenia na zasadzie winy zgodnie z przepisami krajowymi. Oznacza to, że roszczenia odszkodowawcze w oparciu o krajowe prawo deliktów mogą być trudne lub nadmiernie kosztowne do dowiedzenia, i w związku z tym poszkodowani mogą nie otrzymać odpowiedniego odszkodowania. Ważne jest, by osoby poszkodowane w wypadkach spowodowanych przez produkty i usługi, w tym obejmujące nowe technologie cyfrowe, takie jak AI, nie były objęte niższym poziomem ochrony niż poziom obowiązujący w przypadku innych podobnych produktów i usług, za które przysługiwałoby im odszkodowanie na podstawie krajowego prawa deliktów. Mogłoby to zmniejszyć akceptację społeczną dla tych pojawiających się technologii i powodować niechęć do korzystania z nich.

Konieczna będzie ocena, czy wyzwania, jakie niosą ze sobą nowe technologie dla istniejących ram, mogłyby również powodować niepewność prawa co do sposobu stosowania istniejących przepisów (np. w jaki sposób pojęcie winy miałoby zastosowanie do szkód spowodowanych przez AI). Mogłoby to z kolei zniechęcać do inwestowania oraz zwiększać koszty informacji i ubezpieczenia dla producentów i innych przedsiębiorstw w łańcuchu dostaw, zwłaszcza europejskich MŚP. Ponadto gdyby państwa członkowskie miały rozwiązywać problemy związane z krajowymi ramami odpowiedzialności, mogłoby to prowadzić do dalszej fragmentacji, zwiększając tym samym koszty wprowadzania do obrotu innowacyjnych rozwiązań opartych na AI i ograniczając handel transgraniczny na jednolitym rynku. Ważne jest, by przedsiębiorstwa wiedziały, jakie ryzyko odpowiedzialności cywilnej ponoszą w całym łańcuchu wartości i mogły je ograniczyć lub zapobiegać mu, a także skutecznie zabezpieczać się przed tym ryzykiem.

W niniejszym rozdziale wyjaśniono, dlaczego nowe technologie stanowią wyzwanie dla istniejących ram i w jaki sposób można tym wyzwaniom zaradzić. Na dodatkową uwagę zasługuje ponadto specyfika niektórych sektorów, na przykład opieki zdrowotnej.

Złożoność produktów, usług i łańcucha wartości: W ostatnich dziesięcioleciach nastąpiła radykalna ewolucja technologii i przemysłu. W szczególności granica pomiędzy produktami a usługami może już nie być tak oczywista, jak to było przedtem. Produkty i świadczenie usług są ze sobą coraz ściślej powiązane. Chociaż złożone produkty i łańcuchy wartości nie są niczym nowym dla europejskiego przemysłu ani jego modelu regulacyjnego, to – w kontekście odpowiedzialności za produkt – oprogramowanie, a także AI zasługują na szczególną uwagę. Oprogramowanie ma zasadnicze znaczenie dla funkcjonowania dużej liczby produktów i może mieć wpływ na ich bezpieczeństwo. Stanowi ono integralną część produktu, ale może być również dostarczone oddzielnie, aby umożliwić stosowanie produktu zgodnie z przeznaczeniem. Bez oprogramowania komputer czy smartfon byłyby

bezużyteczne. Oznacza to, że oprogramowanie może sprawić, że produkt materialny stanie się wadliwy i spowoduje szkody fizyczne (por. tekst w ramce dotyczący oprogramowania w części na temat bezpieczeństwa). Mogłoby to w efekcie prowadzić do pociągnięcia do odpowiedzialności producenta produktu na podstawie dyrektywy w sprawie odpowiedzialności za produkty.

Jednak ze względu na to, że rodzaje i formy oprogramowania są bardzo zróżnicowane, czasami trudno jest rozstrzygnąć, czy oprogramowanie klasyfikuje się jako usługa czy jako produkt. W związku z tym, o ile oprogramowanie kierujące działaniem produktu materialnego można uważać za część lub element tego produktu, niektóre formy samodzielnego oprogramowania mogą być trudniejsze do sklasyfikowania.

