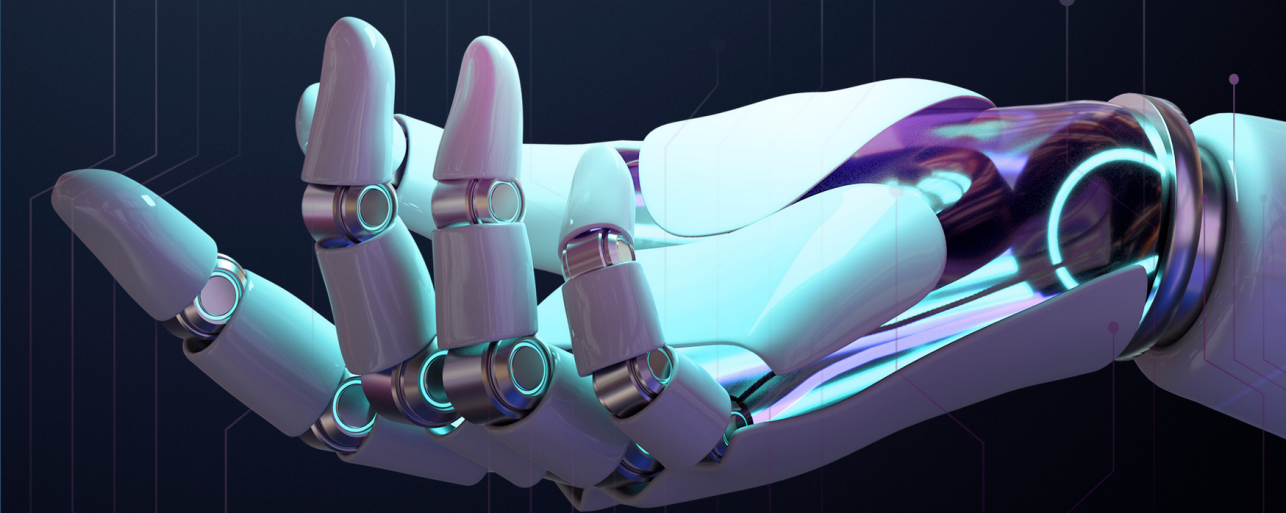
ARCHAEGRAPH
Wydawnictwo Naukowe

OCHRONA DANYCH OSOBOWYCH I SZTUCZNA INTELIGENCJA W PRAWIE POLSKIM I CHIŃSKIM

IGOR SZPOTAKOWSKI
MICHAŁ KALINOWSKI



Ochrona danych osobowych i sztuczna inteligencja w prawie polskim i chińskim

Tom I

Igor Szpotakowski

Michał Kalinowski


ARCHAEGRAPH
Wydawnictwo Naukowe
OCHRONA DANYCH OSOBOWYCH
I SZTUCZNA INTELIGENCJA
W PRAWIE POLSKIM I CHIŃSKIM
IGOR SZPOTAKOWSKI
MICHAŁ KALINOWSKI

Autorzy
Igor Szpotakowski
Michał Kalinowski

Recenzja
dr hab. Iwona Karasek-Wojciechowicz
dr hab. Michał Tomasz Lubina

Korekta redaktorska i skład
Karol Łukomiak
Diana Łukomiak

projekt okładki
Zuzanna Kopania

ISBN: 978-83-67074-19-3

Wersja elektroniczna dostępna na stronie internetowej wydawcy:
www.archaegraph.pl
oraz w Repozytorium Cyfrowym Biblioteki Narodowej
i profilach autorów w internetowych serwisach naukowych

ArchaeGraph
Wydawnictwo Naukowe

Łódź - Kraków 2021

Spis Treści

Przedmowa

Tom pt. „Ochrona danych osobowych i sztuczna inteligencja w prawie polskim i chińskim" stanowi pierwszy krok w dyskusji nad rozwojem badań na styku prawa nowych technologii i ochrony danych osobowych. Tematyka ta jest niezwykle ważna zarówno w Polsce, jak w Chinach, dlatego też właśnie te dwa kraje i porównywanie ich osiągnięć w tych dziedzinach stanowi cel niniejszej monografii, a także kolejnych, które zostaną opublikowane w późniejszym czasie. Tom ten został podzielony na dwie części stanowiące wprowadzenie i zarys poruszanej w tej książce problematyki. Pierwsza część, nosi tytuł „Ochrona danych osobowych w Polsce i w Chińskiej Republice Ludowej w zarysie" i stanowi próbę opisania, jak wyglądał system ochrony danych osobowych w Chińskiej Republice Ludowej do roku 2020, a także krytycznego porównania go z prawem polskim. Druga część, o tytule „Kontraktowa i deliktowa odpowiedzialność odszkodowawcza za działanie Sztucznej Inteligencji z uwzględnieniem problematyki czynów nieuczciwej konkurencji w świetle prawa polskiego", stanowi szersze spojrzenie na kwestie uregulowania w prawie polskim działań Sztucznej Inteligencji, które zostanie uzupełnione w kolejnym tomie o perspektywę chińską. Należy zwrócić uwagę, że stan prawny obu tych części to maj 2020 r., ponieważ głównym celem niniejszej monografii jest przedstawienie genezy pewnych współczesnych rozwiązań, co stanowić ma fundamenty dalszych prac w tej dziedzinie. Mamy nadzieję, że pierwszy tom stanowić będzie przyczynek do podjęcia szerszej dyskusji nad zmianami legislacyjnymi dotyczącymi tej tematyki, a także na dalszy rozwój badań prawnoporównawczych.

Igor Szpotakowski
Michał Kalinowski

Stan prawny: Maj 2020 r.

Ochrona danych osobowych w Polsce i w Chińskiej Republice Ludowej w zarysie[1]

1. Wprowadzenie i założenia metodologiczne

Ochrona danych osobowych jest tematem, który w ostatnich latach nabrał bardzo dużego znaczenia. Tematyka ta dotyczy każdego z nas, ale także jest motorem sukcesu wielu przedsiębiorstw na całym świecie, które wykorzystują te dane w celach marketingowych, poprawienia swoich usług i ich większej personalizacji czy po prostu lepszego poznania swoich klientów. Od kiedy świat stał się „globalną wioską", problematyka ta jest ważna nie tylko na rynkach lokalnych, lecz także w relacjach międzynarodowych, nawet pomiędzy tak oddalonymi od siebie geograficznie państwami, jak Polska i Chiny. Jednak wraz z globalizacją, pojawiły się także nowe problemy związane z przetwarzaniem danych osobowych, takie jak choćby odmienne rozumienie terminu prywatność.

W 2014 r. profesor Graham Greenleaf nazwał etap rozwoju prawa o ochronie danych osobowych w państwach azjatyckich „niemowlęcym"[2]. W roku 2020, takie określenie może wydawać się dziwne, ponieważ pierwsze przykłady takiego prawa sięgają lat 80 XX w. i japońskiej ustawy o sektorze publicznym z 1988 roku[3]. Jednak pierwszym krajem, który uregulował kompleksowo te kwestie w sektorze prywatnym, był dopiero Hongkong w 1995 r.[4]

Celem niniejszej pracy jest jednak analiza funkcjonowania systemów ochrony danych osobowych w dwóch państwach o odmiennych kulturach prawnych i społecznych, a mianowicie w Rzeczypospolitej Polskiej i w Chińskiej Republice Ludowej. Głównym problemem badawczym pracy jest omówienie najważniejszych wątków ochrony danych osobowych

---

[1] Igor Szpotakowski, Uniwersytet Jagielloński w Krakowie; ORCID ID: 0000-0001-8015-8614

[2] G. Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives,* Oxford 2014, s. 554.

[3] *Ibidem.*

[4] *Ibidem.*

w polsko-chińskich relacjach biznesowo-prawnych. Ze względu na złożoność głównego problemu badawczego autor niniejszej pracy sformułował szczegółowe problemy badawcze, które brzmią następująco:

- Jakie jest znaczenie pojęć ochrona danych osobowych oraz prawo ochrony danych osobowych?
- Czym różni się chińskie rozumienie koncepcji prywatności od europejskiego?
- Jak wygląda system ochrony danych osobowych w Polsce?
- Jak wygląda system ochrony danych osobowych w Chinach?
- Czym różnią się te dwa systemy?
- Co jest w tych systemach tożsame?
- Na jakich zasadach następować może przekazywanie danych osobowych pomiędzy Polską a Chinami?
- Jakie problemy dla kontaktów handlowych, prawnych czy naukowych pomiędzy III RP, a ChRL rodzi odmienne spojrzenie na ochronę danych osobowych?

Na podstawie postawionych problemów badawczych wysunięta została następująca hipoteza: Ochrony danych osobowych pełni bardzo ważną rolę w relacjach biznesowo-prawnych między Polską a Chinami.

Z hipotezy głównej wynikają hipotezy szczegółowe w następującym brzmieniu:

- Potrzeba ochrony danych osobowych wynika z koncepcji ochrony prywatności.
- W Polsce problematyka ochrony danych osobowych jest silniej uregulowana niż w Chinach
- Chińskie prawo ochrony danych osobowych pomimo różnić wynikających z innych realiów prawno-społecznych, powoli zaczyna przypominać europejskie ogólne rozporządzenie o ochronie danych

Podstawę napisania niniejszej pracy stanowiła szeroka literatura przedmiotu, zarówno ta polskojęzyczna, jak również źródła zagraniczne, głównie angielsko i chińskojęzyczne, a także akty prawne. Na szczególną uwagę zasługuje pozycja *Asian Data Privacy Laws: Trade & Human Rights Perspectives* autorstwa Grahama Greenleaf'a będąca pierwszą monografią naukową szczegółowo analizującą przepisy dotyczące ochrony danych osobowych i prawa do prywatności w Chinach i trzynastu innych azjatyckich państwach. Posiłkowałem się także licznymi komentarzami do Rozporządzenia o Ochronie Danych Osobowych i do Ustawy o ochronie danych osobowych, a także książką Pawła Fajgielskiego *Prawo ochrony danych osobowych. Zarys*

wykładu, w której syntetycznie omówiono podstawowe zagadnienia i konstrukcje prawne ochrony danych osobowych w Polsce i Unii Europejskiej.

Praca składa się z wprowadzenia, czterech rozdziałów i podsumowania. Rozdział pierwszy poświęcony jest odmiennemu rozumieniu pojęcia prywatności w chińskim i europejskim kręgu kulturowym.

Rozdział drugi, składający się z trzech części, przedstawia tematykę ochrony danych osobowych z perspektywy prawa polskiego. Pierwszy podrozdział przedstawia źródła prawa ochrony danych osobowych w Polsce. Drugi podrozdział skupia się zasadach i podstawach dopuszczalności przetwarzania danych osobowych w prawie polskim. Trzeci podrozdział dotyczy problematyki przekazywania danych osobowych do państw trzecich.

Trzeci rozdział, również składający się z trzech części, przedstawia tematykę ochrony danych osobowych z perspektywy prawa chińskiego. W pierwszym podrozdziale omówione zostaną źródła prawa ochrony danych osobowych w Chińskiej Republice Ludowej. Drugi podrozdział skupia się na zasadach przetwarzania danych osobowych i ich praktycznemu egzekwowaniu w prawie chińskim. Trzeci podrozdział dotyczy zaś możliwości i obostrzeń co do przekazywania danych osobowych poza granice ChRL.

W czwartym rozdziale zostały zebrane charakterystyczne różnice pomiędzy oboma porządkami prawnymi, a także problemy z tych różnic wynikające. Pierwszy podrozdział dotyczy różnic wynikających z regulowania ochrony danych osobowych za pomocą prawa administracyjnego oraz prawa cywilnego. W podrozdziale drugim została przedstawiona pokrótce problematyka tzw. prawa do prywatności funkcjonującego w Polsce i w Chinach. W podrozdziale trzecim zostały opisane rozważania na temat zapewnienia odpowiedniego stopnia ochrony danych osobowych w Chinach.

W niniejszym tekście, w odpowiednim zakresie wykorzystano metody: opisową, historyczną i komparatystyczną. Wszystkie tłumaczenia chińskich aktów i przepisów prawnych, jakie zostały zawarte w tej części, zostały przetłumaczone z języka chińskiego na polski samodzielnie przez autora, chyba że w przypisie zaznaczono inaczej.

2. Pojęcie prywatności w chińskim i europejskim kręgu kulturowym

Koncept prywatności ma długą i niezwykle zróżnicowaną historię w różnych kręgach kulturowych na przestrzeni wieków. Koncepcja prywatności nie raz inspirowała do głębszych przemyśleń filozofów, poetów, prawników,

polityków, kulturoznawców czy antropologów. Nie sposób jest wskazać jednej wyczerpującej definicji prywatności, choć wiele takich definicji tworzono w różnych czasach i różnych miejscach. Różnice co do granic tego pojęcia szczególnie widoczne są w odległych od siebie kręgach cywilizacyjnych. W tym rozdziale postaram się przedstawić różne koncepcje prywatności znane w Europie i innych krajach kultury Zachodu, a także opisać odmienną w wielu aspektach chińską perspektywę rozumienia prywatności. Rozważania te będą stanowiły podstawę teoretyczną dla kolejnych rozdziałów tej pracy.

W Europie, już w antycznej Grecji, Arystoteles w swojej rozprawie *Polityka* oddzielał sferę publiczną związaną z działalnością polityczną (*polis*) od sfery prywatnej (*okis*) kojarzonej z życiem codziennym, a także pojęciem domu i rodziny[5]. Warto jednak podkreślić, że Arystoteles patrzył na prywatność z perspektywy indywidualnej jednostki, a jego punkt widzenia był kontynuowany przez następne stulecia wśród rzymskich poetów, takich jak Horacy, Wergiliusz, Klaudian czy Marcjalis, którzy wychwalali ideał zacisznego życia na wsi[6], jako miejsca funkcjonowania jednostki, a nie grupy. W pewnym sensie to indywidualistyczne spojrzenia na koncept prywatności straciło na znaczeniu wraz z upadkiem Cesarstwa Rzymskiego, gdy w okresie średniowiecza za sprawą Kościoła Katolickiego pojawił się w VI wieku na Wyspach Brytyjskich (głównie na terenie Irlandii i Szkocji) koncept „spowiedzi indywidualnej" (*confessio*), który około VIII wieku rozpowszechnił się też w innych częściach Europy[7]. W czasie spowiedzi wymagano, aby wszystkie sekrety i przestępstwa zostały ujawnione kapłanowi, przez co też w Europie sfera prywatności i ludzkich tajemnic została znacznie ograniczona, nawet dla możnowładztwa[8]. Kolejnym powodem prawie całkowitego zaniku współczesnego nam rozumieniu pojęcia prywatności i indywidualizmu w średniowieczu było głównie relatywne ubóstwo oraz fakt, że większość ludzi żyła na granicy przetrwania[9]. W ówczesnym sposobie życia nie było nawet dosłownie miejsca na prywatność czy indywidualizm. Ciasne pomieszczenia mieszkalne i brak centralnego ogrzewania były przyczyną zbliżania się do siebie ludzi[10]. Niektórzy możnowładcy posiadali nawet ogromne łoża, które pozwalały włodyce, jego

5 M. R. Dowding, *Privacy: Defending an illusion*, Plymouth 2011, s. 1.
6 *Ibidem*, s. 4
7 H. Krzysteczko, *Od publicznej praktyki pokutnej do spowiedzi prywatnej*, Śląskie Studia Historyczno-Teologiczne 29(1996), s. 323, 333.
8 M. R. Dowding, *op. cit.*, s. 4.
9 J. F. Dunningan, A. A. Nofi, *Medieval Life and the Hundred Years War: Medieval Society and Culture*, 1997, http://www.hundredyearswar.com/Books/History/1_help_c.htm [dostęp: 26.01.2020 r.]
10 *Ibidem*.

małżonce, dzieciom, najbliższym sługom i najwierniejszym członkom drużyny spać razem w środku zimy wzajemnie się ogrzewając[11].

Również końcówka XV wieku i początek XVI w. wraz z wyprawami odkrywców, konkwistadorów i poszukiwaczy przygód do obu Ameryk przyniosły świeże spojrzenie na koncepcję prywatności. Europejczycy odkrywając Nowy Świat byli zaskoczeni, gdy odkryli, że natywni mieszkańcy tamtych terenów żyją bez „europejskiej koncepcji prywatności" zapewnianej poprzez noszenie ubrań[12]. W tym też czasie w Europie prywatność zaczyna się powoli przemieniać w indywidualizm jednostki, zakorzeniony jednak wciąż w hierarchii stanowej[13]. W Anglii pomiędzy XVI, a XVIII wiekiem najbardziej oczywistym tego przykładem stał się ewolucyjny rozwój architektury budynków mieszkalnych przedstawicieli wyższych warstw społecznych. Nowy styl budownictwa pozwalał na większe odosobnienie jednostki, a zatem też na większą prywatność, poprzez na przykład osobne pokoje do przebierania się[14]. Amanda Vickery wysnuła tezę, że w tamtym okresie dla bogatych dostęp do prywatność był swoistym wyznacznikiem wpływów jakie ktoś posiadał[15].

Art. X. francuskiej Deklaracji Praw Człowieka i Obywatela z 26 sierpnia 1789 r. stanowił, że „nikt nie powinien być niepokojony z powodu swych przekonań, nawet religijnych, byleby tylko ich objawianie nie zakłócało ustawą zakreślonego porządku publicznego". Postulat ten był w pewnym sensie próbą wskazania pewnych granic prywatności rozumianych w tamtym okresie. Jednak tak naprawdę zagadnienia dotyczące prawa do prywatności i sposobów jej ochrony zaczęły się rozwijać dopiero od końca XIX wieku[16]. Po raz pierwszy pewna forma zdefiniowania i ustalenia granic prawa do prywatności pojawiła się w 1890 r., kiedy dwóch amerykańskich prawników Samuel Warren i Louis Brandeis, określiło ją jako uprawnienie do wyłączności, odrębności tajemnicy i samotności (*a right to be alone*) w artykule *The Right to Privacy* opublikowanym w *Harvard Law Review*[17]. Z kolei w 1907 r. Joseph Kohler zdefiniował pojęcie prywatności jako swobodę rozporządzania informacjami

11 *Ibidem*.
12 M. R. Dowding, *op. cit.*, s. 5.
13 *Ibidem*.
14 *Ibidem*.
15 A. Vickery, *An Englishman's Home is His Castle?,* Past & Present, Volume 199, Issue 1, May 2008, s. 167.
16 M. Pryciak, *Prawo do prywatności*, Wrocławskie Studia Erazmiańskie, 2010, zeszyt IV: Prawa człowieka - idea, instytucje, krytyka, s. 213.
17 S.D. Warren, L. Brandeis, *The Right to Privacy*, Harvard Law Review, vol. IV, December 1890, s. 193–220

na swój temat, w odniesieniu jednak głównie do tajemnicy korespondencji[18]. Z powodu wojen światowych i wykształcenia się systemów totalitarnych, w Europie Zachodniej okres po zakończeniu II wojny światowej stał się czasem wzmacniania praw człowieka, więc także prawa do prywatności[19]. Dzięki temu ochrona sfery życia prywatnego zaliczana jest przez akty międzynarodowe dotyczące praw człowieka do katalogu praw fundamentalnych, a zatem chronionych[20].

