

Małgorzata Gradek Lewandowska¹,
Anna Dębska²
Julia Szcześniak³

Sztuczna inteligencja: prawne science czy fiction?

(Druga część cyklu: „Technologie jutra już dziś w życiu rzecznika patentowego”⁴)

Wstęp

G. Hinton, A. Turing, E. Yudkowsky czy S. Hawking – te wybitne osobistości ze świata nauk ścisłych w pewnym momencie swojego życia przestrzegały nas przed mocą i siłą sztucznej inteligencji. Zdaniem ostatniego z nich – „AI [skrót AI od artificial intelligence – ang. sztuczna inteligencja - dop. MGL] może być najlepszą, albo najgorszą rzeczą, jaka kiedykolwiek przydarzyła się ludzkości”. Niezależnie od tego, jakie rozstrzygnięcie tego stwierdzenia przyniesie przyszłość, nie da się ukryć, że sztuczna inteligencja już teraz odgrywa olbrzymią rolę w codziennym życiu rzecznika patentowego.

- 1 Małgorzata Gradek Lewandowska - radca prawny, rzecznik patentowy, certyfikowany mediator wpisana na listę Centrum Mediacji KIRP, Centrum Mediacji Konfederacji Lewiatan, mediator sądowy Sądów Okręgowych w Warszawie, Katowicach, Lublinie, Poznaniu i Gdańsku, członek komisji problemowej ds. Sądu Arbitrażowego i Centrum Mediacji PIRP, absolwentka m.in. Instytutu Stosunków Międzynarodowych UW, British Centre for English and European Legal Studies – the British government Know-How Fund and Law Faculty Cambridge University, Szkoły Prawa Hiszpańskiego i Europejskiego Uniwersytetu de Castilla-La Mancha, studiów podyplomowych Prawo autorskie na UJ, współwłaścicielka kancelarii prawnej, mediacyjnej i patentowej LGL
- 2 Anna Dębska - rzecznik patentowy, absolwentka Wydziału Prawa i Administracji Uniwersytetu Łódzkiego oraz studiów podyplomowych Corporate Governance, Risk and Compliance Management organizowanych przez SGH, uczestniczka licznych kursów prawa IP organizowanych przez EUIPO
- 3 Julia Szcześniak - studentka V roku prawa na Uniwersytecie Warszawskim oraz absolwentka koreanistyki na Wydziale Orientalistycznym UW, wiceprezesa Koła Naukowego Własności Intelektualnej „IP” UW, uczestniczka XIII edycji kursu IP student Wydziału Prawa i Administracji UJ
- 4 Pierwsza część opublikowana w numerze 1/2022 (str.61-72), kolejny artykuł z tego cyklu serii przyniesie sporą dawkę informacji ze świata cyberbezpieczeństwa, w szczególności w zakresie technologii deepfake, Internetu rzeczy czyli tzw. IoT i innych zagrożeń w kontekście naruszeń przedmiotów ochrony własności intelektualnej.

To, czy AI stanowi bardziej fiction, czy bardziej science, zależy od oczekiwań, jakie stawia się wobec tego pojęcia. Jeśli rozumieć sztuczną inteligencję dosłownie jako myślącą samodzielnie maszynę, zdolną do podejmowania autonomicznych i podyktowanych określoną strategią decyzji, tak rozumiana AI pozostaje na razie w sferze przyszłości. Jednak termin science-fiction oznacza fikcję opartą na nauce, czyli rozwiązanie nieistniejące w rzeczywistości, ale przynajmniej teoretycznie możliwe z punktu widzenia praw nauki. Niewykluczone zatem, że taka AI, jaką znamy z fantastyki naukowej, jest kwestią czasu (nawet jeśli będzie to czas dość odległy). Czy w takim razie aktualnie istnieje sztuczna inteligencja? Czym jest i jakie może mieć zastosowanie? Jakie przykłady istniejącej obecnie AI możemy przytoczyć? Jakie konsekwencje prawne może mieć jej codzienne zastosowanie? Czy AI może być twórcą?

Czym jest sztuczna inteligencja?

Gdyby chcieć odpowiedzieć na przynajmniej część zadanych wyżej pytań z prawnego punktu widzenia, to porządkując pojęcia warto sięgnąć do jednego z możliwych podziałów⁵ i odnieść się do:

- **wąskiej sztucznej inteligencji** (ang. **Narrow AI**) rozumianej jako algorytmy, w tym uczące się, ale dedykowane tylko do konkretnego zadania (np. rozwiązywanie CAPTCHA, rozpoznawanie mowy, obsługa klienta, mechanizm rekomendacji) – stanowi większość otaczającej nas dziś sztucznej inteligencji, a znanymi jej przykładami są: Siri Apple, czy Alexa Amazon,
- **ogólnej sztucznej inteligencji** (ang. **Artificial General Intelligence, AGI**), która do tej pory jeszcze nie powstała, w której maszyna posiadałaby inteligencję równą ludzkiej: samoświadomość ze zdolnością rozwiązywania problemów, uczenia się i planowania przyszłości,
- **sztucznej superinteligencji** (**Artificial Super Intelligence, ASI**), która przewyższyłaby inteligencję i możliwości ludzkiego mózgu.