Mimo że definicja produktu w dyrektywie w sprawie odpowiedzialności za produkty jest szeroka, można by bardziej doprecyzować jej zakres, aby lepiej oddać złożoność pojawiających się technologii i zapewnić, by zawsze istniała możliwość dochodzenia odszkodowania za szkody spowodowane przez produkty wadliwe z powodu oprogramowania lub innych funkcji cyfrowych. Ułatwiłoby to podmiotom gospodarczym takim jak twórcy oprogramowania ocenę, czy można ich uznać za producentów zgodnie z dyrektywą w sprawie odpowiedzialności za produkty.

Zastosowania oparte na AI często stanowią **część złożonych środowisk IoT**, w których zachodzą interakcje wielu różnych urządzeń i usług podłączonych do internetu. Łączenie różnych podzespołów cyfrowych w złożonym ekosystemie i wielość zaangażowanych podmiotów może utrudniać ocenę, gdzie powstaje szkoda i kto ponosi za nią odpowiedzialność. Ze względu na złożoność tych technologii poszkodowanym może być bardzo trudno ustalić, kto jest odpowiedzialny i spełnić wszystkie niezbędne warunki skutecznego dochodzenia roszczeń zgodnie z wymogami prawa krajowego. Zaporowe koszty takich ekspertyz mogą zniechęcać poszkodowanych do ubiegania się o odszkodowanie.

Ponadto produkty i usługi oparte na AI będą wchodzić w interakcje z tradycyjnymi technologiami, co jeszcze bardziej zwiększa złożoność, również w kontekście odpowiedzialności. Na przykład samochody autonomiczne będą przez pewien czas jeździć po tych samych drogach, co samochody tradycyjne. Podobne problemy interakcji podmiotów pojawiają się w niektórych sektorach usług (takich jak zarządzanie ruchem drogowym i opieka zdrowotna), w których częściowo zautomatyzowane systemy oparta na AI będą wspierać człowieka w podejmowaniu decyzji.

Zgodnie ze sprawozdaniem[59] podgrupy odpowiedzialnej za tworzenie nowych technologii w ramach grupy ekspertów ds. odpowiedzialności i nowych technologii można by rozważyć dostosowanie przepisów krajowych w taki sposób, aby ułatwić poszkodowanym ustalenie, na kim spoczywa ciężar dowodu w przypadku szkód związanych z AI. Ciężar dowodu mógłby być na przykład powiązany z przestrzeganiem (przez odpowiedni podmiot gospodarczy) szczególnych zobowiązań w zakresie cyberbezpieczeństwa lub innych zobowiązań w zakresie bezpieczeństwa określonych przez prawo: jeżeli podmiot nie zastosuje się do tych zasad, może nastąpić zmiana, jeżeli chodzi o ciężar dowodu w kontekście winy i związku przyczynowego.

W drodze odpowiedniej inicjatywy UE Komisja zasięga opinii na temat tego, czy i w jakim stopniu konieczne może być złagodzenie skutków złożoności przez zmniejszenie/odwrócenie

[59] Sprawozdanie „Odpowiedzialność w zakresie sztucznej inteligencji i innych powstających technologii”, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

ciężaru dowodu wymaganego na mocy krajowych przepisów dotyczących odpowiedzialności za szkody spowodowane przez zastosowania oparte na AI.

Jeżeli chodzi o przepisy Unii, zgodnie z dyrektywą w sprawie odpowiedzialności za produkty, produkt niespełniający obowiązkowych przepisów w zakresie bezpieczeństwa zostałby uznany za wadliwy bez względu na winę producenta. Mogą jednak również istnieć powody, by zastanowić się nad sposobem ułatwienia poszkodowanym ustalenie, na kim spoczywa ciężar dowodu na podstawie dyrektywy: dyrektywa opiera się na krajowych regułach dowodowych i na ustaleniu związku przyczynowego.