Artykuł 12 Powszechnej Deklaracji Praw Człowieka stanowi: „Nikt nie będzie poddany arbitralnemu wkraczaniu w jego życie prywatne, rodzinę, mieszkanie lub korespondencję, ani też zamachom na jego honor i reputację. Każdy jest uprawniony do ochrony prawnej przed takim wkraczaniem lub takimi zamachami"[21].

Artykuł 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych określa, że: „Nikt nie będzie poddany arbitralnej lub bezprawnej ingerencji w jego życie prywatne, rodzinne, mir domowy czy korespondencję, ani też bezprawnym zamachom na jego część i dobre imię" i „każdy ma prawo do ochrony prawnej przed tego rodzaju ingerencją lub zamachami"[22].

Artykuł 8 Europejskiej Konwencji Praw Człowieka natomiast posiada najbardziej rozbudowaną regulację opisywanych zagadnień, stanowiąc, że:

„1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji.

2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne oraz dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób"[23].

Obecnie ochrona prywatności ściśle koresponduje z systemem ochrony informacji i danych osobowych (w tym danych medycznych), jakie przez różne instytucje publiczne i prywatne są gromadzone i przetwarzane[24]. Specyficzne

---

18 M. Pryciak, *op. cit.*, s. 213.
19 *Ibidem*, s. 220.
20 *Ibidem*, s. 218.
21 *Powszechna Deklaracja Praw Człowieka* z 10 grudnia 1948 r.
22 *Międzynarodowy Pakt Praw Obywatelskich i Politycznych* otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. 1977 nr 38 poz. 167).
23 *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności* sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2. (Dz.U. 1993 nr 61 poz. 284).
24 *Ibidem*, s. 224.

są jednak przejawy realizacji prawa do prywatności w sferze obrotu gospodarczego, która odbywa się z pewnymi odrębnościami w porównaniu z korzystaniem ze swojej prywatności w innych sferach życia człowieka. Przede wszystkim w obrocie gospodarczym mamy do czynienia z prywatnością w wymiarze indywidualnym przy jednoczesnej minimalizacji realizowania prawa do życia rodzinnego[25].

Jeśli chodzi o chińską koncepcję rozumienia prywatności, to warto na wstępie zauważyć, że zwyczajowo społeczeństwu chińskiemu przypisuje się cechy związane z wymiarem kolektywnym. Chińczycy są uważani za ludzi o wiele mniej indywidualistycznych od ludzi Zachodu, a społeczeństwo chińskie — za przykład społeczeństwa w wysokim stopniu kolektywistycznego[26]. Cechą charakterystyczną społeczeństwa chińskiego jest zwracanie uwagi na to jaki wpływ ma działanie danej jednostki na poszczególnych członków wspólnoty[27].

Chińska tradycja prawna oparta jest na kolektywizmie, którego źródeł możemy szukać w systemie patriarchalnym i scentralizowanym nacjonalizmie[28]. System patriarchalny został ukształtowany przez obyczaje, które regulowały stosunki panujące w rodzinie, a scentralizowany nacjonalizm wynikać może z autorytatywności władzy w Państwie Środka[29]. Odosobnienie jednostki, o którym wspominałem wyżej w kontekście architektury XVIII wiecznej Anglii, nie byłoby dobrze postrzegane w społeczeństwie chińskim i kolektywistycznym podejściem.

Dobrym przykładem braku prywatności w sferze publicznej w Chinach cesarskich może być fakt, że anonimowy donos lub pozew był w surowo karany. Artykuł 351 Kodeksu Tang pochodzącego z 624 roku głosił, że: „Wszystkie przypadki, w których wniesiono anonimowo pisemną skargę do sądu oskarżając inną osobę o popełnienie przestępstwa będą karane dożywotnim wygnaniem na odległość 3000 li (646 km)[30]". Każdy zaś kto otrzymałby taki dokument powinien go niezwłocznie spalić, gdyż jeśli tego nie zrobi i zaniesie go do sądu, bądź innego budynku urzędowego zostanie skazany na rok

---

[25] K. Machowicz, *Prawo do prywatności realizowane w sferze obrotu gospodarczego*, w: *Praktyka ochrony praw człowieka*, red. Kinga Machowicz, t. I, Lublin, 2012, s. 124.

[26] K. Sarek, *Zanikający chiński kolektywizm — przyczyny zmian w mentalności i zachowaniu młodych Chińczyków*, Roczniki Humanistyczne, Tom LXVI, zeszyt 9, 2018, s. 112.

[27] G. Hofstede, *Culture's Consequences: Comparing Values, Behaviours, Institutions, and Organizations Across Nations*, Londyn 2001, s. 209-278.

[28] M. Dargas, *Idee i zasady konstytucyjne chińskiego porządku prawnego*, Warszawa 2017, s. 114.

[29] *Ibidem.*

[30] *1 li* (里) jest równe około 0,5 km, podaje to w sekcji „Skróty" W. Johnson w książce *The T'ang Code, Volume I, General Principles*, Princeton, New Jersey 1979.

katorgi, zaś urzędnik, który taki dokument przyjmie i uzna za legalny poniesie karę dwóch lat katorgi[31]. A zatem jedynie oskarżony, jako jedyna zaangażowana w sprawę osoba nie zostanie ukarany, nawet jeśli treść skargi, jak również oskarżenie o popełnienie przestępstwa były prawdziwe, co dobitnie wskazuje, że w cesarskich Chinach w sferze publicznej nie było miejsca na prywatność.

Publikacje naukowe powstałe w latach 80. i 90. ubiegłego wieku, oparte na badaniach empirycznych zachowań i działań potwierdzały intuicyjną ocenę Chińczyków jako ludzi bardziej zorientowanych kolektywistycznie niż indywidualistycznie[32]. Jednak Cheung Kwok Wah i Pan Suyan udowodnili w swoich badaniach, że w okresie od 1980 do 2005 r. zaszły poważne zmiany w podejściu władz oświatowych do zakresu kształcenia dzieci i młodzieży, jak i stopnia wolności nauczycieli w zakresie zmian w programie nauczania, które wpływają na późniejszą mentalność młodych Chińczyków[33]. W wyniku długotrwałych zmian, w Chińczykach wykształcił się tzw. regulowany indywidualizm (regulated individualism), w którym jednostka ani nie jest całkowicie podporządkowana kolektywowi, ani nie cieszy się całkowitą wolnością od presji kolektywu czy państwa[34]. Państwo stopniowo pozwala na coraz większy zakres wolności i pozwala jednostkom na stosunkowo swobodną realizację własnych celów, ale zakres ten jest dostosowywany do socjo-politycznych i ekonomicznych warunków, a jest zwiększany jedynie do tego momentu, gdy nie zagraża interesowi kolektywu[35].

W obecnym chińskim porządku prawnym, o którym szerzej będzie mowa w rozdziale piątym, jednakże warto wspomnieć, że w Konstytucji Chińskiej Republiki Ludowej z roku 1982 art. 40, który dotyczy prawa do prywatności, stanowi, że niedopuszczalne jest bezprawne przeszukiwanie i wtargnięcie do miejsca zamieszkania obywateli, a obywatele mają prawo do wolności i tajemnicy korespondencji[36]. Jednak cenzurowanie korespondencji jest dozwolone w wyjątkowych sytuacjach na potrzeby bezpieczeństwa państwa lub postępowania sądowego[37].

---

31 W. Johnson, *The T'ang Code, Volume II, Specific Articles*, Princeton, New Jersey 1997, s. 403.

32 S.G. Redding, *Cognition as an Aspect of Culture and Its Relation to Management Process: An Exploratory View of the Chinese Case*, Journal of Management Studies 17 (1980), no. 2, s 127–148.

33 Kwok Wah Cheung, Suyan Pan, *Transition of Moral Education in China: Towards Regulated Individualism*, Citizenship Teaching and Learning 2 (2006), no. 2/2, s. 37-50.

34 K. Sarek, *op. cit.*, s. 114.

35 *Ibidem*.

36 Konstytucja Chińskiej Republiki Ludowej z dnia 4 grudnia 1982 r.

37 *Ibidem*.

Współczesne prawa obywateli ChRL są bowiem nierozerwalnie związane z władzą państwową[38]. Państwowa inwigilacja dotyka w mniejszym lub większym stopniu prawie każdego aspektu życia w chińskim społeczeństwie[39]. Tym co nie ma pozwala w Chinach na zachowanie dostatecznej anonimowości i wpływa też na koncepcje prywatności jest system zameldowania hukou wprowadzony w 1958 roku w Państwie, który pozostaje do dziś kluczem do kontrolowania i ograniczania możliwości przemieszczania się obywateli ChRL w obrębie kraju[40].

Podsumowując, europejska i chińska koncepcja prywatności różnią się od siebie w pewnych aspektach. Ta europejska połączona jest z pojęciem indywidualności, oddzielona od sfery publicznej państwowej, która nie powinna przenikać zbyt mocno do sfery prywatnej. Ta chińska koncepcja jest połączona z ideą kolektywizmu, silnej pozycji państwa i rodziny. Jej granice są węższe od tej prywatności znanej w Europie, ze względu na fakt, że ważniejszy jest kolektyw od jednostki, która stanowi tylko jego część. Warto zaznaczyć, że powyższe rozważania stanowią tylko wprowadzenie do problematyki prywatności i ochrony danych osobowych w Polsce oraz w Chinach i będę kontynuowane w kolejnych rozdziałach.

3. Ochrona danych osobowych w prawie polskim

3. 1. Źródła prawa

Analizę problematyki ochrony danych osobowych w prawie polskim należy zacząć od nakreślenia granic obowiązywania i wskazanie określonego zbioru przepisów, które tej tematyki dotyczą. Dlatego też, rozdział ten rozpoczynam od szerszego opisania źródeł prawa ochrony danych osobowych w Rzeczypospolitej Polskiej.

Zgodnie z ustępem 1 art 87 Konstytucji RP źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia[41]. Dlatego też w pierwszej kolejność sięgniemy po artykuł 47 Konstytucji RP, który kształtuje ogólną zasadę ochrony prywatności, w którego myśl

38 M. Dargas, *op. cit.*, 236.
39 G. Greenleaf, *op. cit.*, s. 195.
40 *Ibidem*.
41 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483).

> „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”[42].

Najważniejszy jednak jest artykuł 51 Konstytucji RP, który stanowi w obecnym stanie prawnym ogólną podstawę ochrony osób w związku z przetwarzaniem danych osobowych w naszym kraju[43]. Jego treść znajduje się poniżej:

> „1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
> 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
> 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
> 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
> 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.”

Wynika z tego, że szczegółowych przepisów co do ochrony danych osobowych powinniśmy szukać w ustawie. Jednak ze względu na fakt, że Polska jest krajem członkowskim Unii Europejskiej, to zgodnie z art. 91 Konstytucji RP:

> „3. Jeżeli wynika to z ratyfikowanej przez Rzeczpospolitą Polską umowy konstytuującej organizację międzynarodową, prawo przez nią stanowione jest stosowane bezpośrednio, mając pierwszeństwo w przypadku kolizji z ustawami.”

W związku z tym, od 25 maja 2018 r. podstawowym aktem normatywnym regulującym problematykę ochrony danych osobowych, który wiąże wszystkie państwa członkowskie UE i jest stosowany bezpośrednio jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (RODO)[44].

---

42 *Ibidem.*

43 P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu*, Warszawa 2019, s. 32.

44 P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu*, Warszawa 2019, s. 34-35.

Z uwagi na fakt, że RODO nie wprowadza pełnej harmonizacji w zakresie regulacji zasad ochrony danych osobowych, rozumianej jako zupełne ukształtowanie regulacji danego obszaru przedmiotowego, bez dopuszczalności stosowania regulacji na poziomie krajowym, konieczne stało się uchwalenie ustawy z 10 maja 2018 r. o ochronie danych osobowych[45]. Na gruncie RODO mamy do czynienia bowiem z harmonizacją częściową, w przypadku której państwa członkowskie, takie jak Polska, posiadają uprawnienie do swobodnej samoregulacji w zakresie, którego przepisy RODO nie obejmują[46].

To co zostało zawarte w ustawie, a czego nie uregulowano w unijnym rozporządzeniu, to m.in.: kwestia wyłączeń i ograniczeń stosowania niektórych przepisów unijnego rozporządzenia; regulacje dotyczące organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych oraz kwestii proceduralnych dotyczących prowadzonych przez niego postępowań kontrolnych i postępowań w sprawie naruszenia przepisów, a także nakładania administracyjnych kar pieniężnych oraz wielu kwestii szczegółowych (określenia podmiotów publicznych obowiązanych do wyznaczenia inspektora ochrony danych; warunków i trybu akredytacji podmiotu uprawnionego do certyfikacji; trybu zatwierdzenia kodeksu postępowania; trybu europejskiej współpracy administracyjnej; odpowiedzialności za naruszenie przepisów o ochronie danych osobowych)[47].

Drugim elementem jest wprowadzona na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 r. „w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych (tzw. dyrektywa policyjna)", ustawa z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[48]. Nie ma ona jednak znaczenia z perspektywy celu niniejszego tekstu

45 *Ustawa o ochronie danych osobowych*, red. P. Litwiński, Warszawa 2018, s. 2.
46 *Ibidem.*
47 P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu*, Warszawa 2019, s. 36.
48 Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. 2019 poz. 125).

ze względu na to, że dotyczy ona przetwarzania danych osobowych m.in. przez policję, prokuraturę i sądy (art. 1 pkt. 1)[49].

3. 2. Zasady i podstawy dopuszczalności przetwarzania danych osobowych

Znając już źródła prawa, kolejnym etapem jest omówienie zasad i podstaw dopuszczalności przetwarzania danych osobowych w Polsce.

3. 2. 1. Zasady przetwarzania danych osobowych

Zasady przetwarzania danych osobowych zostały uregulowane na poziomie unijnym i znajdują się w artykule 5 RODO. Zgodnie z ustępem pierwszym dane osobowe muszą być:

> „a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");
> b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("ograniczenie celu");
> c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych");
> d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");
> e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu

[49] Art. 1. Ustawa określa: 1) zasady i warunki ochrony danych osobowych przetwarzanych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności.

ochrony praw i wolności osób, których dane dotyczą ("ograniczenie przechowywania");
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").[50]"

Prawodawca unijny wskazał w art. 5 RODO następujące normatywne zasady przetwarzania danych. Te zasady to: zasada legalności, rzetelności i przejrzystości, zasada ograniczenia celu, zasada minimalizacji danych, zasada prawidłowości (poprawności danych), zasada ograniczenia przechowywania danych, zasada integralności i poufności (bezpieczeństwa) danych, a także w ustępie drugim[51] zasadę rozliczalności[52].

W art. 5 ust. 1 lit. a RODO wskazano zasadę przetwarzania danych zgodnie z prawem, nazywaną również zasadą legalności. Zdaniem Arlety Nerki usytuowanie zasady legalności na samym początku przepisu, bezsprzecznie wskazuje na jej nadrzędny charakter, szczególnie biorąc pod uwagę jej merytoryczny związek z zasadą rzetelności[53]. Zgodnie z komentarzem Pawła Litwińskiego do art. 5 RODO, „rzetelność przy przetwarzaniu danych osobowych rozumiana bywa także jako nakaz przetwarzania danych osobowych zgodnie z regułami uczciwości, rozumianymi jako poszanowanie interesów osób, których dane dotyczą, i niewykorzystywanie ich przymusowej sytuacji"[54]. Paweł Litwiński za przykład podaje angielską sprawę *British Gas Trading Limited v Data Protection Registrar*[55] z 1998 r., w której przyjęto, że *British Gas Trading*, monopolista na rynku brytyjskim, narusza obowiązek rzetelnego przetwarzania danych osobowych, poprzez udostępnianie ich dla celów marketingowych

[50] Art. 5 *Rozporządzenia Parlamentu Europejskiego 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).*

[51] Art. 5 ust. 2. RODO: Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

[52] A. Nerka, *Art. 5,* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, M. Sakowska-Baryła (red.), Warszawa 2018, dostępny w: http://www.legalis.pl, [dostęp: 21.03.2020 r.]

[53] *Ibidem*.

[54] P. Litwiński, *Art. 5*, [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, P. Litwiński(red.), Warszawa 2018, dostępny w: http://www.legalis.pl, [dostęp: 21.03.2020 r.].

[55] http://informationrights.decisions.tribunals.gov.uk//DBFiles/Decision/i162/british_gas.pdf, [dostęp: 21.03.2020 r.].

innym podmiotom bez wyraźnej zgody osób, których dane dotyczą, a jedynie opierając się na braku sprzeciwu[56]. Zasadę przejrzystości odczytuje się jako warunek dokonywania operacji przetwarzania danych osobowych w sposób transparentny dla podmiotów danych[57].

Zasad ograniczenia celu przetwarzania oznacza, że zbieranie danych osobowych powinno się odbywać w konkretnych, wyraźnych i prawnie uzasadnionych celach, a po ich zebraniu nie może przetwarzać ich w sposób niezgodny z celem, dla którego zostały zebrane[58]. Dopełnieniem jest zasada minimalizacji danych, które powinny być adekwatne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane[59], a zatem jeśli do osiągnięcia konkretnego celu potrzebujemy tylko czyjeś imię, nazwisko i datę urodzenia, to nie możemy prosić też o podanie numeru PESEL, bo nie jest on niezbędny.

Zasada (merytorycznej) prawidłowości została określona w artykule 5 ust. 1 lit. d RODO, stanowi on, że dane powinny być zgodne z istniejącym stanem rzeczywistym, więc prawidłowe i w razie potrzeby uaktualniane[60]. Zasada ograniczenia przechowywania danych zabezpiecza osobę, której dane dotyczą, przed przetwarzaniem jej danych osobowych przez nieograniczony okres czasu, dane powinny przez okres nie dłuższy, niż jest to niezbędne do celów, w których są przetwarzane[61]. Warto jednak wspomnieć, że po osiągnięciu przez administratora danych osobowych zakładanego celu ich przetworzenia, możliwe jest ich dalsze przetwarzanie, jednak wyłącznie w formie pozbawionej cech umożliwiających określenie za ich pomocą tożsamości osoby (anonimizacja danych)[62].

Art. 5 ust. 1 litera f RODO określa zasadę integralności i poufności danych zgodnie z którą dane są przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych (jak programy szyfrujące dane, trzymanie danych w chmurze, itd.) lub organizacyjnych, a zgodnie z zasadą rozliczalności administrator jest odpowiedzialny za przestrzeganie omówionych wcześniej zasad dotyczących przetwarzania danych

56 P. Litwiński, *Art. 5, op cit,* dostępny w: http://www.legalis.pl, [dostęp: 21.03.2020 r.].
57 A. Nerka, *Art. 5, op. cit.,* dostępny w: http://www.legalis.pl, [dostęp: 21.03.2020 r.].
58 P. Litwiński, *Art. 5*, *op cit,* dostępny w: http://www.legalis.pl, [dostęp: 21.03.2020 r.].
59 A. Nerka, *Art. 5, op. cit.,* dostępny w: http://www.legalis.pl, [dostęp: 21.03.2020 r.].
60 *Ibidem*.
61 P. Litwiński, *Art. 5*, *op cit,* dostępny w: http://www.legalis.pl, [dostęp: 21.03.2020 r.].
62 *Ibidem*.

i musi być w stanie wykazać realizację tego obowiązku w trakcie audytu lub postępowania przed Urzędem Ochrony Danych Osobowych (UODO)[63].