Obecnie mówimy o wąskiej sztucznej inteligencji. To do niej odnosi się przedstawiony w 2021 roku przez Komisję Europejską projekt Rozporządzenia Parlamentu Europejskiego i Rady Europejskiej w sprawie Sztucznej Inteligencji⁶. W projekcie tym sztuczną inteligencję zdefiniowano w taki sposób, aby definicja ta „w możliwie największym stopniu była neutralna pod względem technologicznym i nie ulegała dezaktualizacji, biorąc pod uwagę szybki rozwój technologiczny i rozwój sytuacji rynkowej w dziedzinie AI”. Sztuczna inteligencja jest zatem w Akcie zdefiniowana z punktu widzenia funkcji, jakie może spełniać i sposobu, w jaki je realizuje,

⁵ <https://www.ibm.com/pl-pl/cloud/learn/what-is-artificial-intelligence> [dostęp 17.10.2022]

⁶ Projekt (wniosek) Rozporządzenia PE i Rady (UE), ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii (dalej: „Akt”): <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021PC0206> [dostęp: 18.03.2022 r.].

bez szczegółowego definiowania wymogów technologicznych, według których jest wytworzona.

Akt w propozycji definicji AI zakłada, że: „<system sztucznej inteligencji> oznacza oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję”.

Techniki, których zastosowanie kwalifikuje system jako sztuczną inteligencję, to: procesy uczenia maszynowego, metody oparte na logice i wiedzy, takie jak bazy wiedzy lub rozumowanie symboliczne, albo podejścia statystyczne, takie jak metody wyszukiwania lub optymalizacji.

Z projektowanej definicji wynika więc, że AI posiada następujące cechy: jest rozwiązaniem informatycznym opartym na programowaniu, stworzono ją w określonym celu, a cel ten ustalił człowiek (co w szczególności oznacza, że AI nie będzie mogła w rozumieniu prawnym sama stworzyć kolejnej AI, nawet jeśli miałyby takie możliwości), jej funkcją jest generowanie wyników w postaci np. treści, przewidywań, decyzji, a efekt działania AI oddziałuje i wchodzi w interakcje z zewnętrznym otoczeniem⁷. Co istotne, system określany mianem AI wykorzystuje konkretne, zaprojektowane w nim metody, dzięki którym może dochodzić do pożądaných wyników.

Posiłkując się Aktem, sztuczną inteligencję można więc określić jako program komputerowy o bardzo konkretnej funkcjonalności, polegającej na generowaniu rezultatów mających wpływ na otoczenie. Owe rezultaty są przy tym niejako autonomicznym i oryginalnym wytworem samej AI. Dla zobrazowania, w tym znaczeniu nie będzie takim rezultatem np. wyprodukowany przez maszynę plastikowy komponent na wzór prototypu identycznego komponentu, wytworzony automatycznie według zaprogramowanej matrycy. Wynik generowany przez AI musi być w pewnym sensie efektem przeprowadzonych przez nią procesów analitycznych na podstawie zaprojektowanych metod opartych na logice, statystyce, obliczeniach, mechanizmie uczenia się lub przetwarzaniu informacji pochodzących z wbudowanej bazy wiedzy. Innymi słowy, AI to maszyna, która „nauczyła się” coś wytwarzać według zadanych jej parametrów wyjściowych i która wytwarza to autonomicznie, zaś efekt jej działania wchodzi w interakcje z otoczeniem.

Przykładem istniejącej aktualnie sztucznej inteligencji może być cyfrowa asystentka marki znanej wyszukiwarki, którą, oglądając film, możemy głosowo zapytać o wiek występującego w nim aktora. Systemy sztucznej inteligencji kojarzone są także z wykorzystaniem ich w medycynie do celów diagnozowania i oceny ryzyka zapażenia na określone choroby, zwłaszcza w kardiologii lub onkologii. Przywołując natomiast powyższy przykład z wytwarzaniem plastikowych komponentów według określonego wzoru, nie będzie raczej sztuczną inteligencją drukarka 3D.