Łączność z internetem i otwartość: Obecnie nie jest w pełni jasne, jakie mogą być oczekiwania co do bezpieczeństwa w odniesieniu do szkód wynikających z naruszenia cyberbezpieczeństwa w zakresie produktu i czy za taką szkodę przysługiwałoby odpowiednie odszkodowanie na podstawie dyrektywy w sprawie odpowiedzialności za produkty.

Niedociągnięcia w zakresie cyberbezpieczeństwa mogą istnieć już od początku, na etapie wprowadzania produktu do obrotu, ale mogą pojawić się też później, na długo po wprowadzeniu go do obrotu.

Ramy odpowiedzialności na zasadzie winy jasno określają zobowiązania w zakresie cyberbezpieczeństwa, dzięki czemu podmioty mogą ustalić, co należy zrobić, by uniknąć konsekwencji odpowiedzialności.

W świetle dyrektywy w sprawie odpowiedzialności za produkty kwestią większej wagi może stać się pytanie, czy producent, biorąc pod uwagę racjonalnie przewidywalne zastosowanie produktu, mógł przewidzieć określone zmiany. Może wzrosnąć na przykład liczba przypadków wykorzystania „linii obrony z tytułu późniejszej wady", zgodnie z którą producent nie ponosi odpowiedzialności, jeżeli wada nie istniała w momencie wprowadzenia produktu do obrotu lub „linii obrony z tytułu ryzyka związanego z rozwojem" (zgodnie z którą ówczesny stan wiedzy nie pozwalał przewidzieć wady). Odpowiedzialność może zostać ponadto ograniczona, w przypadku gdyby strona poszkodowana nie dokonała aktualizacji istotnych z punktu widzenia bezpieczeństwa. Może to być potencjalnie uznane za zaniedbanie wspólne, jakiego dopuściła się osoba poszkodowana, i zmniejszyć w związku z tym odpowiedzialność producenta. Z uwagi na to, że pojęcie racjonalnie przewidywalnego zastosowania i kwestie związane z zaniedbaniem wspólnym, takie jak niepobranie aktualizacji dotyczącej bezpieczeństwa, mogą stać się bardziej rozpowszechnione, osoby poszkodowane mogą mieć trudności z uzyskaniem odszkodowania z tytułu szkód spowodowanych wadą produktu.

Autonomia i nieprzejrzystość: W przypadku gdy zastosowania oparte na AI mogą działać autonomicznie, wykonują one zadania, których etapy nie są wcześniej zdefiniowane i które odbywają się przy zmniejszonej bezpośredniej kontroli lub nadzorze przez człowieka, lub ostatecznie całkowicie bez bezpośredniej kontroli lub nadzoru przez człowieka. Zrozumienie algorytmów opartych na uczeniu się maszyn może być trudne, o ile w ogóle możliwe (tzw. „efekt czarnej skrzynki").

Oprócz złożoności omówionych powyżej kwestii, ze względu na efekt czarnej skrzynki w odniesieniu do niektórych przypadków AI uzyskanie odszkodowania mogłoby stać się trudne w przypadku szkód spowodowanych przez autonomiczne zastosowania wykorzystujące AI. Potrzeba zrozumienia algorytmu i danych wykorzystywanych przez AI wymaga zdolności analitycznych i wiedzy technicznej, które mogą być dla poszkodowanych niezwykle kosztowne. Ponadto dostęp do algorytmu i danych może być niemożliwy bez współpracy strony, na której potencjalnie spoczywa odpowiedzialność. Poszkodowani mogą zatem w praktyce nie być w stanie dochodzić roszczeń z tytułu odpowiedzialności. Nie jest

ponadto jasne, w jaki sposób można by wykazać błąd AI działającej autonomicznie albo co można by uznać za błąd osoby polegającej w swoim działaniu na stosowaniu AI.

W przepisach krajowych opracowano już szereg rozwiązań mających na celu zmniejszenie ciężaru dowodu spoczywającego na poszkodowanych w podobnych sytuacjach.