3. 2. 2. Podstawy przetwarzania danych osobowych

W RODO w art. 6 nastąpiło wskazanie podstaw, na których może opierać się przetwarzanie danych osobowych w odniesieniu do danych osobowych zwykłych, a w art. 9 w odniesieniu do szczególnych kategorii danych osobowych[64]. Ze względu na specyfikę tej pracy, skupię się głównie na przetwarzaniu danych zwykłych z art. 6.

W art. 6 RODO wskazano podstawy dopuszczalności przetwarzania danych, w postaci przesłanek, jakie powinny być spełnione i w ten sposób prawodawca unijny zezwolił na przetwarzanie danych jedynie wówczas, gdy administrator legitymuje się jedną ze wskazanych w przepisach podstaw uprawniających go do tego[65]. Przetwarzanie danych osobowych nie posiadając odpowiedniej podstawy prawnej jest niedopuszczalne i stanowi naruszenie przepisów o ochronie danych osobowych, za co grożą wysokie kary pieniężne[66].

W konsekwencji do warunków prawnych przetwarzania danych osobowych należą:

1) zgoda podmiotu danych;
2) wykonanie lub zawarcie umowy;
3) prawny obowiązek;
4) ochrona żywotnych interesów;
5) wykonywanie zadania publicznego lub władzy publicznej;
6) prawnie uzasadniony interes administratora lub strony trzeciej[67].

Jak wskazuje Paweł Fajgielski pośród wskazanych powyżej przesłanek, szczególną rolę odgrywa przesłanka pierwsza, czyli zgoda osoby, której dane dotyczą[68]. Istnieją dwa modelowe rozwiązania co do konstrukcji prawnej wyrażenia zgody na przetwarzanie danych osobowych: *opt-in*, zakładająca konieczność złożenia oświadczenia o wyrażeniu zgody lub *opt-out*, w której brak sprzeciwu oznacza zgodę[69]. Prawodawca unijny przyjął opcję *opt-in*, czyli bezpośrednie, a nie dorozumiane wyrażenie zgody.

---

63 A. Nerka, *Art. 5, op. cit.,* dostępny w: http://www.legalis.pl, [dostęp: 21.03.2020 r.].
64 P. Litwiński, *Art. 6*, op *cit,* dostępny w: http://www.legalis.pl, [dostęp: 21.03.2020 r.].
65 P. Fajgielski, *op. cit.,* s. 77.
66 *Ibidem.*
67 M. Sakowska-Baryła, A. Nerka, *Art. 6, op. cit.,* dostępny w: http://www.legalis.pl, [dostęp: 21.03.2020 r.].
68 P. Fajgielski, *op. cit.,* s. 77.
69 *Ibidem.*

3. 3. Przekazywanie danych do państw trzecich

Poza określeniem podstaw dopuszczalności przetwarzania danych osobowych, prawo unijne zawiera również unormowania dotyczące przekazywania, czy inaczej transferu danych osobowych do państw trzecich. Unijny prawodawca wychodzi bowiem ze słusznego założenia, że ustalenie pewnych norm przekazywania danych jest konieczne, by nie dopuścić do pozbawienia ochrony osób, których dane zostaną przekazane poza terytorium Europejskiego Obszaru Gospodarczego[70], gdzie standardy unijne transferu danych nie są przestrzegane[71]. Państwa trzecie to wszystkie państwa nienależące do Europejskiego Obszaru Gospodarczego, a zatem również jest takim państwem trzecim Chińska Republika Ludowa.

Problematykę przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych reguluje rozdział V RODO, w artykułach od 44 do 50. Zgodnie z tymi przepisami transfer danych osobowych do państwa trzeciego dopuszczalny jest tylko wtedy, gdy zostanie spełniona jedna ze wskazanych poniżej przesłanek:

1) istnieje decyzja Komisji stwierdzająca, że państwo trzecie, terytorium lub określony sektor w tym państwie trzecim zapewniają odpowiedni poziom ochrony[72];

2) razie braku decyzji na mocy art. 45 RODO, administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego wyłącznie, gdy zostaną zapewnione odpowiednie zabezpieczenia w postaci jednego z następujących instrumentów prawnych: prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi; wiążących reguł korporacyjnych; standardowych klauzul ochrony danych przyjętych przez Komisję lub organ nadzorczy; zatwierdzonego kodeksu postępowania; zatwierdzonego mechanizmu certyfikacji, bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego albo klauzul umownych lub uzgodnień administracyjnych, za zgodą organu nadzorczego, pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej[73];

---

70 Są to: Austria, Belgia, Bułgaria, Chorwacja, Cypr, Czechy, Dania, Estonia, Finlandia, Francja, Grecja, Hiszpania, Holandia, Irlandia, Islandia, Liechtenstein, Litwa, Luksemburg, Łotwa, Malta, Niemcy, Norwegia, Polska, Portugalia, Rumunia, Słowacja, Słowenia, Szwecja, Węgry, Włochy.

71 P. Fajgielski, *op. cit.*, s. 95.

72 *Ibidem*, s. 95-98.

73 *Ibidem.*

3) znajdzie zastosowanie jeden z wyjątków przewidzianych w szczególnych sytuacjach, określonych w art. 49 RODO, kiedy to transfer danych osobowych nie może się opierać na przesłankach wskazanych w punktach wcześniejszych, ze względu, że tamte przesłanki nie zostały spełnione[74]. Nie będę tych wyjątków jednak szerzej w tej pracy omawiać, ze względu, że nie wiążą się one bezpośrednio z jej tematyką.

Przekazanie danych osobowych do państwa trzeciego, zgodnie z art. 45 ust. 1 RODO, może nastąpić, gdy Komisja Europejska stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie zapewniają odpowiedni stopień ochrony[75]. Na moment pisania tej książki Komisja Europejska wydała takie decyzje w stosunku do następujących państw i terytoriów, takich jak: Andora, Argentyna, Kanada, Wyspy Owcze, Jersey, Izrael, Wyspa Man, Japonia, Jersey, Nowa Zelandia, Szwajcaria, Urugwaj oraz Stany Zjednoczone Ameryki, natomiast obecnie toczą się negocjacje nad dołączeniem do tej listy Korei Południowej[76].

Nie ma wśród wymienionych Chińskiej Republiki Ludowej, co znaczy, że aby przesłać dane osobowe z terenu Unii Europejskiej do Chin, należy zapewnić odpowiednie zabezpieczania wymienione powyżej w punkcie 2 i 3.

4. Ochrona danych osobowych w prawie chińskim

4. 1. Źródła prawa

W rozdziale trzecim zajmę się opisaniem systemu ochrony danych osobowych w Chińskiej Republice Ludowej. Tak jak w rozdziale drugim, analizę należy rozpocząć od przedstawienia źródeł prawa ochrony danych osobowych w Państwie Środka.

W teorii najważniejszym aktem prawa w większości krajów na świecie, regulującym prawa i obowiązki obywateli, a także podstawowe zasady funkcjonowania państwa jest konstytucja[77]. Również Konstytucja Chińskiej Republiki Ludowej w rozdziale drugim „Podstawowe prawa i obowiązki obywateli"

---

74 *Ibidem.*

75 Artykuł 45 ust. 1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

76 *Adequacy decisions,* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#relatedlinks [dostęp: 21.03.2020 r.]

77 M. Elliot, R. Thomas, *Public Law*, Oxford 2017, s. 4.

(art. 33-40) określa takie prawa jak: wolność osobista, godność, tajemnica prywatnej korespondencji, a także zakaz bezprawnej rewizji lub wtargnięcia do miejsca zamieszkania obywatela[78]. W przeciwieństwie do wielu innych krajów, w tym Polski, są to jednak bardziej idee niż zasady prawne. Wyrok Najwyższego Sądu Ludowego z 2001 r. w szeroko komentowanej sprawie Qi Yuling przeciwko Chen Xiaoqi, w którym zastosowano bezpośrednio przepisy chińskiej Konstytucji w sprawie cywilnej z powodu luki prawnej w przepisach ustawy, mógłby zostać przywołany, jako przykład, że również chińska ustawa zasadnicza może być bezpośrednim źródłem prawa[79]. Szczególnie, że sprawa dotyczyła kradzieży tożsamości, a zatem z prawem do prywatności i ochroną danych osobowych, była w pewien sposób powiązana[80]. Tak jednak nie jest, ponieważ 18 grudnia 2008 r. NSL cofnął swoją decyzję wydaną w tej sprawie, kończąc w ten sposób istniejącą przez kilka lat możliwość, by stosować bezpośrednio przepisy chińskiej ustawy zasadniczej i ponownie sprawiając, że pozycja konstytucji w Chinach dla praktyki prawa jest czysto symboliczna[81].

Nie można również powołać się w tej kwestii na porozumienia międzynarodowe. Chińska Republika Ludowa jest sygnatariuszem Międzynarodowego Paktu Praw Obywatelskich i Politycznych z 16 grudnia 1966 roku (podpisała go w roku 1998), którego art. 17 chroni szeroko pojętą prywatność, a także zakazuje bezprawną ingerencję w nią, jednak nigdy tego paktu nie ratyfikowała[82]. Nie można zatem, powołać się również w tej kwestii na porozumienia międzynarodowe.

Oznacza to, że kwestia prawa do prywatności i ochrony danych osobowych jest regulowana dopiero na poziomie ustawy. Źródłem może być część ogólna kodeksu cywilnego ChRL, której artykuły 111 i 127 stanowią faktyczne podstawy systemu ochrony danych osobowych w ChRL. Art. 111 CzOKC brzmi:

> „Dane osobowe osób fizycznych są chronione przez przepisy prawa. Organizacja lub osoba fizyczna, która zbiera dane osobowe innych osób, musi zapewnić im odpowiednią i zgodną z przepisami prawa ochronę, zakazane jest bezprawne zbieranie, używanie, przetwarzanie

78 G. Greenleaf, *op. cit.*, s. 196.

79 Pisałem o tym w monografii: G. Lebedowicz, Igor Szpotakowski, B. Wiśniewski, *Zarys chińskiego prawa cywilnego w dobie kodyfikacji,* s. 121.

80 G. Greenleaf, *op. cit.,* s. 196.

81 G. Lebedowicz, I. Szpotakowski, B. Wiśniewski, *op. cit.,* s. 122.

82 G. Greenleaf, *op. cit.,* s. 197

lub przekazywanie ich innym podmiotom. Nielegalny jest handel danymi, a także ich rozpowszechnianie”[83].

Ponadto art 127 CzOKC stanowi, że tam, gdzie prawo przewiduje ochronę danych, ochrona ta ma odbywać się zgodnie z treścią tych przepisów[84]. Prawdą jest, że na pierwszy rzut oka nie można z tych przepisów uzyskać zbyt wielu informacji, ponieważ odsyłają one do regulacji pozakodeksowych, jednakże należy podkreślić, że jest on dla systemu prawnego niezwykle istotny[85]. Poruszam ten wątek głównie dlatego, że w pierwszym, już wspominanym przeze mnie projekcie CzOKC artykuł dotyczący własności intelektualnej wymieniał w swoim katalogu również dane, jednak już w finalnej wersji ustawy zostały one przeniesione do art. 127 CzOKC[86]. Zhang Mingqi uważa decyzję, by umieścić dane w osobnym artykule i objąć je dodatkową ochroną (chodzi tu o wszelkie dane, dane osobowe zostały uregulowane w art. 111) przepisów prawa cywilnego za wartościową, ponieważ ze względu na złożoność i różnorodność problematyki ochrony danych, ułatwi to legislacyjny postęp w tej dziedzinie[87].

W projekcie Kodeksu Cywilnego Chińskiej Republiki Ludowej z sierpnia 2019 roku znajduje się ponadto w księdze poświęconej ochronie dóbr osobistych rozdział VI, o tytule: „Prawa do prywatności i ochrona danych osobowych”[88]. Rozdział ten zawiera osiem artykułów, od 811 do 817[1], dość szczegółowo regulujących problematykę ochrony danych osobowych i prawa do prywatności. Próba umieszczenia księgi zawierającej tak fundamentalne prawa i obowiązki obywatela w kodyfikacji prawa prywatnego jest przejawem postępującego w Chińskiej Republice Ludowej procesu „konstytucjonalizacji” kodeksu cywilnego, przy jednoczesnej „dekonstytucjonalizacji” chińskiej ustawy zasadniczej[89].

---

83 第一百一十一条　自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息.

84 第一百二十七条　法律对数据、网络虚拟财产的保护有规定的，依照其规定.

85 G. Lebedowicz, I. Szpotakowski, B. Wiśniewski, *op. cit.,* s. 139.

86 *Ibidem,* s. 139-140.

87 Mingqi Zhang, 《中华人民共和国民法总则》的制定 (Formulation of the General Principles of Civil Law of the People's Republic of China), „China Legal Science” 2017, vol. 2, s. 22–23.

88 第六章 隐私权和个人信息保护.

89 Szerzej poruszam ten wątek w monografii: G. Lebedowicz, I. Szpotakowski, B. Wiśniewski, *op. cit.,* s. 134-135.

Art. 811 projektu zawiera definicję prywatności jako terminu, który używany odnosi się do przestrzeni prywatnej, prywatnej sfery zachowań, informacji prywatnych i tak dalej[90]. Z kolei art. 813 zawiera definicję terminu dane osobowe, który odnosi się do wszelkiego rodzaju informacji zapisanych elektronicznie lub w inny sposób, które mogą prowadzić do zidentyfikowania określonej osoby fizycznej bezpośrednio lub pośrednio w połączeniu z innymi informacjami, do których zaliczają się imiona i nazwisko, data urodzenia, numery identyfikacyjne, dane biometryczne, adresy, numery telefonów i tak dalej[91].

Dane osobowe chronione też są za pomocą przepisów prawa administracyjnego, z których najważniejsza w kontekście ochrony danych osobowych wydaje się ustawa o cyberbezpieczeństwie z 7 listopada 2016 r.[92]. Zgodnie z definicją z art. 76 punktu 5 ustawy, dane osobowe odnoszą się do wszelkiego rodzaju informacji, zapisanych w formie elektronicznej lub za pomocą innych środków, które bezpośrednio lub pośrednio łącznie z innymi informacjami są wystarczające do zidentyfikowania tożsamości osoby fizycznej, w tym, między innymi, imion i nazwisk obywateli, dat urodzenia, numerów identyfikacyjnych, danych biometrycznych, adresów zamieszkania, numerów telefonów i tak dalej[93]. Jest to zatem dokładnie taka sama definicja, jak ta z projektu księgi poświęconej ochronie dóbr osobistych kodeksu cywilnego ChRL, który opisałem powyżej.

Ponadto, art. 24 ustawy o handlu w Internecie (e-commerce)[94], która weszła w życie 1 stycznia 2019 r., stanowi, że: „W przypadku, gdy operatorzy stron internetowych dotyczących prowadzenia handlu internetowego otrzymują zapytania, żądania modyfikacji lub usunięcia danych użytkownika, niezwłocznie odpowiadają na zapytanie, modyfikują lub usuwają te dane po weryfikacji tożsamości użytkownika”[95].

System prawa ochrony danych osobowych domknie wydana 7 marca 2020 norma bezpieczeństwa GB/T 35273-2020 „Norma bezpieczeństwa

90 隐私是自然人不愿为他人知晓的私密空间、私密活动和私密信息等。

91 个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息,包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱地址、行踪信息等.

92 中华人民共和国网络安全法.

93 个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等.

94 中华人民共和国电子商务法.

95 第二十四条　电子商务经营者应当明示用户信息查询、更正、删除以及用户注销的方式、程序，不得对用户信息查询、更正、删除以及用户注销设置不合理条件.

technologii danych osobowych - Norma bezpieczeństwa danych osobowych"[96], która zostanie wdrożona 1 października 2020 r.[97] i zastąpi dotychczasową normę GB/T 35273-2017[98]. Stanowi ona praktyczne dopełnienie wspomnianej powyżej ustawy o cyberbezpieczeństwie i chociaż w teorii jest ona dobrowolna, jako soft-law, to jednak chińskie organy regulacyjne oczekują, że przedsiębiorstwa każdej wielkości będą jej skrupulatnie przestrzegać[99].

4. 2. Zasady przetwarzania danych osobowych

Na moment pisania pracy zasady przetwarzania danych osobowych w Chińskiej Republice Ludowej są wskazane w wytycznych Ministerstwa Przemysłu i Informatyzacji (MPiI) z 2013 r.[100] Wytyczne MPiI z 2013 r. określają w art. 4.2 osiem podstawowych zasad, których powinien przestrzegać administrator danych osobowych. Są to:

1) Zasada przejrzystości celu przetwarzania, zgodnie z którą, dane osobowe należy przetwarzać w określony, przejrzysty i rozsądny sposób, nie należy rozszerzać zakresu celu przetwarzania i nie należy zmieniać go bez otrzymania zgody od uprawnionego.

2) Zasada ograniczenia celu przetwarzania, zgodnie z którą należy minimalizować gromadzenie danych ograniczając się do tego, co niezbędne do celów, w których są przetwarzane, a po ich osiągnięciu dane osobowe należy usunąć w możliwie najkrótszym czasie.

3) Zasada odpowiedniego informowania, zgodnie z którą należy w jasny, zrozumiały i odpowiedni sposób, zgodnie z prawdą, poinformować podmiot danych osobowych o celu przetwarzania tych danych, zakresu ich gromadzenia i wykorzystywania, a także zastosowanych środków ochrony.

4) Zasada pozyskania zgody, zgodnie z którą przed rozpoczęciem przetwarzania danych osobowych należy uzyskać zgodę od podmiotu, do którego

---

96 GB/T 35273-2020 信息安全技术 个人信息安全规范, dostępna na stronie: https://www.tc260.org.cn/upload/2019-02-01/1549013548750042566.pdf [dostęp: 29.03.2020 r.].

97 国家标准《个人信息安全规范》2020版正式发布（附下载）[*Krajowa norma* bezpieczeństwa danych osobowych 2020 *oficjalnie wydana]*, https://www.secrss.com/articles/17713 [dostęp: 29.03.2020 r.].

98 GB/T 35273-2017 信息安全技术 个人信息安全规范.

99 L. Ross, K. Zhou, Tingting Liu, *China Issues New Personal Information Security Specification, March 24, 2020,* https://www.wilmerhale.com/en/insights/client-alerts/20200324-china-issues-new-personal-information-security-specification [dostęp: 29.03. 2020 r.].

100 G. Greenleaf, *op. cit.,* s. 209

dane osobowe należą (nie określono jednak w przeciwieństwie do RODO, czy zgoda ma być wyraźna, czy wystarczy milcząca).

5) Zasada zapewnienia jakości, zgodnie z którą należy zagwarantować, że poufność, integralność i dostępność danych osobowych, będzie stale zapewniana.

6) Zasada zagwarantowania bezpieczeństwa, zgodnie z którą administrator powinien zapewnić odpowiednie co do ilości i istotności zebranych danych osobowych środki bezpieczeństwa.

7) Zasada działania w dobrej wierze, w dużej mierze powtarza ona pierwszą i drugą zasadę, dodając jedynie konieczność zgodności z wymogami stawianymi przez przepisy prawa, więc zasadę legalności.