Dlatego w ogóle prawodawca unijny postanowił uregulować AI, i to potencjalnie w akcie bezpośrednio obowiązującym podmioty prawa w państwach

⁷ Art. 3 pkt. 1) Aktu.

członkowskich? To, czym jest AI, w rozumieniu technicznym oraz prawnym (jeśli odnieść się do przesłanek zawartych w projektowanym Akcie), daje się ustalić już dzisiaj na gruncie obowiązujących aktów prawnych. Jeśli bowiem AI w sensie technicznym jest programem komputerowym, czyli oryginalnym opisem stworzonym w języku programowania, na gruncie prawnym będzie utworem prawnie-autorskim, zatem będzie stosować się do niej reżim ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych⁸, a już tylko z tego wynika wiele praktycznych wniosków, ale też ochrona ta wzbudza mniej emocji niż „patentowalność” sztucznej inteligencji.

Literalne brzmienie ustawy z dnia 30 czerwca 2000 r. Prawo własności przemysłowej i Konwencji o patencie europejskim, wyłącza możliwość udzielenia ochrony patentowej „programom komputerowym jako takim” ze względu na abstrakcyjny, nietechniczny charakter oprogramowania. Zatem oprogramowanie będzie mogło zostać objęte ochroną patentową wtedy, gdy będzie posiadało techniczny charakter. W świetle orzecznictwa Europejskiego Urzędu Patentowego⁹ o technicznym charakterze oprogramowania możemy mówić między innymi, wtedy, kiedy dany program powoduje tzw. „dalszy skutek techniczny” lub oprogramowanie jest związane z określonym urządzeniem, co nadaje programowi komputerowemu materialny, nie-abstrakcyjny charakter. Za J.Jezierskim można przytoczyć przykład oprogramowania wspomagającego określony nowatorski system hamulcowy. Wykluczone jest uzyskanie patentu na program komputerowy, który steruje takim systemem, natomiast możliwe jest objęcie ochroną patentową określonego sposobu hamowania, którego częścią jest sterujący program komputerowy.¹⁰

Akt podchodzi do tematyki sztucznej inteligencji z punktu widzenia społecznych aspektów jej wykorzystania. Projektodawca dostrzega potencjalne zagrożenia związane z użyciem inteligentnych maszyn. Projekt proponuje m.in. uregulowanie zakazanych praktyk w zakresie sztucznej inteligencji, wśród których można wymienić przykłady znane widzom *sci-fi*, takie jak: sztuczna inteligencja wykorzystująca techniki podprogowe używane bez świadomości osoby będącej obiektem oddziaływania, w celu zniekształcenia jej zachowania i mogąca wyrządzić szkody psychiczne lub fizyczne, sztuczna inteligencja wykorzystywana przez organy publiczne na potrzeby oceny lub klasyfikacji osób fizycznych, prowadzonej na podstawie ich zachowania społecznego, cech osobistych lub cech osobowości, kiedy to punktowa ocena społeczna prowadzi do krzywdzącego lub niekorzystnego traktowania, czy

8 Warto sięgnąć w tym zakresie do A.Tarkowska „Ochrona warstwy dźwiękowej gry komputerowej” w Zeszyty Uniwersytetu Jagiellońskiego zeszyt 2 (144) 2019

9 Szeroko omówionego w literaturze z czego na szczególną uwagę zasługuje kilka pozycji: Marek Porzeżyński „Zdolność patentowa programów komputerowych”, Wydawnictwo C.H.Beck 2017, Katarzyna Chalubińska-Jentkiewicz, Mirosław Karpiuk, Prawo nowych technologii. Wybrane zagadnienia, Lex a Wolters Kluwer business, Warszawa 2015, Karolina Sztobryn „Ochrona programów komputerowych w prawie własności intelektualnej w Unii Europejskiej”, Lex Wolters Kluwer business, Warszawa 2015, Prawo sztucznej inteligencji i nowych technologii pod red. B. Fischer, A. Pązik, M Świerczyński, Wolters Kluwer Warszawa 2021

10 https://www.parp.gov.pl/component/content/article/57209:ochrona-programow-komputerowych-w-prawie-wlasnosci-intelektualnej-czesc-ii#_edn1 [dostęp 17.10.2022]

wykorzystywanie systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa.

Ponadto w projekcie znajdują się propozycje uregulowania systemów sztucznej inteligencji wysokiego ryzyka, obowiązków dostawców i użytkowników systemów, wprowadzenia procesów notyfikacji lub kodeksów postępowania.