W myśl zasady przyświecającej Unii w odniesieniu do bezpieczeństwa produktów i odpowiedzialności za produkty to nadal producent musi zadbać o to, by wszystkie produkty wprowadzane do obrotu były bezpieczne, przez cały ich cykl życia, oraz za stosowanie produktu, którego można racjonalnie oczekiwać. Oznacza to, że producent musiałby się upewnić, że produkt wykorzystujący AI spełnia określone parametry bezpieczeństwa. Cechy AI nie wykluczają istnienia prawa do posiadania oczekiwań co do bezpieczeństwa w odniesieniu do produktów, niezależnie od tego, czy chodzi o automatyczne kosiarki lub roboty chirurgiczne.

Autonomia może mieć wpływ na bezpieczeństwo produktu, ponieważ może ona znacząco zmienić właściwości produktu, w tym jego zabezpieczenia. Pojawia się pytanie, na jakich warunkach cechy związane z samouczeniem się powodują przedłużenie odpowiedzialności producenta i w jakim zakresie producent powinien przewidzieć pewne zmiany.

Pojęcie „wprowadzenia do obrotu", które jest obecnie stosowane w dyrektywie w sprawie odpowiedzialności za produkty, może zostać zmienione – w ścisłej koordynacji z odpowiednimi zmianami w unijnych ramach bezpieczeństwa – w celu uwzględnienia faktu, że produkty mogą się zmieniać i być modyfikowane. Mogłoby to również pomóc w wyjaśnieniu, kto ponosi odpowiedzialność za wszelkie zmiany wprowadzane do produktu.

Zgodnie ze sprawozdaniem[60] podgrupy odpowiedzialnej za tworzenie nowych technologii w ramach grupy ekspertów ds. odpowiedzialności i nowych technologii, korzystanie z niektórych autonomicznych urządzeń i usług opartych na AI mogłaby posiadać specyficzny profil ryzyka w zakresie odpowiedzialności, ponieważ urządzenia te i usługi mogą powodować istotne szkody dla ważnych dóbr prawnych, takich jak życie, zdrowie i mienie, oraz narażać ogół społeczeństwa na ryzyko. Może to dotyczyć głównie urządzeń opartych na AI, które przemieszczają się w przestrzeni publicznej (np. w pełni autonomiczne pojazdy, drony[61] i roboty dostarczające paczki) lub usług opartych na AI o podobnym ryzyku (np. usługi zarządzania ruchem polegające na prowadzeniu lub kontrolowaniu pojazdów lub usługi zarządzania dystrybucją energii elektrycznej). Problemy związane z autonomią i nieprzejrzystością w odniesieniu do krajowego prawa deliktów można rozwiązać, stosując podejście oparte na analizie ryzyka. Systemy odpowiedzialności na zasadzie ryzyka mogą gwarantować, że, w przypadku urzeczywistnienia się tego ryzyka, poszkodowany otrzymuje odszkodowanie niezależnie od winy. Należałoby starannie ocenić konsekwencje wyboru, kto powinien ponosić odpowiedzialność na zasadzie ryzyka za takie działania w zakresie rozwoju i wdrażania AI, oraz rozważyć podejście oparte na analizie ryzyka.

W odniesieniu do eksploatacji zastosowań opartych na AI o szczególnym profilu ryzyka Komisja zasięga opinii, czy i w jakim stopniu może istnieć potrzeba odpowiedzialności na zasadzie ryzyka, tak jak ma to miejsce w prawie krajowym w odniesieniu do podobnych zagrożeń, na jakie narażona jest ludność (np. podczas eksploatacji pojazdów silnikowych,

[60] Sprawozdanie „Odpowiedzialność w zakresie sztucznej inteligencji i innych powstających technologii", https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

[61] Zob. bezzałogowych systemów powietrznych, o których mowa w rozporządzeniu wykonawczym Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych.

samolotów lub elektrowni jądrowych), aby ewentualni poszkodowani mogli skutecznie dochodzić odszkodowania. W celu zapewnienia odszkodowania niezależnie od wypłacalności osoby ponoszącej odpowiedzialność oraz w celu obniżenia kosztów szkód, Komisja zasięga również opinii co do ewentualnego powiązania odpowiedzialności na zasadzie ryzyka z obowiązkiem zawarcia dostępnego ubezpieczenia, na wzór dyrektywy w sprawie ubezpieczeń pojazdów.