8) Zasada wyraźnej odpowiedzialności - wymaga jasnego zdefiniowania i wskazania administratora gromadzącego i przetwarzającego dane osobowe w celu ułatwienia późniejszego ewentualnego dochodzenia roszczeń z tytułu naruszeń[101].

Jest to jasne i dość mocne określenie podstawowych zasad ochrony danych osobowych, niestety jedynie w formie zaleceń. Nie obejmuje to jednak wszystkich obowiązków zawartych w innych wytycznych, w tym sytuacji, gdy potrzebna jest wyraźna zgoda, specjalne zabezpieczenia danych wrażliwych, dodatkowe ograniczenia transferu danych osobowych za granicę, obowiązki w zakresie zapobiegania naruszeniom danych osobowych oraz jakie są prawa osób, których dane dotyczą[102].

Po uchwaleniu kodeksu cywilnego ChRL, co pomimo pandemii koronawirusa, powinno mieć miejsce w 2020 r. zasady przetwarzania danych osobowych będą uregulowane w art. 814, zgodnie z którym gromadzenie i przetwarzanie danych osobowych osób fizycznych ma odbywać się zgodnie z zasadami legalności, uzasadnienia celu i niezbędności oraz spełniać następujące warunki:

> „(1) odbywać się za zgodą osoby fizycznej lub jej opiekuna prawnego, chyba że przepisy ustawowe i administracyjne stanowią inaczej;
> (2) odbywać się zgodnie z zasadami gromadzenia i przetwarzania danych osobowych;
> (3) administrator powinien wskazać wyraźny cel, metodę i zakres zbierania i przetwarzania danych osobowych;
> (4) zbieranie i przetwarzanie danych nie powinno naruszać przepisów ustawowych i administracyjnych oraz ustaleń stron. Przetwarzanie

101 *Ibidem,* s. 209-210.
102 *Ibidem,* s. 210.

danych osobowych obejmuje wykorzystanie, przetwarzanie, przesyłanie, przekazywanie i ujawnianie danych osobowych"[103].

W nowym kodeksie cywilnym, zasady przetwarzania danych osobowych zostały ujęte również w formie zakazów, w art. 812, który stanowi, że „o ile ustawa lub zgoda posiadacza praw nie stanowią inaczej, żadna organizacja lub osoba fizyczna nie może:

(1) wyszukiwać, wchodzić na teren, obserwować ani fotografować prywatnych przestrzeni, takich jak domy i pokoje hotelowe innych osób;

(2) filmować, nagrywać, publikować, podglądać lub podsłuchiwać życia prywatnego innych osób;

(3) fotografować lub podglądać intymnych części ciał innych osób;

(4) zbierać i przetwarzać danych osobowych osób trzecich;

(5) zakłócać spokoju życia innych osób za pomocą wiadomości tekstowych, połączeń telefonicznych, komunikatorów, wiadomości e-mail, ulotek itp.;

(6) naruszać prawa do prywatności innych osób w inny sposób"[104].

Poza tymi dwoma aktami, system ochrony danych osobowych jest w Chinach niezwykle rozdrobniony, co pokazuje, że system ten jest jeszcze niekompletny. Warto jednak podkreślić, że wraz z wejściem w życie nowego kodeksu cywilnego w Państwie Środka prawo do prywatności, a także ochrona danych osobowych nabierze większego znaczenia. Co ciekawe chiński prawodawca chce wprowadzić przepisy dotyczące ochrony danych osobowych za pomocą prawa cywilnego, czyli sfery prywatnej, a nie jak prawodawca unijny za pomocą przepisów administracyjnych, będących sferą prawa publicznego. Szersze rozważania na temat ochrony danych osobowych za pomocą prawa cywilnego umieściłem w rozdziale następnym, porównując podejście europejskie z podejściem chińskim.

103 (一)征得该自然人或者其监护人同意,但是法律、行政法规另有规定的除外; (二)公开收集、处理信息的规则; (三)明示收集、处理信息的目的、方式和范围; (四)不违反法律、行政法规的规定和双方的约定。个人信息的处理包括个人信息的使用、加工、传输、提供、公开等.

104 第八百一十二条 除法律另有规定或者权利人同意外,任何组织或者个人不得实施下列行为: (一)搜查、进入、窥视、拍摄他人的住宅、宾馆房间等私密空间; (二)拍摄、录制、公开、窥视、窃听他人的私密活动; (三)拍摄、窥视他人身体的私密部位; (四)收集、处理他人的私密信息; (五)以短信、电话、即时通讯工具、电子邮件、传单等方式侵扰他人的生活安宁; (六)以其他方式侵害他人的隐私权.

4. 3. Przekazywanie danych osobowych poza terytorium ChRL

Podstawowe regulacje, na moment pisania pracy, dotyczące przekazywania danych osobowych poza terytorium ChRL znajdują się we wspomnianej w poprzednim podrozdziale ustawie o cyberbezpieczeństwie z 2016 r. Zgodnie z art. 37 tej ustawy, dane osobowe i inne ważne dane dotyczące działalności gospodarczej, które są gromadzone lub przetwarzane przez operatorów krytycznej infrastruktury informatycznej na terytorium Chin powinny być również przechowywane na terenie ChRL[105]. Jeżeli ze względu na specyfikę działalności gospodarczej niezbędne jest przekazanie ich poza terytorium Chińskiej Republiki Ludowej, należy się wtedy stosować do zaleceń sformułowanych wspólnie przez organy państwowe, chyba, że przepisy szczególne stanowią inaczej[106]. W przypadku gdy operatorzy krytycznej infrastruktury informatycznej naruszą art. 37 ustawy, przechowując dane w niej wymienione poza terytorium ChRL lub przekazując te dane osobom fizycznym lub organizacjom znajdującym się poza Chinami bez przeprowadzenia oceny bezpieczeństwa, zgodnie z art. 66 ustawy właściwy organ może nakazać wykonanie takiej oceny, wydać ostrzeżenie, objąć przepadkiem na rzecz państwa bezprawne zyski, nałożyć kary pieniężne w wysokości od 50,000 do 500,000 juanów, a także może zarządzić: tymczasowe zawieszenie działalności przedsiębiorstwa, zamknięcie stron internetowych, cofnięcie odpowiednich zezwoleń na działalność lub unieważnienie licencji na działalność[107]. Natomiast osoby, które są bezpośrednio odpowiedzialne, mogą zostać ukarane grzywnami w wysokości od 10,000 do 100,000 juanów[108].

Powyższe regulacje dotyczą jednak operatorów krytycznej infrastruktury informatycznej, która co ciekawe wciąż nie została szczegółowo zdefiniowana, pomimo kilku lat obowiązywania już ustawy o cyberbezpieczeństwie. Taki stan pozostawia w niepewności wiele przedsiębiorstw, zarówno zagranicznych, jak i krajowych, co do tego czy powyższe reguły będą stosowane w ich

105 第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储.

106 因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定.

107 第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照.

108 对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款.

przypadku[109]. Poza sektorem krytycznej infrastruktury informatycznej chińskie przepisy nie nakładają żadnych ograniczeń dotyczących transferu danych osobowych do państw trzecich[110]. Dlatego, tak jak wspomniałem już w rozdziale 2, chińskie spółki chcąc przetwarzać dane osobowe obywateli Unii Europejskiej muszą zapewnić odpowiednie zabezpieczania wynikające z RODO.

Na zakończenie rozdziału warto też wspomnieć, że 13 czerwca 2019 r. poddano pod publiczną dyskusję projekt normy oceny bezpieczeństwa transferu danych osobowych poza terytorium ChRL[111].

5. Perspektywa prawno-porównawcza i problemy z niej wynikające

Porównując współczesne spojrzenia na ochronę danych osobowych, zarówno w Polsce oraz Unii Europejskiej ze spojrzeniem chińskim, można zauważyć odmienne podejścia co do rozwiązywania pozornie tożsamych zagadnień. Rodzi to wiele problemów i dyskusji pośród naukowców i prawników, a także może w pewnym stopniu wpływać na handel międzynarodowy. Mając to na uwadze, najważniejsze z tych różnic omówię w tym rozdziale.

5. 1. Prawo prywatne czy publiczne?

W ostatnich latach tym co najbardziej różni unijny system ochrony danych osobowych od chińskiego, jest z pewnością kwestia: Czy ochrona danych osobowych powinna być na podstawie przepisów administracyjnych czy cywilnych? Jak wskazuje Yuxiao Duan, to gdzie znajduje się w systemie prawa definicja danych osobowych determinuje zasadniczo też środki ich ochrony[112].

W Polsce, prawo ochrony danych osobowych nie jest odrębnym działem prawa, lecz mieści się głównie w obszarze prawa publicznego – administracyjnego, w niewielkim tylko stopniu dotykając prawa konstytucyjnego, cywilnego czy karnego. Ponadto Paweł Fajgielski wskazuje, że:

---

109 G. Webster, S. Sacks, P. Triolo, *Three Chinese Digital Economy Policies at Stake in the U.S.–China Talks*, April 2, 2019 https://www.newamerica.org/cybersecurity-initiative/digichina/blog/three-chinese-digital-economy-policies-at-stake-in-the-uschina-talks/ [dostęp: 29.03.2020].

110 G. Greenleaf, *op. cit.,* s. 501.

111 国家互联网信息办公室关于《个人信息出境安全评估办法（征求意见稿）》公开征求意见的通知 http://www.cac.gov.cn/2019-06/13/c_1124613618.htm [dostęp: 29.03.2020 r.].

112 Yuxiao Duan, *China's Private Law Approach to Personal Data Protection* (May 26, 2019), s. 15, https://ssrn.com/abstract=3484725 [dostęp: 31.03.2020].

> „administracyjnoprawny charakter regulacji ochrony danych osobowych przejawia się przede wszystkim w tym, że prawodawca nakłada na podmioty, które przetwarzają dane, wiele obowiązków, ich spełnienie zabezpieczone jest sankcją administracyjną, a nadzór nad przestrzeganiem przepisów powierzony został organowi nadzorczemu prowadzącemu postępowania w oparciu o przepisy procedury administracyjnej i wyposażonemu we władztwo administracyjne (organ wydaje w tym zakresie decyzje administracyjne, może również nakładać administracyjne kary pieniężne za naruszenie przepisów o ochronie danych)"[113].

W Chinach ochrona danych osobowych to głównie gałąź prawa cywilnego[114], z wyraźnym podkreśleniem dóbr osobistych, pomimo istnienia przepisów prawa administracyjnego regulujących tę problematykę. Definicja danych osobowych znajduję się w art. 111 CzOKC, o czym wspominałem już przy omawianiu źródeł prawa. Pytaniem, które może się nasuwać, jest: czy taka ochrona może być skuteczna?

W przypadku Chin argumentem za wykorzystania prawa cywilnego do ochrony danych osobowych, może być słabość prawa administracyjnego. Można założyć, że chińskie prawo cywilne jest doskonałym narzędziem uzupełniającym egzekwowania przepisów prawa administracyjnego, ponieważ ze względu na rozdrobnienie tego drugiego, zapewnia skuteczniejsze środki i sposoby ochrony praw[115]. Jednak, jak wskazuje Yuxiao Duan powodem, dla którego prawo prywatne nie działa poprawnie w Chinach, jest to, że nie radzi sobie ono z pogodzeniem z sobą dwóch zasadniczych wartości: z jednej strony potrzeby ochrony danych osobowych, a z drugiej konieczności zachowania swobodnego przepływu informacji[116]. Tym co charakteryzuje ochronę danych osobowych za pomocą prawa deliktów, jest bowiem nacisk kładziony właśnie na ochronę, zaniedbując przy tym swobodny przepływ informacji, co we współczesnym świecie wydaje się równie kluczowe[117].

---

113 P. Fajgielski, *op. cit.,* s. 37, szerzej w: G. Szpor, *Publicznoprawna ochrona danych osobowych*, Przegląd Ustawodawstwa Gospodarczego, 1999/12, s. 2–13.

114 Yanfang Wu, Tueyu Lau, D. Atkin, C. A. Lin, *A comparative study of online privacy regulations in the U.S. and China,* Telecommunications Policy, August 2011, s. 613.

115 Tiantian Zhai, Yen-Chiang Chang, *The Contribution of China's Civil Law to Sustainable Development: Progress and Prospects, Sustainability*, Vol. 11, Issue 1, January (I) 2019, s. 7, https://doi.org/10.3390/su11010294 [dostęp: 05.04.2020 r.].

116 Yuxiao Duan, *op. cit.*, s. 23.

117 *Ibidem*, s. 23,

5. 2. Prawo do bycia zapomnianym

W Unii Europejskiej prawo do bycia zapomnianym swoje korzenie ma w art. 12 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. *w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych*[118], wzmocnionej 13 maja 2014 r., wyrokiem Trybunału Sprawiedliwości Unii Europejskiej, który uznał istnienie indywidualnego prawa do bycia zapomnianym w sprawie Google Spain SL i Google Inc. przeciwko Agencia Espanola de Proteccion de Datos (AEPD) i Mario Coseja Gonzales (sprawa C-131/12)[119]. Następnie w 2016 roku unijny prawodawca uregulował prawo do usunięcia danych w art. 17 ust. 1 RODO[120]. Zgodnie z tym przepisem, administrator danych osobowych na żądanie osoby, której dane dotyczą, ma obowiązek bez zbędnej zwłoki usunąć jej dane osobowe. W literaturze wskazuje się, że nadużywanie przez osoby, których dane dotyczą, prawa do bycia zapomnianym, może zaszkodzić małym, średnim i dużym przedsiębiorstwom, które opierają swój model biznesowy na sprzedaży zebranych danych osobowych reklamodawcom i innym stronom trzecim poszukującym takich informacji[121]. Chociaż wielkie spółki, jak Facebook czy Google, które przetwarzają ogromne ilości danych, nie zostały założone na terenie Unii Europejskiej, RODO wpływa

[118] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:31995L0046&from=en [dostęp: 05.04.2020 r.].

[119] Wyrok dostępny na stronie Trybunału: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN, [dostęp: 05.04.2020 r.].

[120] Art. 17 ust. 1. RODO stanowi: Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności: a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane; b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 zgodność przetwarzania z prawem ust. 1 lit. a) lub art. 9 przetwarzanie szczególnych kategorii danych osobowych ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania; c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 prawo do sprzeciwu ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 prawo do sprzeciwu ust. 2 wobec przetwarzania; d) dane osobowe były przetwarzane niezgodnie z prawem; e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator; f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego ust. 1.

[121] Ch. Garrison, C. Hamilton, *A comparative analysis of the EU GDPR to the US's breach notification*s, Information & Communications Technology Law, nr 28:1, s. 103.

na zbieranie przez nich i wykorzystywanie danych osobowych mieszkańców Europy[122].

W Chinach prawo do bycia zapomnianym ma znacznie krótszą historię. W maju 2016 r. sąd rejonowy (sąd szczebla podstawowego) dzielnicy Haidian w Pekinie wydał w sprawie cywilnej wyrok na korzyść chińskiej wyszukiwarki internetowej Baidu, odmawiając powodowi prawa do bycia zapomnianym, uznając, że nie istnieje ono w prawie chińskim[123]. Wraz z wejściem w życie ustawy o cyberbezpieczeństwie pojawiło się ono w ograniczonym stopniu, w art. 43, w przypadkach, w których w których operator sieci naruszył prawo lub umowę między stronami[124]. Od 1 stycznia 2019 r. funkcjonuje też, art. 24 ustawy o handlu w Internecie, którego tekst przytaczałem w rozdziale 3, jednak ogranicza się on tylko do operatorów stron internetowych zajmujących się prowadzeniem handlu w Internecie. Oznacza to, że Chińskiej Republice Ludowej prawo do bycia zapomnianym działa w o wiele węższym zakresie, niż na terenie Unii Europejskiej.

5. 3. Zapewnienie odpowiedniego stopnia ochrony danych osobowych

Trzecią wątkiem, który chciałbym poruszyć w tym rozdziale, są dyskusje wokół zawartej w RODO zasady zapewnienia odpowiedniego stopnia ochrony danych osobowych. Jak już pisałem w rozdziale 2, zgodnie z art. 45 ust. 1 RODO, przekazanie danych osobowych do państwa trzeciego, może nastąpić, gdy Komisja Europejska stwierdzi, że to państwo trzecie zapewnia odpowiedni stopień ochrony[125]. Pomimo, że Komisja Europejska nie wydała decyzji uznającej, że Chiny odpowiedni stopień ochrony zapewniają, to jednak specjaliści od prawa chińskiego, Chao Jing i Tom Zwart, uważają, że system ochrony danych osobowych w ChRL w dużym stopniu spełnia unijne standardy[126]. Przyjmują oni w ten sposób odmienny punkt widzenia niż autorzy raportu dla unijnej Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) z 2015 r. - Paul de Hert i Vagelis

122 *Ibidem.*

123 E. Pernot-Lepla, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU*, Penn State Journal of Law & International Affairs, vol. 8.1, s. 44.

124 *Ibidem*.

125 Artykuł 45 ust. 1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

126 S. van Deursen, H. Kummeling, *The New Silk Road: a bumpy ride for Sino-European collaborative research under the GDPR?*, Higher Education (2019) nr 78, s. 923.

Papakonstantinou, którzy określili chiński system ochrony danych osobowych mianem nieadekwatnego[127].

Widzimy też niepokojący rozwój zwiększenia kontroli władzy wykonawczej nad całością społeczeństwa, zwłaszcza ze względu na fakt, że obecne zasady ochrony danych osobowych są niejasne lub wręcz nie istnieją w odniesieniu do przetwarzania danych osobowych w sektorze publicznym[128]. Przetwarzanie danych osobowych, stanowi ważny element rozwoju Systemu Zaufania Społecznego w Chinach[129], zwiększa się też kontrola w sektorze akademickim[130], co rodzi pytania o odpowiedni stopień zabezpieczeń danych osobowych, mając świadomość, że chińscy naukowcy po zakończeniu badań będą musieli przekazywać zebrane dane agencjom rządowym[131].

Jak wskazują Stijn van Deursen i Henk Kummeling, dopóki system ochrony danych osobowych w Chinach nie będzie spełniał standardów unijnych, z prawnego punktu widzenia, bezpieczniejszym sposobem wciąż wydawać się może anonimizacja danych osobowych, które są przekazywane do Państwa Środka lub uzyskanie wyraźnej zgody osób, których dane dotyczą, po poinformowaniu ich o ryzyku towarzyszącym takiemu transferowi[132].

6. Podsumowanie

W pracy przedstawiona została problematyka ochrony danych osobowych w Rzeczypospolitej Polskiej i w Chińskiej Republice Ludowej. Omówiono również najważniejsze wątki dotyczące ochrony tych danych, które mogą okazać się istotne w polsko-chińskich relacjach biznesowo-prawnych. Zaprezentowano odmienne spojrzenie na kwestię prywatności i potrzeby ochrony danych osobowych w kręgu kultury europejskiej oraz chińskiej. Przedstawiono też wybrane problemy, z którymi można się zetknąć analizując tak odmienne od siebie porządki prawne.

---

127 P. de Hert, V. Papankonstantinou, *The data protection regime in China – in depth analysis for the LIBE Committee* (2015), s. 13 -14, http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf. [dostęp: 05.04.2020. r.].