Przetwarzanie danych osobowych przez AI

Istotą działania AI jest przetwarzanie informacji w celu wyciągnięcia na ich podstawie określonych wniosków, np. szacowania prawdopodobieństwa wystąpienia zdarzeń, wydawania diagnoz, identyfikowania ryzyk. Przetwarzanie dużej ilości danych określane jest mianem „Big Data”. Termin ten pochodzi z lat 90-tych, ale nabrał istotnego znaczenia w ostatnich czasach, wobec postępu technologicznego i dostrzeżenia potencjału danych dla biznesu. Czym charakteryzuje się to zjawisko? W materiałach Parlamentu Europejskiego możemy znaleźć określenie Big Data jako pojęcie odnoszące się m.in. do dużych i złożonych zbiorów danych, których przetwarzanie, ze względu na kompleksowość, wymaga nowoczesnych technologii, takich jak chociażby właśnie sztuczna inteligencja. Dane pochodzą przy tym z wielu źródeł, a dzięki technologii ich przetwarzanie jest bardzo szybkie¹¹.

Uczenie maszynowe a Big Data

Czym z kolei jest uczenie maszynowe i jaki ma związek z danymi? Uczenie maszynowe to podkategoria (gałąź) sztucznej inteligencji. Komputery są w niej nauczane, jak automatycznie doskonalić jakość podejmowanych decyzji lub wydajność poprzez nieustannie modyfikowaną wiedzę. Maszyna otrzymuje wiele przykładów i poddawana jest nowym scenariuszom, ucząc się znajdować powiązania, tendencje i wzorce między informacjami w zbiorach danych¹². Należy uznać, że z im większej ilości danych korzysta AI, tym wyniki wygenerowane przez nią stają się dokładniejsze. Przykładem zastosowania uczenia maszynowego mogą być technologie marketingowe polegające na formułowaniu spersonalizowanych propozycji reklamowych w oparciu o zbieranie i analizę jak największej ilości danych o konsumencie, w tym przez dostrzeganie trendów wynikających z jego poprzednich zachowań, przykładowo w sieci.

Wśród informacji, z których korzysta sztuczna inteligencja, mogą oczywiście znajdować się też dane osobowe. Jako przykład jej zastosowania w takim kontekście można wskazać chociażby systemy służące do diagnozowania chorób lub szacowania ryzyka ich wystąpienia, np. ryzyka zawału serca, w oparciu o dane o stanie zdrowia i dane demograficzne osoby. Zastosowanie uczenia maszynowego

11 <https://www.europarl.europa.eu/news/pl/headlines/society/20210211STO97614/big-data-definicja-korzysci-wyzwania-infografika> [dostęp: 29.01.2022 r.];

12 Za Ośrodkiem Przetwarzania Informacji – Państwowym Instytutem Badawczym na: <https://www.sztuczna inteligencja.org.pl/slownik/> [dostęp: 29.01.2022 r.];

w diagnostyce może uwzględniać np. wykrywanie zdarzeń w oparciu o wiedzę nabytą przez program na podstawie analizy niezmierzonej liczby zdjęć rentgenowskich lub opisów badań patomorfologicznych. Inną tego typu kategorią zastosowania AI są systemy wykorzystujące biometrię (rozumianą jako metody mierzenia cech ludzi i zwierząt), rozpoznającą unikalne biologiczne dane osobowe, wynikające z zachowania lub anatomii, do celów identyfikacji lub ustalenia tożsamości osób. W konsekwencji w oparciu o rozpoznawanie biometryczne możliwe jest tworzenie systemów informatycznych służących do świadczenia określonych usług, takich jak np. płatności biometryczne, wykorzystujące uwierzytelnienie za pomocą odcisku palca, brzmienia głosu, rozpoznania tętnówki oka czy też do wydawania decyzji względem danej osoby - ostatni przykład może dotyczyć np. zwalczania przestępczości. Kolejnym zastosowaniem są systemy AI, które mogą wykorzystywać dane poprzez ich profilowanie, czyli zautomatyzowane przetwarzanie danych osobowych polegające na analizie zachowania osoby.

W chwili obecnej podstawowym aktem prawnym mającym zastosowanie do przetwarzania danych osobowych przez systemy sztucznej inteligencji jest Rozporządzenie RODO¹³. Czy ów akt prawny jest dostosowany do rewolucji technologicznej? Wydaje się, że część jego rozwiązań była projektowana z myślą o ochronie prywatności w dobie digitalizacji i z uwzględnieniem wpływu nowych technologii na życie społeczne, w przyszłości okaże się jednak, na ile skutecznie obowiązujące przepisy poradzą sobie z rozwiązywaniem problemów ochrony prywatności w zetknięciu człowieka ze sztuczną inteligencją.

Wśród rozwiązań RODO, które mogą mieć szczególne znaczenie z punktu widzenia systemów sztucznej inteligencji, można wymienić: profilowanie, uwzględnianie ochrony danych w fazie projektowania systemu, wymagania dla ustawień domyślnych (privacy by design, privacy by default) oraz ocenę wpływu planowanych operacji na prawa osób fizycznych dokonywaną przed wdrożeniem przetwarzania (privacy impact assessment).