Jeżeli chodzi o eksploatację wszystkich pozostałych zastosowań opartych na AI, które stanowiłyby znaczną większość zastosowań opartych na AI, Komisja rozważa, czy należy dostosować ciężar dowodu dotyczący związku przyczynowego i winy. W tym względzie jedną z kwestii zasygnalizowanych w sprawozdaniu[62] podgrupy odpowiedzialnej za tworzenie nowych technologii w ramach grupy ekspertów ds. odpowiedzialności i nowych technologii jest sytuacja, w której potencjalnie odpowiedzialna strona nie zarejestrowała danych istotnych z punktu widzenia oceny odpowiedzialności lub nie jest chętna udostępnić ich poszkodowanemu.

4. Wniosek

Pojawienie się nowych technologii cyfrowych, takich jak AI, IoT i robotyka stwarza nowe wyzwania w zakresie bezpieczeństwa produktów i odpowiedzialności za produkt, takie jak łączność z internetem, autonomia, zależność od danych, nieprzejrzystość, złożoność produktów i systemów, aktualizacje oprogramowania oraz bardziej złożone systemy zarządzania bezpieczeństwem i łańcuchy wartości.

W obecnych przepisach dotyczących bezpieczeństwa produktów istnieje szereg luk, którymi należy się zająć, w szczególności w dyrektywie w sprawie ogólnego bezpieczeństwa produktów, dyrektywie w sprawie maszyn, dyrektywie w sprawie urządzeń radiowych oraz w nowych ramach prawnych. Przyszłe prace nad dostosowaniem poszczególnych aktów prawnych objętych tymi ramami będą prowadzone w sposób spójny i zharmonizowany.

Nowe wyzwania w zakresie bezpieczeństwa stwarzają również nowe wyzwania w zakresie odpowiedzialności. Te wyzwania w zakresie odpowiedzialności należy uwzględnić, aby zapewnić taki sam poziom ochrony, z jakiego korzystają poszkodowani w kontekście tradycyjnych technologii, przy jednoczesnym utrzymaniu równowagi w stosunku do potrzeb innowacji technologicznych. Przyczyni się to do tworzenia klimatu zaufania do nowo pojawiających się technologii cyfrowych i stabilności inwestycji.

Istniejące unijne i krajowe przepisy dotyczące odpowiedzialności są zasadniczo w stanie uwzględnić problematykę pojawiających się technologii, jednak zakres i łączne konsekwencje wyzwań związanych z AI mogą utrudniać poszkodowanym uzyskanie odszkodowania we wszystkich przypadkach, w których byłoby to zasadne[63]. Dlatego też na podstawie obecnych przepisów podział kosztów w przypadku wystąpienia szkody może być niesprawiedliwy lub nieskuteczny. Aby zaradzić tej sytuacji i rozwiązać problem ewentualnych niepewności w istniejących ramach, można rozważyć wprowadzenie pewnych zmian w dyrektywie w sprawie odpowiedzialności za produkty i krajowych systemach odpowiedzialności, przy pomocy odpowiednich inicjatyw UE stosujących ukierunkowane

[62] Sprawozdanie „Odpowiedzialność w zakresie sztucznej inteligencji i innych powstających technologii”, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

[63] Zob. sprawozdanie podgrupy odpowiedzialnej za tworzenie nowych technologii, s. 3 oraz zalecenie polityczne 27.2. grupy ekspertów wysokiego szczebla ds. sztucznej inteligencji.

podejście oparte na analizie ryzyka, tj. uwzględniających fakt, że z różnymi zastosowaniami AI wiążą się różne rodzaje ryzyka.