128 G. Greenleaf, *China's new cybersecurity law – also a data privacy law?*, Privacy Laws & Business International Report, nr 144, s. 3.

129 Więcej w: Yongxi Chen, A. S. Y. Cheung, *The transparent self under big data profiling: privacy and Chinese legislation on the social credit system*, Journal of Comparative Law, nr 12 (2), 2017, s. 356–378.

130 D. Normille, *China asserts firm grip on research data,* 9 kwietnia 2018 r., http://www.sciencemag.org/news/2018/04/china-asserts-firm-grip-research-data [dostęp: 05.04.2020 r.].

131 Y. Sharma, *New data red tape could hamper international research*, 20 lipca 2018, www.universityworldnews.com/post.php?story=20180720072113906 [dostęp: 05.04.2020 r.].

132 S. van Deursen, H. Kummeling, *op. cit.*, s. 927.

Celem pracy była analiza funkcjonowania problematyki ochrony danych osobowych w Rzeczypospolitej Polskiej i w Chińskiej Republice Ludowej. Praca wykazała, że w Chinach, choć poczyniono liczne legislacyjne kroki, by uregulować tę materię, system aktów prawnych dotyczący ochrony danych osobowych wciąż pozostaje w porównaniu do Polski i Unii Europejskiej niekompletny.

W pracy postawiono hipotezę w następującym brzmieniu: Ochrony danych osobowych pełni bardzo ważną rolę w relacjach biznesowo-prawnych między Polską a Chinami. Z hipotezy głównej wyznaczono następujące hipotezy szczegółowe:

- Potrzeba ochrony danych osobowych wynika z koncepcji ochrony prywatności.
- W Polsce problematyka ochrony danych osobowych jest silniej uregulowana niż w Chinach.
- Chińskie prawo ochrony danych osobowych pomimo różnić wynikających z innych realiów prawno-społecznych, powoli zaczyna przypominać unijne ogólne rozporządzenie o ochronie danych.

Wykorzystując metodę opisową, historyczną i komparatystyczną udowodniono w pracy, że potrzeba ochrony danych osobowych wynika z koncepcji ochrony prywatności, jaka wytworzyła się w danej kulturze, a także, że to, gdzie znajduje się w systemie prawa definicja danych osobowych determinuje zasadniczo środki ich ochrony. Ponadto wskazano, że w Polsce, a zatem także w Unii Europejskiej problematyka ochrony danych osobowych jest silniej uregulowana niż w Chińskiej Republice Ludowej. Dowodem na to jest zarówno opisane w rozdziale 4 prawo do bycia zapomnianym, jak także brak w chińskim systemie prawnym regulacji, która przypominałaby RODO. Co ważniejsze, udowodniono także, że pomimo braku w prawie chińskim zwartego aktu prawnego będącego odpowiednikiem unijnego ogólnego rozporządzenia o ochronie danych, to jednak część ogólna kodeksu cywilnego ChRL, ustawa o cyberbezpieczeństwie, a także ustawa o handlu w Internecie tworzą system, który w wielu aspektach przypomina regulacje polskie i unijne.

Finalnie, jak zostało wykazane w pracy, ochrona danych osobowych pełni bardzo ważną rolę w relacjach biznesowo-prawnych między Polską a Chinami, choć oba państwa podchodzą do niej odmiennie. Dlatego też tak ważne są dalsze badania i analizy komparatystyczne dotyczące tej tematyki. Szczególnie, że już 1 listopada 2021 r. w życie wejdzie nowa ustawa

o Ochronie Danych Osobowych ChRL[133], która została uchwalona 20 sierpnia 2021 r. przez Stały Komitet OZPL. To wielki krok w historii prawa chińskiego i dlatego też, zasługuje on na dokładne opisanie go w następnym tomie. Szczególnie, że na ten moment nie wiadomo jak bardzo nowa ustawa zmieni Chiny i Chińczyków.

7. Bibliografia

Monografie i komentarze:

1. Błażewski M., Behr J., *Środki prawne ochrony danych osobowych*, Wrocław 2018.

2. *Chinese Legal Reform and the Global Legal Order: Adaption and Adaptation*, Y. Zhao, M. Ng (red.), Cambridge 2018.

3. Dargas M., *Idee i zasady konstytucyjne chińskiego porządku prawnego*, Warszawa 2017.

4. *Developing Key Privacy Rights*, M. Colvin (red.), Portland 2002.

5. Dowding M. R., *Privacy: Defending an illusion*, Plymouth 2011.

6. Elliot M., Thomas R., *Public Law*, Oxford 2017.

7. Etzioni A., *The limits of privacy*, New York 1999.

8. Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999.

9. Greenleaf G., *Asian Data Privacy Laws: Trade & Human Rights Perspectives*, Oxford 2014.

10. Hofstede G., *Culture's Consequences: Comparing Values, Behaviours, Institutions, and Organizations Across Nations*, Londyn 2001.

11. Johnson W., *The T'ang Code, Volume II, Specific Articles*, Princeton, New Jersey 1997.

12. Lambert P., *Understanding the New European Data Protection Rules*, Taylor & Francis Group, Boca Raton 2018

13. Lebedowicz G., Szpotakowski I., Wiśniewski B., *Zarys chińskiego prawa cywilnego w dobie kodyfikacji*, Toruń 2019.

133 中华人民共和国个人信息保护法.

14. Masuda Yoneji, *The Information Society as Post-Industrial Society, World Future Society*, Washington D. C. 1980.

15. Marcinkowski B., *Dane osobowe: Polska – UE – USA. Współczesne wyzwania. Administracyjnoprawne zagadnienia odpowiedniości poziomu ochrony danych osobowych na przykładzie amerykańskiego prawa federalnego*, Warszawa 2018.

16. Murray A., *Information Technology Law: The Law and Society*, Oxford 2016.

17. Nissenbaum H., *Privacy in Context, Technology, Policy and the Integrity of Social Life*, Stanford 2010.

18. *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* M. Sakowska-Baryła (red.), Warszawa 2018.

19. *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, P. Litwiński (red.), Warszawa 2018.

20. Stępień A., Biały P., *Bezpieczeństwo danych osobowych zgodnie z RODO*, Warszawa 2017.

21. Taczkowska-Olszewska J., Chałubińska-Jentkiewicz K., Nowikowska M., *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019.

22. *Ustawa o ochronie danych osobowych. Komentarz*, M. Kawecki, M. Czerniewski (red.), Warszawa 2019.

23. *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, A. Grzelak(red.), Warszawa 2019.

24. Voigt F., von Bussche A., *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer, Cham 2017.

Artykuły, rozdziały i źródła internetowe:

25. Banyś T.A.J., *Funkcje prawa ochrony danych osobowych*, [w:] T.A.J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak, *Prawo ochrony danych osobowych*, Warszawa 2016.

26. Baran B., Południak-Gierz K., *Perspektywa regulacji prawa do bycia „zapomnianym" w Internecie. Zarys problematyki*. Zeszyty Naukowe Towarzystwa Doktorantów UJ. Nauki Społeczne, nr 2 (2017), s. 139-159.

27. Braxton Craven Jr. J., *Personhood: the right to be let alone*, Duke Law Journal 1976, s. 699-720.

28. Chen Yongxi, Cheung A. S. Y., *The Transparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System*, The Journal of Comparative Law (2017), vol. 12, no. 2, s. 356-378.

29. Cheung Kwok Wah, Pan Suyan, *Transition of Moral Education in China: Towards Regulated Individualism*, Citizenship Teaching and Learning 2 (2006), no. 2/2, s. 37-50

30. De Hert P, Papankonstantinou V, *The data protection regime in China – in depth analysis for the LIBE Committee* (2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf. [dostęp: 05.04.2020. r.].

31. Duan Yuxiao, *China's Private Law Approach to Personal Data Protection* (May 26, 2019), s. 1-23, https://ssrn.com/abstract=3484725 [dostęp: 31.03.2020].

32. Dunningan J. F., Nofi A. A., *Medieval Life and the Hundred Years War: Medieval Society and Culture*, 1997, http://www.hundredyearswar.com/Books/History/1_help_c.htm [dostęp: 26.01.2020 r.].

33. Farral K. N., *Global Privacy in Flux: Illuminating Privacy across Cultures in China and the U.S.*, International Journal of Communication 2 (2008), s. 993-1030.

34. Garrison Ch., Hamilton C., *A comparative analysis of the EU GDPR to the US's breach notifications*, Information & Communications Technology Law, nr 28:1, s. 99-114.

35. 个人信息出境安全评估办法 https://gfw-blog.netlify.com/2019/07/14/concern-personal-information-evaluation-method [dostęp: 29.03.2020 r.].

36. Greenleaf G., *China's new cybersecurity law – also a data privacy law?*, Privacy Laws & Business International Report, nr 144, s. 1–7.

37. Greenleaf G., Livingston S., *China's Personal Information Standard: The Long March to a Privacy Law*, Privacy Laws & Business International Report, nr 150(2017), s. 25-28.

38. 国家标准《个人信息安全规范》2020版正式发布 (附下载) [*Krajowa norma* bezpieczeństwa danych osobowych 2020 *oficjalnie wydana]*, https://www.secrss.com/articles/17713 [dostęp: 29.03.2020 r.].

39. Krzysteczko H., *Od publicznej praktyki pokutnej do spowiedzi prywatnej*, Śląskie Studia Historyczno-Teologiczne 29(1996), s. 323-334.

40. Ma Yuanye, *Unnmapped Privacy Expectations in China: Discussions Based on the Proposed Social Credit System* [w:] *Information in Contemporary Society: 14th International Conference, iConference 2019, Washington, DC, USA, March 31-April 3, 2019, Proceedings*, N. G. Taylor, C. Christian-Lamb, M. H. Martin, B. Nardi(eds.), Cham 2019, s. 799-805.

41. Machowicz K., *Prawo do prywatności w kontekście ochrony danych osobowych*, Studia Bobolanum 29, nr 3(2018), s. 167-176.

42. Młynarska-Sobaczewska A.*, Trzy wymiary prywatności. Sfera prywatna i publiczna we współczesnym prawie i teorii społecznej*, Przegląd Prawa Konstytucyjnego 2013, nr 1(13), s. 33-52.

43. Motyka K., *O amerykańskiej koncepcji prawa do prywatności i jej wpływie na prawo międzynarodowe (Wokół monografii Agnieszki Czubik*), Studia Prawnicze KUL 1 (69) 2017, s. 205-220.

44. Motyka K., *Prawo do prywatności*, Zeszyty Naukowe Akademii Podlaskiej w Siedlcach, Seria: Administracja i Zarządzanie, Nr 85, 2010, s. 9 – 36.

45. Machowicz K., *Prawo do prywatności w kontekście ochrony danych osobowych*, Studia Bobolanum 29, nr 3(2018), s. 167-176.

46. Normille D., *China asserts firm grip on research data*, 9 kwietnia 2018 r.. http://www.sciencemag.org/news/2018/04/china-asserts-firm-grip-research-data [dostęp: 05.04.2020 r.].

47. Pernot-Lepla E., *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU*, Penn State Journal of Law & International Affairs, vol. 8.1, s. 1-60.

48. Pryciak M., *Prawo do prywatności*, Wrocławskie Studia Erazmiańskie, zeszyt IV: Prawa człowieka - idea, instytucje, krytyka, 2010, s. 211-229.

49. Redding S. G., *Cognition as an Aspect of Culture and Its Relation to Management Process: An Exploratory View of the Chinese Case*, Journal of Management Studies 17 (1980), no. 2, s. 127-250.

50. Ross L., Zhou K., Liu Tingting, *China Issues New Personal Information Security Specification, March 24, 2020,* https://www.wilmerhale.com/en/insights/client-alerts/20200324-china-issues-new-personal-information-security-specification [dostęp: 29.03.2020 r.].

51. Sarek K., *Zanikający chiński kolektywizm — przyczyny zmian w mentalności i zachowaniu młodych Chińczyków*, Roczniki Humanistyczne, Tom LXVI, zeszyt 9, 2018, s. 109-120.

52. Sharma Y., *New data red tape could hamper international research*, 20 lipca 2018, www.universityworldnews.com/post.php?story=20180720072113906 [dostęp: 05.04.2020 r.].

53. Szpor G., Publicznoprawna ochrona danych osobowych, Przegląd Ustawodawstwa Gospodarczego, 1999/12, s. 2–13.

54. Szpor G., *Strategia ochrony danych osobowych w polityce społecznej*, Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach, 2012, Nr 87, s. 137-155.

55. Warren S.D., Brandeis L., *The Right to Privacy*, Harvard Law Review, vol. IV, December 1890, s. 193-220.

56. Webster G., Sacks S., Triolo P., *Three Chinese Digital Economy Policies at Stake in the U.S.–China Talks*, April 2, 2019 https://www.newamerica.org/cybersecurity-initiative/digichina/blog/three-chinese-digital-economy-policies-at-stake-in-the-uschina-talks/ [dostęp: 29.03.2020].

57. Wu Yanfang, Lau Tueyu, Atkin D.J., Lin C. A., *A comparative study of online privacy regulations in the U.S. and China*, Telecommunications Policy, nr 35 (2011), s. 603-616.

58. Van Deursen S., Kummeling H., *The New Silk Road: a bumpy ride for Sino-European collaborative research under the GDPR?*, Higher Education (2019) nr 78, s. 911–930.

59. Vickery A., *An Englishman's Home is His Castle?*, Past & Present, vol. 199, Issue 1, May 2008, s. 147–173.

60. Zhai Tiantian, Chang Yen-Chiang, *The Contribution of China's Civil Law to Sustainable Development: Progress and Prospects*, Sustainability, vol. 11, issue 1, January (I) 2019, s. 1-19, https://doi.org/10.3390/su11010294 [dostęp: 05.04.2020 r.].

61. Zhang Mingqi, 《中华人民共和国民法总则》的制定 (Formulation of the General Principles of Civil Law of the People's Republic of China), China Legal Science, 2017, vol. 2, s. 5-24.

Akty prawne:

62. *Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych* https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:31995L0046&from=en [dostęp: 05.04.2020 r.].

63. *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW* (Dz. Urz. UE L 119 z 4.05.2016 r., s. 89 ze zm.).

64. *GB/T 35273-2020* 信息安全技术 个人信息安全规范，dostępna na stronie: https://www.tc260.org.cn/upload/2019-02-01/1549013548750042566.pdf [dostęp: 29.03.2020 r.].

65. *Konstytucja Chińskiej Republiki Ludowej* z dnia 4 grudnia 1982 r.

66. *Konstytucja Rzeczypospolitej Polskiej* z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.).

67. *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (Dz. U. poz. 1000)

68. *Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości* (Dz.U. 2019 poz. 125).

69. *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (Dz. U. z 2016 r., poz. 922 ze zm.).

70. *Powszechna Deklaracja Praw Człowieka* z 10 grudnia 1948 r.

71. *Międzynarodowy Pakt Praw Obywatelskich i Politycznych* otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. 1977 nr 38 poz. 167).

72. *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności* sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2. (Dz.U. 1993 nr 61 poz. 284).

Kontraktowa i deliktowa odpowiedzialność odszkodowawcza za działanie Sztucznej Inteligencji z uwzględnieniem problematyki czynów nieuczciwej konkurencji w świetle prawa polskiego[1]

1. Wstęp do problemu

Niniejsza praca ma na celu odpowiedzieć na pytanie o odpowiedzialność za działanie bądź zaniechanie sztucznej inteligencji[2] biorąc pod uwagę obowiązujące obecnie przepisy prawa cywilnego. Końcowe spojrzenie na zagadnienie będzie poszerzone jednak o analizę przepisów ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji[3], gdyż obecnie bardzo wiele naruszeń związanych jest ze wzajemną rywalizacją podmiotów o określonych klientów na rynku. Praca ta stanowić będzie rozwinięcie problemu poruszonego przeze mnie w pracy licencjackiej, a dotyczącego odpowiedzialności za działania[4] SI w świetle przepisów ustawy z dnia 16 lutego 2007 roku o ochronie konkurencji i konsumentów[5]. Tamto ujęcie problemu odpowiada jedynie na pytania dotyczące odpowiedzialności administracyjnoprawnej, w szczególności kar pieniężnych nakładanych przez Prezesa Urzędu Ochrony Konkurencji i Konsumentów. Jest to jedynie wierzchołek góry lodowej, gdyż problem ten sięga znacznie głębiej. Żaden z poszkodowanych działaniami sankcjonowanymi przez wymienioną ustawę nie ma realnej korzyści czy odszkodowania wynikającego z nałożonej kary pieniężnej, w związku z czym w żaden sposób nie może zrekompensować straty klientów i pieniędzy, która to strata była

---

1 Michał Kalinowski, Uniwersytet Jagielloński w Krakowie.

2 Dalej „SI"

3 Dz.U. 1993 nr 47 poz. 211, dalej „UZNK"

4 W braku wyraźnego rozróżnienia w dalszej części pracy pod pojęciem „działania" mieści się także „zaniechanie"

5 Dz.U. 2007 nr 50 poz. 331

spowodowana działaniami zakazanymi. Co więcej, ustawa o ochronie konkurencji i konsumentów chroni jedynie przed naruszeniami równowagi rynku, w tym chroni równości dostępu do rynku jako całości. Nie reaguje zatem w przypadkach nieuczciwej konkurencji między indywidualnymi podmiotami. Taki cel ma właśnie wskazana ustawa o zwalczaniu nieuczciwej konkurencji. W zakresie odpowiedzialności za szkodę ustawa ta odsyła do przepisów kodeksu cywilnego. Słusznie wskazuje się w doktrynie, że „Artykuły 361–363 oraz art. 415 i n. KC stosują się do roszczenia o naprawienie wyrządzonej szkody wprost, ponieważ ZNKU nie zawiera odmiennej regulacji."[6] W szczególności będę chciał zwrócić uwagę na problem ograniczania dostępu do rynku, niemniej jednak sygnalizować będę inne potencjalne zagrożenia.

Sztuczna Inteligencja to technologia coraz bardziej rozwijana, a coraz więcej podmiotów stara się wdrażać rozwiązania technologiczne oparte o rozpoznawanie obrazów czy uczenie maszynowe. Potrzeba bardzo szybkiej analizy dużych ilości informacji wynika z tego jak dużo danych produkowanych jest każdego dnia na świecie. Możliwość ich wymiany w Internecie, cyfryzacja, powszechny dostęp do komputera, sieci Internet i telewizji sprawiła, że obecnie każdego dnia zalewa nas fala informacji, których człowiek nie jest w stanie w żaden sposób zidentyfikować, nie mówiąc już o analizie i sprawdzeniu ich autentyczności. Problem ten napędza badania nad coraz bardziej nowoczesnymi rozwiązaniami jak chociażby komputery kwantowe, które prawdopodobnie staną się motorem napędowym SI i pozwolą osiągnąć poziom analizy danych trudny do wyobrażenia dla ludzkiego mózgu. Stosowanie SI jest szczególnie widoczne w handlu, zwłaszcza internetowym. Wiele systemów sprzedażowych opiera się na profilowaniu klientów, na analizie popularności, jakości produktu. Rzecz jasna jest to bardzo duże ułatwienie dla konsumentów i przedsiębiorców. Bardzo często proponowane nam produkty okazują się trafione, zakupy są krótsze, często też mamy okazję trafić na jakiś nieznany nam model, który okazuje się jeszcze lepszy niż ten, o którym marzyliśmy. Stosowanie SI niesie za sobą jednak wiele zagrożeń, wynikających głównie z tego, że bardzo ciężko jest, przy stosowaniu zaawansowanych algorytmów, utrzymać działanie SI pod kontrolą. Może to prowadzić do naruszania przepisów prawa, powstawania szkód, zarówno po stronie osób trzecich, jak również samego użytkownika czy też dysponenta SI. Oczywiście zagrożenia SI wychodzą znacznie poza rynek konkurencji, jednak w mojej opinii jest to

[6] red. J. Szwaja, „*Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz.*", Warszawa 2019, wyd. 5, komentarz do art. 18, nb 98, Legalis

bardzo duże pole do popisu dla tego typu oprogramowania, także w negatywnym znaczeniu tego słowa.