Profilowanie

Zgodnie z RODO, profilowaniem jest „*dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się*”.¹⁴

Na gruncie ww. aktu, osoba fizyczna ma co do zasady prawo do tego, aby nie podlegać decyzji opartej wyłącznie na profilowaniu i jednocześnie wywołującej

¹³ Rozporządzenie PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (dalej RODO).

¹⁴ Art. 4 pkt. 4) RODO;

wobec niej skutki prawne lub w inny sposób istotnie na nią wpływającej.¹⁵ Motyw 71 RODO jako przykłady takich decyzji wskazuje automatyczne odrzucenie wniosku kredytowego (w oparciu o ocenę ryzyka kredytowego dokonaną przez program komputerowy) lub elektroniczne metody rekrutacji odbywające się bez udziału czynnika ludzkiego (w zakresie decyzji o zatrudnieniu lub jego braku w oparciu o analizę cech osoby, przeprowadzoną wyłącznie przez algorytmy).

Podejmowanie decyzji wobec człowieka w oparciu o profilowanie będzie jednak dozwolone w kilku przypadkach. Przykładowo, podmiot danych może wyrazić zgodę na to, by być poddanym profilowaniu. Ponadto, profilowanie jest również dopuszczalne, jeśli jest to wyraźnie dozwolone na podstawie szczególnych przepisów prawa, o ile takie przepisy przewidują należyte środki ochrony praw i interesów osoby poddanej profilowaniu¹⁶. Wspomniany motyw 71 RODO wskazuje w tym zakresie następujące uzasadnione cele: zapobieganie oszustwom, uchylaniu się od podatków, czy konieczność zapewnienia bezpieczeństwa usług administratora. Ponadto, RODO nakłada w takiej sytuacji wymóg informowania o profilowaniu osoby, której dane dotyczą, a także przewiduje jej prawo do uzyskania interwencji człowieka, prawo wyrażenia własnego stanowiska lub do zakwestionowania decyzji wynikającej z profilowania. Jednocześnie profilowanie nie powinno dotyczyć dzieci¹⁷.

Privacy by design, privacy by default

Art. 25 RODO wymaga, aby już w fazie projektowania rozwiązania uwzględnić techniczne i organizacyjne środki ochrony danych osobowych, takie jak np. pseudonimizacja, z uwzględnieniem zwłaszcza stanu wiedzy technicznej, kosztów wdrożenia i ryzyka naruszenia praw podmiotów danych.¹⁸

Ponadto, domyślne przetwarzanie danych, a więc domyślne ustawienia danego programu, czy systemu, powinno zapewniać, aby przetwarzane były wyłącznie dane w minimalnym, niezbędnym zakresie i ilości. Zarazem dane przetwarzane w ramach ustawień domyślnych mogą być udostępnione nieograniczonej liczbie osób tylko za zgodą danej osoby.¹⁹

Privacy impact assessment

Art. 35 RODO przewiduje, że jeżeli dany rodzaj przetwarzania danych, w szczególności z użyciem nowoczesnych technologii, wskazuje na wysokie ryzyko naruszenia praw i wolności osób fizycznych, administrator danych (np. twórca lub producent systemu) ma obowiązek przeprowadzić przed wdrożeniem ocenę skutków planowanych operacji dla ochrony danych osobowych. Taka ocena wpływu rozwiązania na prywatność jest wymagana przykładowo w przypadku systematycznego

¹⁵ Art. 22 ust. 1 RODO;

¹⁶ Art. 22 ust. 2 RODO;

¹⁷ Motyw 71 RODO;

¹⁸ Art. 25 ust. 1 RODO;

¹⁹ Art. 25 ust. 2 RODO;

i kompleksowego podejmowania decyzji wobec osób fizycznych w oparciu o profilowanie, systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie lub przetwarzanie na dużą skalę tzw. wrażliwych danych osobowych (np. danych o stanie zdrowia)²⁰. Jednym z przykładów narzędzi nowoczesnych technologii działających dzięki zastosowaniu sztucznej inteligencji, mogących służyć przetwarzaniu danych osobowych, są coraz częściej stosowane w różnych elektronicznych urządzeniach oraz stosowane na co dzień boty.

Bot – wirtualny asystent

Botyka to wykorzystywanie wiedzy o zachowaniach ludzi do modelowania i symulowania cyfrowych postaci – botów, czyli programów wykonujących pewne czynności w zastępstwie człowieka. Ich nazwa pochodzi od słowa robot – czyli zautomatyzowanej do danych celów maszyny. W rzeczywistości bot to program komputerowy działający online, pewien zbiór algorytmów odpowiadających za prowadzenie konwersacji i wszystkie działania z nią związane. Korzysta z własnych baz danych, ale ma także możliwość czerpania informacji z zewnętrznych źródeł, takich jak inne bazy danych, wyszukiwarki czy informacyjne strony internetowe. Dzięki tej wiedzy potrafi udzielić odpowiedzi na niemal każde pytania z danego zakresu, a jednocześnie uczy się ich i zapamiętuje je na podstawie zadawanych mu pytań.