Nasze prawo wywodzi się z kultury europejskiej, kontynentalnego systemu prawnego, co w dużym uproszczeniu sprowadza się do tego, że prawo zapisane jest w aktach prawnych, a sądy powołane są jedynie do jego stosowania. W Stanach Zjednoczonych Ameryki natomiast, także w Wielkiej Brytanii czy Australii, obowiązuje system common law. System ten opiera się, oprócz prawa wpisanego w aktach prawnych, na wyrokach sądowych. Sądy mają kompetencję stanowienia prawa na równi z ustawodawcą. Wyroki sądowe są często przełomowe w wielu sprawach znajdujących się w centrum uwagi społeczeństwa. System taki ma jeden zasadniczy plus – pozwala stosunkowo szybko reagować na zmiany w społeczeństwie, w szczególności zaś zmiany w obszarze wykorzystywanych technologii.

Powyższe odwołanie do systemu common law ma zwrócić uwagę na to, że nasz system nie nadaje się do tego, aby w sposób zadowalający regulować stosowanie nowych technologii. Jakiekolwiek zmiany wprowadzane przez ustawodawcę zawsze będą kilka kroków za tym, co udało się wdrożyć do obrotu. Ta niemoc prawna jest bardzo dużym zagrożeniem dla całego rynku, a prawników zmusza do szukania podstaw regulowania nowych zjawisk w starych przepisach. Jest to rozwiązanie niewłaściwe, ale jedyne. Taki właśnie cel ma ta praca. Jej wymiar ma być przede wszystkim praktyczny, pobudzić skąpą dyskusję na temat tego, że prawo nie nadąża za technologią, równocześnie przedstawić rozwiązanie, pewnie nie jedyne, w sytuacji, w której trzeba będzie podjąć problem SI w konkretnym przypadku. Dojście do konkluzji, że obecne przepisy nie mogą być stosowane w odniesieniu do SI, a zatem pozostawiamy cały ten problem poza regulacją, jest nietrafiony. Należy raczej próbować naciągać przepisy do tego, jak wygląda rzeczywistość. Próba kreatywnego podejścia do analizowanych reguł może doprowadzić do wniosku, że - przynajmniej w części - obecne przepisy są wystarczające, a umiejętne posługiwanie się analogią da możliwość pokazania, że być może w wielu aspektach SI to jedynie nowość technologiczna, ale prawnie podobna do tego, co już obecnie nas otacza.

W pierwszej części pracy wskazany zostanie rys historyczny rozwoju SI, a następnie próby nakreślenia tego, jak SI jest definiowana. W dalszej części przejdę do badania możliwości posługiwania się SI przy składaniu oświadczeń woli, a także korzystania z przepisów o wadach tych oświadczeń. Kolejny fragment to odpowiedzialność kontraktowa za działania SI, zaś następny rozdział dotyczyć będzie odpowiedzialności deliktowej za czyny SI. Ostatni znaczący

rozdział to analiza wydanych 4 maja 2020 roku przez komitet ds. prawnych Unii Europejskiej rekomendacji[7] dotyczących konkretnego brzmienia przepisów rozporządzenia UE w sprawie odpowiedzialności deliktowej SI. Na samym końcu pracy przyjrzę się przepisom UZNK w świetle tego, jakie realne zagrożenia niesie dla uczciwości konkurencji posługiwanie się systemami SI, także z perspektywy konsumentów, wskazując na potencjalne podstawy i zasady ich ochrony odszkodowawczej.

2. Definicja sztucznej inteligencji

2. 1. Historia sztucznej inteligencji[8]

Warto zwrócić uwagę na to, że temat sztucznej inteligencji nie jest niczym nowym. Mogłoby się wydawać, że dyskusja na temat tej technologii rozpoczęła się stosunkowo niedawno i jest to zupełna nowość w technologicznym świecie. Nic bardziej mylnego. Co prawda dopiero od niedawna technologia pozwala nam na rozwijanie i pełne praktyczne wykorzystywanie wiedzy leżącej u podstaw SI, jednak sama koncepcja powstała już kilkadziesiąt lat temu.

W pierwszej kolejności należy wyróżnić osobę Alana Turinga[9], który jest wybitną osobowością w zakresie informatyki i kryptologii, nauk stanowiących fundament dla technologii SI. Potocznie nazywany jest nawet „ojcem sztucznej inteligencji". Szczególnie kojarzony powinien być z maszyną Turinga i z tzw. testem Turinga, którego zadaniem jest badanie inteligencji danego oprogramowania oraz kwalifikowania go jako inteligentne bądź nie. Maszyna Turinga[10] była abstrakcyjnym projektem maszyny, która składać miałaby się z: „nieskończonej taśmy podzielonej na klatki w taki sposób, że każda klatka może pomieścić 1 symbol z ustalonego zbioru, głowicy czytającej i piszącej w klatkach taśmy symbole z określonego zbioru, pamięci stanów — pojedynczej klatki mogącej pomieścić 1 symbol z ustalonego zbioru urządzenia sterującego wraz z programem tej maszyny Turinga, które powoduje działanie

[7] Pełna treść https://www.europarl.europa.eu/doceo/document/JURI-PR-650556_EN.pdf (dostęp:10.04.2020)

[8] Zob. szerzej np. U. Król, *Sztuczna inteligencja i systemy ekspertowe. Omówienie wybranych zagadnień w świetle piśmiennictwa 2005-2010,* Kraków 2011, s. 9 i n, a także https://www.coe.int/en/web/artificial-intelligence/history-of-ai (dostęp: 9.01.2020) i http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/ (dostęp: 9.01.2020)

[9] https://encyklopedia.pwn.pl/haslo/Turing-Alan-Mathison;3990107.html (dostęp: 20.11.2019)

[10] https://encyklopedia.pwn.pl/haslo/Turinga-maszyna;3990108.html (dostęp: 20.11.2019)

głowicy (tj. czytanie i pisanie), przesuwanie taśmy (w obydwu kierunkach) i zmianę zawartości pamięci stanów"[11]. Maszyna ta to bardzo ważny koncept w dziedzinie informatyki, gdzie porozumiewanie się z komputerem sprowadza się do zapisu informacji w systemie binarnym (tj. zer i jedynek). Maszyna pozwalała zapisać nieskończony ciąg czynności wykonywanych na podstawie ustalonego algorytmu.

Natomiast Test Turinga, zaprezentowany przez autora w 1950 roku, w swoim założeniu jest bardzo prosty i ta prostota, niestety, okazała się także jego słabością. Maszyna wyposażona w oprogramowanie, które poddajemy testowi, prowadzi rozmowę z człowiekiem zwanym „sędzią". Po zakończonej rozmowie sędzia może podjąć dwie decyzje: uznać, że rozmawiał z człowiekiem, bądź że rozmawiał z maszyną. Test Turinga jest zaliczony, a oprogramowanie uznane za inteligentne wtedy, kiedy sędzia uzna maszynę, z którą rozmawiał, za człowieka.

Test ten został jednak poddany krytyce. Zarzutów było kilka, ja wspomnę tylko o dwóch. Po pierwsze, co jest widoczne szczególnie w czasach obecnych, nie ma problemu w stworzeniu oprogramowania, które będzie nastawione na zaliczenie testu Turinga, a w żadnym stopniu nie będzie wykazywać elementów inteligencji. Po drugie, test ten nie jest w pełni obiektywny, gdyż ocena danego rozmówcy może być uzależniona od wielu czynników jak np. język ojczysty sędziego i jego wykształcenie. Zupełnie inne odczucia po rozmowie z daną maszyną będzie mieć wykształcony Amerykanin, a zupełnie inne niewykształcony Kolumbijczyk, ponieważ różni ich poziom posiadanej wiedzy, doświadczenia, zależności kulturowe i językowe. Pierwszy argument został poparty przez inny koncept myślowy autorstwa Johna Searle'a[12], wybitnego amerykańskiego filozofa. Test chińskiego pokoju[13] w bardzo prosty sposób pokazuje, że niestety test Turinga może być bardzo nieefektywny. Założenie jest następujące: w zamkniętym pokoju siedzi człowiek, może to być Polak, który nie zna języka chińskiego. Za drzwiami jest jego rozmówca, porównując to do definicji z testu Turinga nazwijmy go sędzią. Zapisuje on na kartce papieru wiadomość po chińsku i wsuwa ja pod drzwi. Zamknięty w pokoju człowiek widzi kartkę zapisaną zupełnie nieznanymi dla siebie znakami. Na szczęście jednak w pokoju znajduje się księga, instrukcja działania. W księdze tej umieszczone zostały wytyczne co do tego, w jaki sposób odpowiadać

[11] *Ibidem*

[12] https://encyklopedia.pwn.pl/haslo/Searle-John-Rogers;3973438.html (dostęp: 20.11.2019)

[13] https://plato.stanford.edu/entries/chinese-room/ (dostęp: 21.11.2019)

na określone znaki. Nasz człowiek zamknięty w pokoju sprawdza więc swoje znaki z kartki, następnie odpisuje na nie w sposób wskazany w księdze i wsuwa odpowiedź pod drzwi. Znajdujący się za drzwiami człowiek dostaje piękną odpowiedź w swoim ojczystym języku. Dla niego więc osoba wewnątrz pokoju z całą pewnością zna język chiński, w końcu poprawnie odpowiedziała na jego wiadomość. Oczywiście w rzeczywistości cały proces zajmowałby dużo czasu, ale przekładając to na systemy mające olbrzymie moce obliczeniowe wykonanie takiej operacji, nawet przy gigantycznej ilości wprowadzonych danych, trwać będzie krótką chwilę.

Terminu „sztuczna inteligencja" użył po raz pierwszy John McCarthy, amerykański matematyk i informatyk, który w roku 1971 otrzymał nagrodę Turinga, która przyznawana jest za wybitne osiągnięcia w dziedzinie informatyki. Zgodnie z jego definicją sztuczna inteligencja to „nauka i inżynieria tworzenia inteligentnych maszyn".[14] Samo pojęcie pojawia się po raz pierwszy na konferencji w Dartmouth w roku 1956. Konferencja ta jest przełomowa dla całej nauki o SI, a zainicjowana została przez takich ludzi jak wspomniany John McCarthy, a także Marvin L. Minsky, Nathaniel Rochester i Claude E. Shannon w ich „wniosku dotyczącym projektu badawczego nad Sztuczną Inteligencją na konferencji w Dartmouth".[15] Podczas konferencji zaprezentowany został także program „The Logic Theorist" stworzony przez Allena Newella, Cliffa Shawa i Herberta Simona, a który uważany jest obecnie za pierwszy program sztucznej inteligencji.[16] Od czasu wspomnianej konferencji dynamika prac nad rozwojem SI rosła coraz bardziej, będąc realnym do spełnienia marzeniem o robotach, które w wielu dziedzinach będą mogły wyręczyć człowieka. Zainteresowanie SI przejawiały także organizacje rządowe takie jak amerykańska agencja rządowa Defense Advanced Research Projects Agency (DARPA), która wsparła finansowanie badań nad SI w kilku instytucjach. Rząd amerykański był szczególnie zainteresowany maszyną, która potrafiłaby transkrybować i tłumaczyć język mówiony, a także przetwarzać dane o wysokiej wydajności.[17] Optymizm wzrósł tym bardziej, kiedy w roku 1970 w wypowiedzi dla magazynu „Life Magazine" wspomniany już Marvin

[14] zob. https://jmc.stanford.edu/articles/whatisai/whatisai.pdf (dostęp: 9.01.2020), https://www.artificial-solutions.com/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence (dostęp: 9.01.2020)

[15] zob. „*AI Magazine*" 2006, nr 4, s. 12-14, http://www-formal.stanford.edu/jmc/history/dartmouth.pdf (dostęp: 9.01.2020)

[16] http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/ (dostęp: 09.01.2020)

[17] *Ibidem*

Minsky powiedział, że osiągnięcie przez technologię SI poziomu inteligencji typowego człowieka zajmie „od trzech do ośmiu lat".[18] Niestety rozwój nad SI przystopował aż do połowy lat 80 XX w., głównie z powodów ograniczeń technologicznych. W tym czasie rozwijały się jednak badania nad, wykorzystywanymi obecnie na bardzo szeroką skalę w zakresie budowania SI, koncepcjami uczenia maszynowego, za którymi stali John Hopfield i David Rumelhart oraz technologią sztucznych sieci neuronowych. Sztuczne sieci neuronowe mają zasadniczo odwzorowywać sieci neuronowe w mózgu człowieka w pełnym jego zakresie, dzięki czemu maszyna może myśleć jak człowiek. Uczenie maszynowe natomiast pozwala algorytmowi SI uczyć się nowych funkcjonalności na podstawie danych, jakie są wprowadzane i zbierane na przestrzeni czasu pracy algorytmu. Okres ten to także prace nad systemami eksperckimi, za sprawą Edwarda Feigenbauma, które stanowią zdecydowaną większość algorytmów SI. Systemy eksperckie obejmują swoim zakresem działania tylko wąskie dziedziny takie jak diagnozowanie nowotworów, przygotowywanie prostych umów, zwłaszcza w obrocie masowym (umowy adhezyjne) czy analiza przestrzeni powietrznej dla wojska. Nie są one więc w stanie zaproponować nam zakupów na podstawie przeglądanych stron w Internecie czy przeprowadzić z nami zwykłej rozmowy.

Początek lat 90 XX w. to kolejny skok w pracach nad SI. Szerokim echem odbił się pojedynek ówczesnego szachowego mistrza i niepodważalnego autorytetu w tej dyscyplinie Garego Kasparova z algorytmem SI Deep Blue autorstwa IBM.[19] Algorytm od IBM pokonał mistrza w tym pojedynku. Jednak już od dłuższego czasu sukces ten nie jest uznawany za spektakularny, ponieważ gra w szachy nie jest bardzo skomplikowana i opiera się na obliczeniach matematycznych. Program nauczony reguł gry jest w stanie tak dostosować swoją taktykę, aby osiągnąć określoną wartość matematyczną, która da mu zwycięstwo. Nie przejawia zatem żadnych inteligentnych cech. Dużo większą wagę przywiązuje się do zwycięstwa w 2011 roku w programu Jeopardy, gdzie program IBM o nazwie Watson pokonał ówczesnych mistrzów w popularnym amerykańskim teleturnieju.[20] Co prawda nie obyło się bez błędnych odpowiedzi, powtarzanych niekiedy po rywalach, czy też wynikających ze zwykłego braku wiedzy, jednak ostatecznie wynik był taki,

[18] *Ibidem*

[19] *Ibidem*; https://www.spidersweb.pl/2017/12/sztuczna-inteligencja-szachy.html (dostęp: 9.01.2020); https://www.newsweek.pl/wiedza/historia/deep-blue-wygral-20-lat-temu-w-szachy-z-garrim-kasparowem/1g9xnt7 (dostęp: 9.01.2020)

[20] https://kreczmar.gadzetomania.pl/58784,watson-sztuczna-inteligencja (dostęp: 09.01.2020)

że Watson zmiażdżył swoich rywali, a IBM ogłosił olbrzymi sukces. Od tego czasu w algorytm została wpompowana ogromna ilość pieniędzy, a jego wykorzystanie przejawia się np. w medycynie, gdzie Watson zajmuje się terapią raka płuc. Kolejny znaczący sukces należał już do Googla, a konkretnie firmy DeepMind będącej w koncernie giganta z Kalifornii. Stworzyli oni program o nazwie „AlphaGo", który miał mierzyć się z zawodowymi graczami w grze „Go", uznawanej za jedną z najbardziej skomplikowanych gier logicznych. Pierwszy sukces AlphaGo to rok 2015, kiedy program pokonał w grę zawodowego gracza, jednak prawdziwy sukces to rok 2017, kiedy to SI pokonała arcymistrza w grze Go, wybitnego 19-letniego gracza, uznawanego za „cudowne dziecko" tej gry.[21] Pojedynek zakończył się zwycięstwem do zera, co udowodniło, że aktualnie nie ma na świecie innego przeciwnika, poza inną maszyną, z którym AlphaGo mógłby się mierzyć. Sam algorytm jest oparty o dwa „mózgi" sztucznych sieci neuronowych, gdzie jeden z nich odpowiada za wybór kolejnego ruchu, natomiast drugi analizuje ten ruch, jego skutki i przewidywanego zwycięzcę pojedynku, sięgając w swoich obliczeniach o około 50 ruchów naprzód.[22] Gra, przynajmniej w moim odczuciu, wymaga dużo większej analizy wykonywanych ruchów niż gra w szachy. Jak zresztą powiedział dyrektor generalny DeepMind Demis Hassabis [jeżeli zapyta się szachistę: "dlaczego zrobiłeś ten ruch", on lub ona prawdopodobnie opowie o swoim planie: "ponieważ A, B i C". Ale jeżeli zada się to samo pytanie zawodnikowi Go, w odpowiedzi usłyszy się przeważnie: "ponieważ to wydaje się dobrym ruchem"].[23]Żeby uzmysłowić czytelnikowi jak olbrzymi sukces odniósł algorytm AlphaGo warto jeszcze przytoczyć wypowiedzi pokonanego mistrza Ke Jie, który był zszokowany przebiegiem przegranego pojedynku, a zdaniem którego wiele ruchów wykonanych przez SI nigdy by się nie zdarzyło w rywalizacji z ludzkim przeciwnikiem. Co więcej, po zakończonym pojedynku powiedział on, że „jest on (AlphaGo) poza moim zasięgiem" oraz „to gracz o boskich zdolnościach".

Obecnie SI wykorzystywana jest w bardzo wielu branżach. Z powodzeniem diagnozuje przypadki medyczne, w dodatku dużo lepiej niż ludzie, a w Chinach udało jej się nawet z przyzwoitym wynikiem zdać państwowy egzamin lekarski.[24] Obecnie w naszych domach także nie brak urządzeń

21 https://businessinsider.com.pl/wiadomosci/sztuczna-inteligencja-alphago-od-google-wygrala-z-arcymistrzem/p9c7r42 (dostęp: 9.01.2020)
22 *Ibidem*
23 *Ibidem*
24 https://antyweb.pl/robot-zdaje-egzamin-lekarski/ (dostęp: 10.01.2020)

inteligentnych – lodówki, które same zamawiają produkty czy usługi serwisowe, roboty sprzątające skanujące pomieszczenie, wykrywające kiedy wjechały na dywan i powinny zwiększyć moc ssania, autonomiczne samochody, które w związku ze zbliżającym się terminem wdrożenia sieci 5G zaczną być coraz bardziej powszechne. W marketingu wszechobecne jest dobieranie produktów na podstawie przeglądanych przez daną osobę stron internetowych, ale także posiadanego modelu urządzenia, na którym te strony są przeglądane. Jeśli np. nasze konto Google będzie połączone z telefonem, laptopem i telewizorem danej marki to znacznie częściej właśnie tej marki produkty będziemy oglądać. Stacje paliwowe czy Uber, świadczący usługi transportu osób, to z kolei przykład inteligentnego sterowania cenami w zależności od natężenia ruchu, pory dnia, pogody itp. Z kolei bardzo często wyświetlające się nam ekrany służące potwierdzeniu, że nie jesteśmy robotem, w ten sposób, że musimy wybrać zdjęcia z określonym przedmiotem np. sygnalizacją świetlną, to nic innego jak system służący do nauki algorytmu SI.