Szczególną odmianą bota jest tzw. „Chatter-bot”, czy też w spolszczonej wersji „czatbot”. To wirtualny asystent, który dzięki zastosowaniu sztucznej inteligencji prowadzi rozmowę za pośrednictwem strony internetowej z jej użytkownikiem. Rozmowa ta ma charakter konwersacji na czacie. Dzięki wgraniem oprogramowaniu wirtualny doradca rozpoznaje zadane mu na czacie pytanie i potrafi udzielić jak najbardziej dopasowanej do niego odpowiedzi. Oprócz tego może on także samodzielnie nawiązywać kontakt z użytkownikiem strony internetowej, na przykład zachęcając go do zapoznania się z ofertą.

Za pierwszego czatbota uznawana jest Eliza, sztuczny psychoterapeuta. Stworzył ją w 1966 r. Joseph Weizenbaum w Massachusetts Institute of Technology. Eliza była próbą realizacji projektu CMC (Computer Mediated Communications). Kolejnym projektem, najbardziej znanym na świecie, jest ALICE stworzona przez Richarda Wallace’a w 1995 r. i rozwijana przez wielu fascynatów. ALICE była projektem otwartym, tworzonym na opracowanym do tego celu przez zespół ludzi języku znaczników AIML (Artificial Intelligence Mark-up Language) na wzór HTMLa. Przykładem bardzo złożonych chatbotów są też zautomatyzowani inteligentni asystenci, jak na przykład Google Assistant i czy asystent głosu firmy Apple – Siri. W obecnych czasach, gdy większość spraw załatwiamy online, z botami spotykamy się praktycznie codziennie. Najczęściej pomagają na stronach www, jako wirtualny asystent lub doradca, który odpowiada na najczęściej zadawane pytania, opowiada

20 Art. 35 ust. 3 RODO.

o ofercie, kieruje na właściwe strony serwisu, asystuje w wypełnianiu formularzy, wirtualny urzędnik stworzony do pomocy na stronach urzędów w szybkim wyszukiwaniu informacji i załatwianiu typowych spraw urzędowych, czy pomocnik w e-learningu, czyli asystent szkoleń online, taki wirtualny nauczyciel, który pomaga pokonywać kolejne etapy kursów i szkoleń.

W przypadku botów możemy spotkać dobre sposoby ich wykorzystania (jak te wymienione wyżej – wspierające działania przedsiębiorców, urzędów i przyspieszające obsługę klienta), ale również te złe – wykorzystywane do nielegalnych działań. Zaliczyć można do nich tzw. „spam boty”, czyli niechciane wiadomości e-mail, które mają zachęcać użytkownika do odwiedzenia poszczególnych stron w Internecie, często zawierające także złośliwe oprogramowanie, które po kliknięciu w link śledzi nasze działania w sieci, boty rejestracyjne korzystające z danych zdobytych przez spam boty po to, by rejestrować fałszywe konta w różnych serwisach, czy „fraud boty” służące do zawyżania raportów marketingowych lub afiliacyjnych, na podstawie których wypłacane są prowizje.

Zainfekowanie sprzętu tego typu botami może nieść dla użytkownika negatywne skutki w postaci wykradania jego danych, podszywania się pod niego, a nawet doprowadzić do rozporządzenia jego środkami w niechciany sposób, na przykład przez doprowadzenie do wykonania przelewu bankowego na fikcyjne konto. Dla prawników oznacza to konieczność zmierzenia się z problemami odpowiedzialności za działania bota oraz pozyskiwania przez niego danych. Pierwsza z kwestii wpisuje się w szerszy problem podziału na silną i słabą sztuczną inteligencję. Jak zauważa T. Zalewski: *„z punktu widzenia informatyki, pojęcie sztucznej inteligencji jest zazwyczaj używane do opisu systemów komputerowych, które najpierw analizują duże ilości danych w celu m.in. ich kategoryzacji i znalezienia w nich powtarzalności, a następnie podejmują decyzje na podstawie tych danych. Takie systemy potrafią się „uczyć” na podstawie analizowanych danych, a także kontynuować taką naukę podczas swojego działania, w ramach którego sposób podejmowania decyzji jest optymalizowany, a baza danych i wiedzy rozszerzana. Tak działające systemy określa się jako tzw. słabą sztuczną inteligencję – odróżniając ją od silnej sztucznej inteligencji. Słaba AI to zdolność do działania w sposób podobny do działania inteligencji człowieka. Natomiast silna AI to zdolność do faktycznego myślenia, czyli myślenia w sposób niesymulowany. Przy takim założeniu silna AI byłaby zapewne obdarzona świadomością swego istnienia”*.²¹