Rozważania na temat przeszłości i teraźniejszości SI należy zakończyć odniesieniem do tego, co nas czeka w przyszłości. Obecnie jeszcze SI posiadająca samoświadomość i uczucia, swoje własne cele i wartości, jest dla nas tematem odległym. Prawdopodobnie jednak również i takie algorytmy powstaną. Warto w tym miejscu przytoczyć wypowiedź prof. Stephena Hawkinga, według którego „Prawdziwym ryzykiem związanym z rozwojem sztucznej inteligencji nie jest to, że będzie złośliwa, a to w jakie kompetencje będzie wyposażona. Superinteligentna SI będzie świetnie radzić sobie z osiąganiem określonych celów, a jeśli te cele nie będą spójne z naszymi, to będziemy mieli problem.[25] Pewnym krokiem naprzód w rozwoju SI będzie wprowadzenie algorytmu w systemy oparte o komputery kwantowe. Tego typu komputery mają moc obliczeniową nieporównywalnie większą niż nawet najlepsze obecne jednostki. Ma to kluczowe znaczenie dla SI, która swoją przewagę opiera na możliwości analizy setek milionów danych w niesamowicie szybkim czasie. Nie tak dawno, bo na jesieni 2019 roku Google pochwalił się, że zbudował pierwszy komputer kwantowy z prawdziwego zdarzenia.[26]

[25] https://businessinsider.com.pl/technologie/profesor-stephen-hawking-o-sztucznej-inteligencji/ph31g7z (dostęp: 10.01.2020)

[26] Zob. szerzej https://tech.wp.pl/google-zbudowalo-najpotezniejszy-komputer-kwantowy-na-swiecie-totalny-przelom-6426886742259329a (dostęp: 10.01.2020)

2. 2. Sztuczna inteligencja – czyli co?

Dużo już razy w tej pracy padało pojęcie sztucznej inteligencji, a jeszcze więcej razy pojawi się ono w dalszej jej części. Warto więc poświęcić trochę uwagi temu czym ona właściwie jest. Ścierają się tutaj dwie perspektywy definicyjne. Pierwsza to ta techniczna. Nie mam wystarczającej wiedzy technicznej, aby opisać kompleksowo jak działa SI, niemniej jednak pewne podstawowe kwestie należy wyjaśnić. Druga perspektywa to już spojrzenie prawnicze. Zdefiniowanie SI jest kluczowym i podstawowym krokiem w kierunku właściwego stosowania przepisów, a jeszcze bardziej jest ona potrzebna do tego, aby nowe przepisy tworzyć. Wszelkie nowe regulacje będą skuteczne tylko wtedy, jeżeli ich zakres zastosowania będzie obejmować SI. Na tym etapie brak jednolitej definicji SI, a stworzenie jej będzie prawdopodobnie bardzo trudne, z uwagi na złożoność tego typu programów, a także to, że jak każdy algorytm działają one na innym urządzeniu, poprzez inne urządzenie czy też w innym urządzeniu (tzw. powłoce). Niemniej jednak Unia Europejska we wspomnianych na początku rekomendacjach komitetu ds. prawnych zdecydowała się na stworzenie definicji legalnej SI. Analiza tej definicji zostanie dokonana w rozdziale poświęconym tej propozycji.

Na początek warto jednak, w ślad za prof. Chłopeckim, którego praca „Sztuczna inteligencja – szkice prawnicze i futurologiczne”[27] będzie stanowić główny punkt odniesienia mojej pracy, krótko zdefiniować samą inteligencję. Sięgając do definicji inteligencji w encyklopedii PWN przeczytamy, że jest to „jedno z najbardziej wieloznacznych pojęć w psychologii odnoszące się do sprawności w zakresie czynności poznawczych; w języku potocznym przez inteligencję rozumie się najczęściej zdolność rozwiązywania problemów praktycznych, zdolności językowe lub kompetencje społeczne”[28]. Jak widać więc fragment powyższego cytatu odnoszący się do zdolności do rozwiązywania problemów pokrywa się z tym, czego oczekujemy od SI. Im bardziej zaawansowany algorytm, tym trudniejsze i bardziej złożone problemy powinien rozwiązywać, a jego zdolności językowe mają służyć jak najbardziej przejrzystemu gromadzeniu i prezentowaniu informacji. Zagłębiając się w powyższą definicję słownikową przeczytamy, że zdaniem ekspertów inteligencja jest „zdolnością uczenia się na podstawie własnych doświadczeń oraz zdolnością przystosowania się do otaczającego środowiska”. Jest to kolejny element wspólny z rozumieniem algorytmów SI, które wspominaną wcześniej

[27] Warszawa 2018, wyd. 1

[28] https://encyklopedia.pwn.pl/haslo/inteligencja;3915042.html (dostęp: 11.01.2020)

zdolność rozwiązywania problemów czerpią z własnej nauki tzw. machine learning, w oparciu o analizę danych, które są do algorytmu wprowadzane, a z kolei dzięki tej nauce SI potrafi sama dostosować się do otaczającego ją świata. Już obecnie coraz więcej pojawia się przypadków, gdy SI sama zmienia swój algorytm, aby dostosować się do sytuacji np. pies-robot, który stracił jedną nogę przekształca swój algorytm tak, aby móc chodzić na trzech nogach. Jest to przykład, który niekiedy widzimy u prawdziwych zwierząt np. psów, które straciły jedną z nóg w wypadku. Na koniec wreszcie definicji PWN czytamy, że „inteligencja ujmowana jako cecha ludzkiego umysłu to zdolność myślenia, rozwiązywania problemów oraz angażowania adekwatnych do okoliczności procesów poznawczych (takich jak np. uczenie się, szybkość przetwarzania informacji, zasoby uwagi, pamięć robocza, kontrola poznawcza), od których zależy skuteczność przystosowania się do nowych sytuacji i sprawność działania."[29] Chociaż w definicji tej znajdujemy odwołanie do inteligencji jako cechy ludzkiej, to jednak wymienione tutaj cechy jak uczenie się, szybkość przetwarzana informacji czy zdolność rozwiązywania problemów to cechy przejawiane przez każdą liczącą się SI, a w zakresie przetwarzania informacji SI już od dawna jest w stanie przeprowadzać analizy znacznie szybciej i lepiej niż człowiek. Chociaż zatem inteligencja jest cechą przypisywaną jedynie człowiekowi to należy zastanowić się nad tym, i jest to problem dla psychologów czy socjologów, czy nie należy definicji tej rozszerzyć także na SI, zwłaszcza tzw. silną SI. Silna SI obecnie jeszcze nie istnieje, a jej stworzenie pozostaje nieco odległe. To co jest jej cechą wyróżniającą to samoświadomość, autonomiczność. Taki algorytm potrafiłby uczyć się funkcji społecznych, mieć poczucie humoru, uczucia, a co dla nas groźne, o czym przestrzega prof. Hawking, miałaby także własne cele.

Po zdefiniowaniu bardzo ogólnie inteligencji można zacząć zastanawiać się nad tym czym jest sztuczna inteligencja. Wspominałem już o definicji, którą przedstawił John McCarthy. Sięgając ponownie do definicji w encyklopedii PWN czytamy, że SI to „dział informatyki badający reguły rządzące zachowaniami umysłowymi człowieka i tworzący programy lub systemy komputerowe symulujące ludzkie myślenie".[30] Obie definicje odnoszą się jednak do dziedziny nauki, a nie ujęcia tego czym jest dany algorytm. W tym miejscu nie ma potrzeby i sensu przedstawiać żadnych naukowych i technicznych opracowań dotyczących SI, gdyż praca ta ma pomagać ludziom, którzy nie

[29] *Ibidem*

[30] https://sjp.pwn.pl/sjp/sztuczna-inteligencja;2466532.html (dostęp: 11.01.2020)

mają wykształcenia informatycznego czy technicznego. Najlepszym więc sposobem uchwycenia tego, czym jest SI, jest przedstawienie jej cech, które każdy z nas jest w stanie zidentyfikować.

Dla przykładu można wskazać kilka definicji słownikowych. W słowniku Oxfordu czytamy, że jest to „teoria i rozwój systemów komputerowych zdolnych do wykonywania zadań normalnie wymagających ludzkiej inteligencji, takich jak percepcja wzrokowa, rozpoznawanie mowy, podejmowanie decyzji i tłumaczenie między językami". [31] Definicja Merriam-Webster z kolei wskazuje, że jest to „zdolność maszyn do naśladowania inteligentnych ludzkich zachowań".[32] Warto wskazać, że SI to "zbiór technologii, obejmujących machine learning (ML), systemy rozpoznawania dźwięku i obrazów, przetwarzania języka naturalnego (NLP), transkrypcji i symulacji głosu oraz innych specjalistycznych narzędzi, wykorzystujących głębokie sieci neuronowe (deep learning)."[33] Wystarczająca dla tego opracowania definicję przedstawia w swoim artykule[34] Michał Konrad Derdak, który pojęci SI „uznaje za zbieżne z pojęciem [inteligentnych agentów programowych] (inteligent software agents), a więc programów komputerowych nakierowanych na osiągnięcie efektu określonego przez użytkownika, odbierających bodźce pochodzące ze środowiska zewnętrznego i reagujące na nie w sposób wpływający na to środowisko". Za cechy wyróżniające uznaje pewien stopień autonomiczności, możliwość uczenia się i wykorzystanie wiedzy w celu osiągania efektów.[35]

Sztuczną inteligencję dzieli się zasadniczo na tzw. słabą SI i silną SI. Jak już wyżej zaznaczono silna SI to taka, która posiada własną świadomość i będzie potrafiła wyjść poza zaprogramowane schematy w celu osiągniecia swoich własnych celów, więc zasadniczo będzie poza kontrolą człowieka. Będzie jak małe dziecko, które z czasem zacznie się uczyć i uzyskiwać coraz dalej idącą autonomiczność. Natomiast słaba SI otacza nas już dzisiaj. Są to inteligentne algorytmy, które działają w celu określonym przez programistę. To jak działają zależy już od konkretnych rozwiązań tj. głównie zabezpieczeń wbudowanych w kod źródłowy, bazy danych, z której czerpią wiedzę oraz od nadzoru człowieka. Nadzór ten dotyczy wspomnianego już machine learning czyli

[31] https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/#69f0c12f4f5d (dostęp: 13.01.2020)
[32] *Ibidem*
[33] https://planetpartners.pl/czym-jest-sztuczna-inteligencja/ (dostęp: 13.01.2020)
[34] „*Czy androidy śnią o zmowach cenowych? Algorytmy cenowe, sztuczna inteligencja i prawo konkurencji*" Michał Konrad Derdak, Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2018, nr 8(7), www.ikar.wz.uw.edu.pl
[35] *Ibidem*

uczenia maszynowego. Algorytmy rozwijają się dzięki możliwości uczenia się z danych, które wpadają do sytemu i są przetwarzane przez algorytm. Na przykład algorytm cenowy na podstawie zbieranych danych zauważa, że w porze deszczowej więcej osób zamawia taksówki czy Ubera. W związku z tym postanawia w tym okresie zwiększyć cenę za przejazd, kontrolując jednocześnie to, o ile maksymalnie może te ceny podnieść, tak aby ruch nie spadł. Uczenie maszynowe powinno być nadzorowane i kwestii tej warto poświęcić chwilę, gdyż to będzie jedno z możliwych odniesień w przypadku ustalania odpowiedzialności SI. Uczenie maszynowe można podzielić na:[36]

- nadzorowane *(ang. supervised);*
- nienadzorowe *(ang. unsupervised);*
- półnadzorowane *(ang. semi-supervised);*
- ze wzmocnieniem *(ang. reinforcement).*

Nie zagłębiając się w szczegóły techniczne warto nakreślić czym charakteryzuje się każdy z tych modeli.[37]

Uczenie nadzorowane wykorzystywane jest w sytuacji, kiedy mamy jasno określony cel i jasno określone dane. W powołanym artykule „A beginner's guide to AI: Supervised and unsupervised learning" podaje się przykład SI zajmującej się rozpoznawaniem obrazów. Programiści przepuszczają przez algorytm SI ogromną ilość obrazów np. zwierząt, starając się nauczyć SI odróżniać psa od kota. Proces ten opiera się na wyszukiwaniu charakterystycznych cech danych zwierząt na podstawie jak największej ilości danych. Następnie poszczególne obrazy są grupowane przez SI, a to grupowanie sprawdzają programiści, następnie nanoszą niezbędne poprawki i ponownie zalewają algorytm zbiorem określonych danych. Założenie jest dosyć proste, a sam proces nie bardzo skomplikowany, stąd udział czynnika ludzkiego jest istotny, aby prawidłowo dopasować reakcje algorytmu.

Uczenie nienadzorowane, jak nazwa wskazuje, jest przeciwieństwem przedstawionego powyższej modelu. Stosowane jest wtedy, kiedy nie wiemy czego szukamy i czego nasz algorytm ma się nauczyć. W artykule podaje się przykład podejrzenia wyprowadzania pieniędzy ze spółki. Nie da się nauczyć SI jak wykrywać takie zachowanie bez wprowadzenia odpowiedniej ilości

[36] https://planetpartners.pl/czym-jest-sztuczna-inteligencja/ (dostęp: 13.01.2020); https://thenextweb.com/artificial-intelligence/2019/07/06/a-beginners-guide-to-ai-supervised-and-unsupervised-learning/ (dostęp: 13.01.2020)

[37] Na podstawie https://thenextweb.com/artificial-intelligence/2019/07/06/a-beginners-guide-to-ai-supervised-and-unsupervised-learning/ (dostęp: 13.01.2020); https://www.datarobot.com/wiki/semi-supervised-machine-learning/ (dostęp: 13.01.2020)

przykładów. Można jednak wykorzystać ją do wykrywania pewnych grup zachowań, anomalii płatniczych i tzw. kreatywnej księgowości. SI nie odpowie nam kto, jak i kiedy dokonał takiej kradzieży, ale da nam zestaw pewnych grup działań i powtarzalnych czynności, które będziemy mogli właściwie zinterpretować. Bardzo głośnym przykładem nienadzorowanego uczenia maszynowego SI był program Tay firmy Microsoft. Tay miało imitować 19-letnią przeciętną Amerykankę. Algorytm został umieszczony na portalu społecznościowym Twitter i każdy swobodnie mógł nawiązać z nim interakcję. Program uczył się i poszerzał zasób swojego słownictwa oraz czegoś na kształt światopoglądu w oparciu o dane z rozmów z prawdziwymi użytkownikami.[38] Niestety ledwo w dobę po uruchomieniu projektu należało go zawiesić, ponieważ system SI zaczął wychwalać Hitlera, stał się rasistą i używał słów niecenzuralnych. Oczywiście wszystko to było wynikiem tego jacy ludzie pisali do Tay i jakiej treści były powyższe wiadomości. Niemniej jednak odpowiedzialni za tego typu zdarzenia, w przypadku wyrządzenia realnej szkody, mogą być programiści, którzy powinni przewidzieć pewne możliwe i prawdopodobne scenariusze. Sam algorytm i jego uruchomienie w trybie nienadzorowanym stanowiło eksperyment, dzięki któremu wiemy, że przy podobnych programach koniecznym będzie zastosowanie odpowiednich filtrów treści, zablokowanie używania pewnych słów, być może nawet wykluczenie możliwości włączenia do bazy wypowiedzi, w których pojawiają się określone frazy. Tak czy inaczej jest to dobry przykład tego, że uczenie nienadzorowane to olbrzymie możliwości, obarczone jednak ryzykiem, które należy przewidzieć i chociaż starać się je zminimalizować, ponieważ niepodjęcie żadnych działań z całą pewnością nie może zostać uznane za rzetelne działanie.

Uczenie półnadzorowane jest już nieco bardziej skomplikowanym procesem. Jak nazwa wskazuje łączy on w sobie elementy obu poprzednich rozwiązań. Stosuje się go wtedy, kiedy mamy jasno określony cel i wiemy czego szukamy, ale mamy za mało danych, które nie są wystarczające do uruchomienia modelu nadzorowanego. W przypadku wyprowadzania pieniędzy ze spółki sytuacja jest następująca: mamy zidentyfikowany jeden konkretny przypadek, równocześnie posiadamy jednak wiedzę o tym, że jest ich więcej. Wprowadzamy więc posiadane dane o kradzieży do systemu, który analizuje inne, neutralne dla nas dane i zwraca nam wynik z szeregiem swoich wniosków. Na tej podstawie możemy zidentyfikować inne nieprawidłowości, dzięki czemu

[38] https://www.spidersweb.pl/2016/03/tay-bot-microsoft-sztuczna-inteligencja.html (dostęp: 13.01.2020)

nasza baza danych jest większa. Kolejny raz powtarzamy cały proces, tym razem jednak z posiadanymi, nowymi danymi. W ten sposób dochodzimy do momentu, gdy dane są wystarczające do tego, aby z powodzeniem stosować już model nadzorowanego uczenia maszynowego.

Ostatni wspomniany model czyli uczenie ze wzmocnieniem jest nieco skomplikowany. Opiera się on na podejmowaniu przez algorytm sekwencji decyzji.[39] Całość opiera się na metodzie prób i błędów, a celem SI jest uzyskanie określonej „nagrody". Nagroda przyznawana jest przez człowieka. W przypadku błędnych decyzji algorytm spotyka „kara". Nie dostaje on żadnych wskazówek, działa więc wyłącznie w celu osiągniecia nagrody i wybiera drogę do tego celu według własnego uznania. W związku z tym stosowane jest mnóstwo różnych kombinacji, a im dłużej działa algorytm, tym więcej się nauczy. Dla przykładu wyobraźmy sobie grę, nazwijmy ją „Grzybobranie", w której naszym zadaniem jest omijanie przeszkód (np. drzewa, krzaki, ptaki) i zbieranie grzybów (ale bez muchomorów!). Gra wygląda jak klasyczna platformówka w stylu Mario. Nasz algorytm idzie w prawo i uderza w drzewo. Koniec gry. Kolejna próba – już wie, że ma uważać na drzewa. Niestety wpadł na krzak. Kolejna próba – bank informacji się powiększył i nasz algorytm z sukcesem omija kolejne przeszkody aż natrafia na grzyba, który podnosi. Dostaje za to nagrodę w postaci np. punktów, więc zapisuje, że grzyby należy podnosić. Zebrał kilka grzybów, trafił na muchomora, koniec gry. Tutaj już można zakończyć naszą symulację, gdyż to jak zachowa się SI w kolejnej próbie jest oczywiste. Intuicyjnie wydaje się, że ten system jest najbardziej zaawansowany i rzeczywiście obecnie najbardziej doceniane SI opierają się na takim modelu. Zalety są dwie - po pierwsze algorytm nie jest pozostawiony sam sobie, bo dana osoba kontroluje jego zachowania i ustala wstępne zasady działania, ale równocześnie w zakresie tego systemu SI ma absolutną dowolność kształtowania swoich decyzji. Dzięki temu może dochodzić do rozwiązań, o których człowiek by nie pomyślał, a równocześnie nie narusza ustalonych z góry granic czy też reguł gry.