Aktualnie uregulowaną przepisami kwestią jest dostęp bota do danych. Aby bot funkcjonował prawidłowo, niezbędne jest zastosowanie dużych ilości danych, które zostają przetworzone i stanowią podstawę do uczenia algorytmów. Rodzaje danych różnią się w zależności od zastosowania konkretnej sztucznej inteligencji. Może zatem chodzić o dane takie, jak obrazy, które mogą, ale nie muszą zawierać informacji dotyczących konkretnych osób, co trudno jednak w stu procentach

21 T. Zalewski, Rozdział I. Definicja sztucznej inteligencji [w:] Prawo sztucznej inteligencji, red. Luigi Lai, prof. UKSW dr hab. Marek Świerczyński, Warszawa 2020 [dostęp: Legalis, 18.03.2022 r.].

kontrolować. Jednocześnie w grę wchodzi kwestia powierzenia danych podmiotowi obsługującemu oprogramowanie oraz zainfekowania urządzeń złośliwym oprogramowaniem rozprowadzanym przez boty.

Ze względu na potrzebę udostępnienia, jak i ochronę danych zastosowanie do działań botów mają przepisy związane z ochroną danych osobowych, dóbr osobistych (w tym wizerunku), praw autorskich, praw własności przemysłowej, tajemnicy przedsiębiorstwa, danych osobowych a także z naruszeniem prywatności, kradzieżą tożsamości czy kradzieżą dóbr intelektualnych. Z tego względu twórcy chatbotów, jak i ich użytkownicy powinni odpowiednio zabezpieczyć się przed niechcianymi konsekwencjami korzystania z bota – ważne jest odpowiednie zabezpieczenie przed złośliwym oprogramowaniem botów nie tylko komputerów, ale również smartfonów i tabletów.

Na powstanie chatbota składa się kilka etapów: od ustalenia zapotrzebowania na automatyzację danego obszaru i rozpisanie możliwych scenariuszy, na podstawie których rozpoczyna się prace programistyczne, które prowadzą do powstania oprogramowania, kończąc na testach prawidłowego działania i jego analizie w celu wyłapania ewentualnych błędów.

Podobnie jak w przypadku umów dotyczących tworzenia i wdrożenia oprogramowania, umowy na stworzenie i wdrożenie chatbota powinny kompleksowo regulować powstanie, wdrożenie i obsługę takiej aplikacji. Oprócz kwestii technicznych powstania chatbota, umowy takie powinny także regulować przeniesienie praw lub udzielenie licencji na korzystanie z oprogramowania. Poza precyzyjnym określeniem przedmiotu przeniesienia autorskich praw majątkowych oraz pól eksploatacji, w umowie należy ustalić wysokość wynagrodzenia z tytułu przenoszonych praw. Twórcy oprogramowania najczęściej jednak zgadzają się na udostępnienie swoich programów w ramach licencji. Wynika to z pewnej powtarzalności programów, która sprawia, że ich twórcy, dokonując odpowiednich modyfikacji, są w stanie dostosować je do potrzeb danego użytkownika. Decydując się na udostępnienie programu w ramach licencji, przy licencjodawcy pozostają więc wszystkie prawa do programu i jego dokumentacji – może je więc dalej modyfikować, ulepszać, czy wykorzystywać poszczególne komponenty do tworzenia innego oprogramowania. Umowa o stworzenie chatbota będzie zatem umową o dzieło z elementami umowy o świadczenie usługi, jaką jest zapewnienie dostępu do oprogramowania. Utrzymanie bota w dobrej kondycji zwykle zapewnia umowa zlecenia, wdrożenie zaś najczęściej zawiera elementy obu umów.

Stworzenie botów do kontaktu z klientem pozwala na automatyzację części procesów w firmach, usprawniając proces obsługi oraz zapewniając oszczędność czasu i kosztów zatrudnianych pracowników. Prawidłowo zaprogramowany bot pozwala, pomimo automatyzacji, na indywidualne podejście do każdego klienta i dopasowanie do jego potrzeb. To zaś, jak boty będą wykorzystywane: do wspierania przedsiębiorców, czy urzędów, przyspieszając i poprawiając jakość obsługi klienta,

czy do nielegalnych działań - zależy od twórców botów, od ludzi. Przynajmniej tak długo, jak dzięki AI boty nie uzyskają faktycznego myślenia, czyli myślenia w sposób niesymulowany przez twórcę, przed którym to czarnym scenariuszem przestrzegali nas między innymi wybitni znawcy tematu sztucznej inteligencji.

AI twórcą, osobą, podmiotem praw?

Bot zwykle ma jakieś imię. Lubimy myśleć, że odpowiedzi w aplikacji bankowej udziela nam Anna, Siri lub Alexa, ale to oznacza, że personalizujemy AI. Stąd o krok do pytania o potencjalną podmiotowość prawną AI, w tym o jej zdolność do bycia podmiotem praw autorskich, czy wynalazczych. Nie jest to już pytanie czysto akademickie. Okazuje się, że sądownictwo niektórych państw dopuszcza możliwość przyznania sztucznej inteligencji statusu wynalazcy.

Dr Stephen Thaler, naukowiec i wynalazca z Missouri jest twórcą systemu sztucznej inteligencji zwanego DABUS (Device for the Autonomous Bootstrapping of Unified Sentience). System jest oparty na działaniu wielu sieci neuronowych i jest w stanie generować pomysły dzięki zmianom połączeń między nimi. Za pomocą system DABUS stworzono dwa rozwiązania: pojemnik na żywność oparty o geometrię fraktalną, którego powierzchnia posiada wiele wybrzuszeń, dzięki czemu możliwe jest korzystanie z wielu pojemników połączonych ze sobą oraz światło, które, rytmicznie pulsując ma naśladować aktywność neuronową człowieka.

Dr Thaler poszukiwał ochrony w różnych urzędach patentowych wskazując jako wynalazcę system DABUS, zaś siebie jako właściciela patentu na wynalazek stworzony przez system sztucznej inteligencji DABUS.

W USA, zarówno Urząd Patentów i Znaków Towarowych Stanów Zjednoczonych, jak i w następstwie odwołania, federalny sąd dla wschodniej Wirginii, odrzucił zgłoszenie patentowe Thalera, argumentując, że twórcą wynalazku może być wyłącznie człowiek. Z tego samego powodu dwa zgłoszenia patentowe Thalera, ze wskazaniem systemu sztucznej inteligencji jako wynalazcy, odrzucił Europejski Urząd Patentowy.

Przełomowy sukces dr Thaler odniósł w Republice Południowej Afryki, gdzie urząd patentowy przyznał Thalerowi patent na wynalazek stworzony przez DABUS – nowatorskie wykorzystanie geometrii fraktalnej. Australijski sąd federalny, pomimo odrzucenia zgłoszenia przez australijski urząd patentowy, orzekł, że system sztucznej inteligencji posiada zdolność do uznania go za twórcę wynalazku na gruncie australijskiego prawa patentowego, jednak tylko człowiek lub osoba prawna może być właścicielem patentu na taki wynalazek²².

²² <http://patentblog.kluweriplaw.com/2021/09/08/robots-are-taking-over-the-patent-world-ai-systems-or-devices-can-be-inventors-under-the-australian-patents-act/>, [dostęp 07.10. 2022]

Od przyznania sztucznej inteligencji statusu twórcy warto odróżnić przyznanie jej podmiotowości prawnej, czyli bycia podmiotem praw i obowiązków. Osobowość prawna to zdolność do samodzielnego, tj. we własnym imieniu, występowania w obrocie prawnym w charakterze podmiotu praw i obowiązków jako strona stosunku cywilnoprawnego. Przykładowo, w październiku 2017 r. obdarzony sztuczną inteligencją humanoidalny robot Sophia otrzymał obywatelstwo Arabii Saudyjskiej.

Stąd ciekawym i wartym rozważenia pomysłem jest przedstawiona przez Parlament Europejski koncepcja „elektronicznej osoby prawnej”²³ I tak, „mając na uwadze, że istnieje możliwość, że w perspektywie długoterminowej sztuczna inteligencja przewyższy ludzkie zdolności intelektualne” postuluje się „nadanie robotom specjalnego statusu prawnego w perspektywie długoterminowej, aby przynajmniej najbardziej rozwiniętym robotom autonomicznym można było nadać status osób elektronicznych odpowiedzialnych za naprawianie wszelkich szkód, jakie mogłyby wyrządzić, oraz ewentualne stosowanie osobowości elektronicznej w przypadkach podejmowania przez roboty autonomicznych decyzji lub ich niezależnych interakcji z osobami trzecimi”. Czy zatem jest to krok w kierunku uznania twórczości tworzącej skutek podejmowania przez roboty autonomicznych decyzji lub ich niezależnych interakcji z osobami trzecimi? Jak taka sytuacja wpłynie na nasze bezpieczeństwo w zetknięciu się ze sztuczną inteligencją?

23 Rezolucja Parlamentu Europejskiego z 16.2.2017 r. zawierająca zalecenie dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103(INL)), (Dz.Urz. UE C z 2018 r. Nr 252, s. 239); dalej jako: rezolucja 2015/2103