Te rozważania techniczne należy zakończyć jeszcze propozycją definicji SI na potrzeby tej pracy. Obecnie brak w polskim prawie definicji SI. W Rezolucji Parlamentu Europejskiego z dnia 16 lutego 2017 roku zawierającej zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczącego

[39] https://deepsense.ai/what-is-reinforcement-learning-the-complete-guide/

robotyki (2015/2103 (INL)) zaproponowano stworzenie definicji SI w oparciu o kryteria takie jak:[40]

- zdolność zdobycia autonomii za pomocą czujników lub wymiany danych z otoczeniem (wzajemna łączność) i analizy tych danych;
- zdolność uczenia się w oparciu o doświadczenie i interakcję;
- forma wsparcia fizycznego robota;
- zdolność dostosowania zachowania i działań do otoczenia.

Postulaty te zostały zrealizowane w zaproponowanej w art. 3 lit a rekomendacji komitetu ds. prawnych Unii Europejskiej, o następującej treści (tłumaczenie autora) „Systemy SI oznaczają system, który wykazuje inteligentne zachowanie poprzez analizę pewnych danych wejściowych i podejmowanie działań, z pewnym stopniem autonomii, w celu osiągnięcia konkretnych celów. Systemy SI mogą być oparte jedynie na oprogramowaniu, działać w świecie wirtualnym lub mogą być wbudowane w urządzeniach sprzętowych”[41]. Oczywiście stworzenie definicji legalnej należy uznać za jak najbardziej prawidłowe działanie, jednak stworzenie dobrej definicji legalnej może okazać się niezwykle trudne. Powyższa definicja chociaż dobrze opisuje to, co obecnie rozumiemy pod pojęciem SI, posługuje się wieloma pojęciami niedookreślonymi, które przy definiowaniu wszelkiego rodzaju przedmiotów prawa jest niepożądane i problematyczne. Szerzej na temat unijnej propozycji w rozdziale 6 niniejszej pracy Wcale niewykluczone jest również, że SI znając prawo postanowi tak zmodyfikować swoje parametry, aby pod definicję SI nie podpadać i pozostawać bezkarną. To oczywiście scenariusz na daleką przyszłość, aczkolwiek wcale nie niemożliwy do spełnienia.

Próby definiowania SI pojawiają się także w Stanach Zjednoczonych, gdzie taka definicja została wprowadzona do National Defense Authorization Act for Fiscal Year 2019 (ustawa upoważniająca do obrony narodowej w roku 2019)[42], zgodnie z którą pod pojęciem SI rozumie się:

(1) Każdy sztuczny system, który wykonuje zadania w zmiennych i nieprzewidywalnych okolicznościach bez znaczącego nadzoru ze strony człowieka

[40] Pełna treść https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52017IP0051 (dostęp: 15.01.2020)

[41] Treść oryginalna „ai's systems means a system that displays intelligent behaviour by analysing certain input and taking action, with some degree of autonomy, to achieve specific goals. AI systems can be purely software-based, acting in the virtual world, or can be embedded in hardware devices”, pełna wersja dokumentu https://www.europarl.europa.eu/doceo/document/JURI-PR-650556_EN.pdf (dostęp: 10.05.2020)

[42]

lub który może uczyć się na podstawie doświadczenia i poprawiać wyniki w przypadku wystawienia na działanie zbiorów danych.

(2) Sztuczny system opracowany jako oprogramowanie komputerowe, sprzęt fizyczny lub w innej formie, który rozwiązuje zadania wymagające ludzkiego postrzegania, poznawania, planowania, uczenia się, komunikowania lub działania fizycznego.

(3) Sztuczny system zaprojektowany do myślenia lub działania jak człowiek, w tym architektury poznawcze i sieci neuronowe.

(4) Zestaw technik, w tym uczenie się maszynowe, który ma na celu wykonanie zadania poznawczego.

(5) sztuczny system zaprojektowany do racjonalnego działania, w tym inteligentny agent oprogramowania lub wcielony robot, który osiąga cele za pomocą percepcji, planowania, rozumowania, uczenia się, komunikowania, podejmowania decyzji i działania.

Definicja powyższa wydaje się być bardzo ciekawym pomysłem i głosem w dyskusji nad tym jak należy przygotować naszą polską czy też ostateczną europejską definicję SI. Zwraca ona uwagę przede wszystkim na uczenie maszynowe, które jest nadzorowane w ograniczonym zakresie, a także na kwestie techniczne takie jak sztuczne sieci neuronowe, na których opiera się aktualnie SI.

W ślad za D. Flisakiem [43] i K. Kuroszem [44] można przytoczyć propozycję, gdzie SI jest zdefiniowana jako zdolność cyfrowych maszyn do naśladowania, imitowania ludzkiej inteligencji, dzięki wykorzystaniu zaimplementowanego w nich oprogramowania. Definicji tej można jednak zarzucić to, że SI to nie tylko maszyny jako takie. Oprogramowanie SI może istnieć w oderwaniu od robota czy komputera, być zawieszone np. na blockchainie, dlatego utożsamianie go z fizycznym przedmiotem jest nieco błędne, chociaż być może wspominane ujęcie kryję się pod dodatkiem „cyfrowych". Ten aspekt został uwzględniony w propozycji uregulowań unijnych i dla niniejszej pracy przyjąć należy właśnie tam zaproponowaną definicję, gdyż być może w najbliższej przyszłości, z pewnymi modyfikacjami, stanie się prawem powszechnie obowiązującym w całej Unii Europejskiej na mocy projektowanego Rozporządzenia.

---

[43] D. Flisak, „Sztuczna inteligencja – jak chronić prawa autorskie twórczości robotów", „Rzeczpospolita", 22.05.2017,https://www.rp.pl/Opinie/305229984-Sztuczna-inteligencja--jak-chronic-prawa-autorskie-tworczosci-robotow.html (dostęp: 15.01.2020).

[44] K. Kurosz *„Zawieranie umów przez sztuczną inteligencję (systemy autonomiczne) a wady oświadczeń woli – wprowadzenie do problemu"* [w:] red. W. Robaczyński *„Czynić postęp w prawie. Księga jubileuszowa dedykowana Profesor Birucie Lewaszkiewicz-Petrykowskiej"*, Łódź 2017, s. 73 i n.

3. Odpowiedzialność kontraktowa

3. 1. Oświadczenie woli

Polski kodeks cywilny w art. 60 stanowi, że „Z zastrzeżeniem wyjątków w ustawie przewidzianych, wola osoby dokonującej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli w postaci elektronicznej (oświadczenie woli)". Ta definicja oświadczenia woli w polskiej doktrynie przeszła pewnego rodzaju ewolucję od teorii woli, przez teorię oświadczenia aż do znajdującej się gdzieś pośrodku nich teorii doniosłości prawnej.

Teoria woli wywodzi się z nauki niemieckiej. Obowiązujący tam termin „oświadczenie woli" (die Willenserklärung) w niemieckiej nauce o czynnościach prawnych rozumiany był jako „wyraz realnie przeżywanego przez człowieka aktu woli zwanego wolą wewnętrzną".[45] Wola ta była rozdzielona pomiędzy akt wewnętrzny, definiowany jako „pragnienie wywołania skutków prawnych" oraz zewnętrzny wyraz tej woli.[46] W przypadku niezgodności woli z jej zewnętrznym przekazem dane oświadczenie było traktowane jako nieważne, a ujmując to najbardziej poprawnie, jak słusznie zauważono, jako oświadczenie nieistniejące, gdyż brak jest woli jako takiej. Teoria ta ma za zadanie chronić interesy osoby składającej to oświadczenie, a jej najbardziej znanym zwolennikiem był B. Windscheid.[47] Jak łatwo się domyślić w obecnych czasach praktykowanie teorii woli byłoby bardzo utrudnione i niepożądane. Po pierwsze, co podnoszą także przeciwnicy tej teorii, a o czym poniżej, bardzo ciężko jest ustalić rzeczywistą wolę danej osoby. Odwoływanie się do psychicznych doświadczeń danego człowieka jest z punktu widzenia dowodowego bardzo problematyczne, chociaż w Polskim prawie praktykowane np. w sprawach karnych. Tam jednak dużo łatwiej przy wykorzystaniu aparatury państwa zgromadzić dużą ilość materiału dowodowego, która pomoże w ustaleniu zamiaru sprawcy. Przy procesach cywilnych podobne praktyki wiązałyby się z niewspółmiernymi kosztami i ingerencją w sferę prywatności

[45] Zob. Z. Radwański, K. Mularski [w:] red. Z. Radwański *„Prawo cywilne – część ogólna. System Prawa Prywatnego. Tom 2",* Warszawa 2019, Legalis, Komentarz do art. 60, Nb 30 i n. (dostęp: 16.01.2020).

[46] *Ibidem*.

[47] Zob. P. Sobolewski [w:] red. K. Osajda *„Kodeks cywilny. Komentarz."* wyd. 24, Warszawa 2020, komentarz do art. 60, Legalis (dostęp: 16.01.2020); A. Jędrzejewska *„Koncepcja oświadczeń woli w prawie cywilnym"*, Warszawa 1992, s. 10-14

poszczególnych osób. Po drugie teoria ta rodzi poważne zagrożenie dla bezpieczeństwa obrotu prawnego, gdyż każdy mógłby w dowolnym momencie uchylić się od swoich oświadczeń twierdząc, że jego wola była inna niż jej wyraz zewnętrzny odczytany przez stronę. Nakłada się na to wszystko jeszcze rzeczywistość jaką jest obrót oparty o komunikację elektroniczną.[48] Algorytmy SI działają na systemach operacyjnych, z którymi porozumiewa się użytkownik. Nawet przyjmując, że jest to słaby algorytm, którego możliwości modyfikujące oferty są nikłe, nie sposób ustalić rzeczywistej woli podmiotu, który algorytm ten uruchomił dla swoich potrzeb. W każdej takiej sytuacji uwolnienie się przez daną osobę od skutków działań algorytmu byłoby w pełni skuteczne.

Teoria oświadczenia (die Erklärungstheorie) stoi w kontrze do teorii woli.[49] Kładzie ona nacisk na oświadczenie danego podmiotu, które jest obierane przez potencjalnego adresata. Jest to więc kryterium obiektywne. Najbardziej znany niemiecki reprezentant tej teorii E. Danz definiuje tą teorię jako „zachowanie osoby, która według doświadczenia obrotu i przy uwzględnieniu wszelkich okoliczności pozwala wnosić o określonej woli, bez względu na to, czy wniosek taki w poszczególnym wypadku jest zasadny, tzn. czy rzeczywiście tego rodzaju wolę wewnętrzną, jaka wynika z oświadczenia, miała dana osoba".[50] Teoria ta na pierwszym miejscu stawia pewność obrotu, praktycznie bardzo mocno ograniczając możliwość ochrony osoby składającej oświadczenie woli. Oświadczenie to zamienia się w ogół słów i znaków, pewnych czynności, które łącznie stanowią przekaz dla odbiorcy, który interpretuje go zgodnie z dana sytuacją. Tak daleko idąca teoria rodzi pewne niebezpieczeństwo przypadkowego złożenia oświadczenia woli, w ogóle nie będąc świadomym tego, że je składamy. Prof. Radwański jako przykład podaje przypadek tzw. aukcji wina w Trieście[51] (das Triererveinversteigerungfall). Otóż cudzoziemiec, który nie zna języka danego państwa, pojawia się w restauracji, gdzie trwa aukcja wina. Podnosi rękę do góry w celu przywołania kelnera, a gest ten, czemu trudno się dziwić, zostaje przez wszystkich odebrany jako oferta w licytacji, która następnie wygrywa.

Teoria doniosłości prawnej (die Geltungstheorie) znajduje się gdzieś pośrodku obu przedstawionych powyżej, próbując odnaleźć dla nich punkt wspólny. Teorie tą stworzył K. Larenz, który twierdzi, że „skutek prawny

---

48 Szerz. zob. W. J. Kocot „*Wpływ Internetu na prawo umów*" Warszawa 2004, s. 65 i n.

49 Szerz. zob. Z. Radwański, „*Kodeks cywilny – część ogólna…"* nb 31*;* K. Osajda „*Kodeks cywilny…"*

50 *Ibidem* w ślad za E. Danz, „*Die Auslegung der Rechtsgechäfte"*, Berlin 1911, s.14

51 Z. Radwański „*Kodeks cywilny – część ogólna…"* nb 30

wywołuje jednolity akt", który łączy w sobie element woli urzeczywistniający się, nabierający kształtu w dostrzegalnym na zewnątrz oświadczeniu.[52] Jak wskazuje prof. Radwański pojawiają się dwa możliwe rozumienia tej koncepcji. Pierwsze z nich wskazuje, że rzeczywista wola oświadczającego jest niezbędna, co przeciąga tą teorię w stronę teorii woli. Drugi natomiast, dominujący w nauce niemieckiej, bardziej dopasowany do sensu całej konstrukcji opiera się na tym, że sama świadomość podmiotu nie jest konieczna, jeżeli przemawia za tym uzasadnione zaufanie odbiorcy oświadczenia wywołane przez zachowanie osoby, która składa dane oświadczenie. Ta koncepcja jest rozwijana w formie tzw. teorii uzasadnionych oczekiwań. [53] Teoria ta opiera się na kryterium uważnego (rozsądnego) uczestnika obrotu. Ocena zachowania powinna opierać się na towarzyszących jej okolicznościach, z uwzględnieniem bezpieczeństwa obrotu i zaufania jakie wywołuje u danej osoby konkretnego zachowanie, jednak powinniśmy spoglądać na całe zdarzenie nie przez pryzmat jednej czy drugiej strony, ale z punktu widzenia im wspólnego.[54]

Najbardziej więc przystosowana do obrotu zautomatyzowanego i elektronicznego, na którym opierają się systemy SI, jest teoria opowiadająca się za jak najbardziej obiektywnym odczytywaniem okoliczności złożenia oświadczenia oraz jego treści, jednak bez całkowitego wyłączania elementu subiektywnego, a więc teoria uzasadnionych oczekiwań, w której element subiektywny, a więc wola składającego oświadczenie za pomocą SI, będzie miała mniejsze znaczenie. Jest ona adekwatna do sposobu zawierania transakcji w automatyzowanym obrocie elektronicznym, w którym nie mamy bezpośredniego kontaktu z drugą osobą, a ponadto oświadczenie woli składane jest w sposób zautomatyzowany i często nie ma dostatecznie dużej możliwości modyfikacji treści przesyłanego pomiędzy stronami komunikatu. W procesie zawierania takich umów nie ma sposobu na sygnalizowanie swoich wątpliwości co do rozumienia wyświetlanych komunikatów, nie ma też możliwości zmiany pewnych ustalonych schematów. Trudne też mówić o realnej woli jakiegoś podmiotu, skoro po drugiej stronie transakcji jest SI. Osoba fizyczna nie jest w stanie zatem w żaden sposób zidentyfikować woli oprogramowania, która nie istnieje, z kolei SI nie ma możliwości analizowania woli osoby fizycznej, ponieważ systemy nie są wyposażone w takie narzędzia. Decydujące będzie więc zawsze obiektywne wrażenie wywołane przez osobę posługująca się systemem

52 *Ibidem*, nb 32

53 Szerzej zob. W. J. Kocot *„Wpływ Internetu…"* s. 61 i n.

54 *Ibidem* w ślad za Z. Radwański *„Kodeks cywilny – część ogólna…"* nb 57 i n.; także A. Jędrzejewska *„Koncepcja oświadczeń…"*

SI, które można wzruszyć tylko poprzez instytucję wad oświadczeń woli (ale tylko tam, gdzie specyfika SI na to pozwala, o czym więcej w kolejnym podrozdziale) albo sytuacje od strony niezależne i przez nią niezawinione np. sytuację, w której doszło do złożenia oświadczenia w wyniku błędu systemu, włamania hackerskiego czy kradzieży tożsamości. Wtedy jednak konieczne jest wykazanie dochowania należytej staranności w zakresie odpowiedniego korzystania z systemu, instalacji wymaganych aktualizacji czy zabezpieczania systemu w zakresie cyberbezpieczeństwa. W ten sposób ujęta została także w regulacji unijnej odpowiedzialność osoby wdrażającej systemy SI – jeżeli dochodzi do wyrządzenia szkody drugiej osobie w wyniku działania osoby trzeciej, której nie uda się zidentyfikować, odpowiedzialny będzie podmiot wdrażający. W przypadku zawierania umów przyjmując przedstawioną powyżej koncepcję chronimy pewność obrotu prawnego. Strony, które decydują się na korzystanie z takich systemów muszą być świadome istniejących ryzyk i wątpliwości, a w konsekwencji albo je zaakceptować albo zdecydować się na korzystanie z innego sposobu zawierania umów. Przyjęcie takiej koncepcji należy jeszcze uzupełnić o obowiązek informowania drugiej strony transakcji o tym, że ma do czynienia z systemem SI. Obowiązek taki powinien zostać nałożony w akcie prawnym o randze ustawy lub rozporządzenia Unii Europejskiej.

Powstaje także pytanie, czy w przypadku SI można rzeczywiście mówić o składaniu oświadczenia woli przez podmiot, który SI się posługuje. Skoro za cechę algorytmu uznaliśmy pewną jego autonomię i możliwość samo uczenia się, to można dojść do wniosku, że to nie osoba posługująca się danym programem składa oświadczenie woli. Wniosek ten jest tylko częściowo poprawny. A. Chłopecki wskazuje w swojej pracy, że SI decyduje o wszystkich składowych zasady swobody umów tj.:[55]

- czy zawrzeć umowę,
- z kim zawrzeć umowę i
- jakiej treści zawrzeć umowę.

Podany przez autora przykład odwołuje się do maszyny sprzedającej napoje, która zaczyna modyfikować swój algorytm uwzględniając temperaturę panującą na zewnątrz, godziny szczytu, datę ważności danego produktu i inne adekwatne czynniki. Wniosek wyprowadzony przez autora, że w takiej sytuacji nie mamy do czynienia z oświadczeniem woli właściciela automatu nie jest trafny. Właściciel automatu stawiając go w określonym miejscu

[55] A. Chłopecki, *„Szkice prawnicze i futurologiczne"*, Warszawa 2018, wyd. 1, Rozdział 3, Legalis (dostęp: 16.01.2020)

oraz ustalając pewne jego funkcje oświadcza gotowość do zawarcia umowy sprzedaży. Chociaż cena nie jest ustalona w sposób jednoznaczny to jednak mieści się w określonym uprzednio przez właściciela przedziale cenowym, została określona konkretna waluta i zakres towarów. Nie ma możliwości, żeby w wyniku takiej interakcji doszło do zakupu samochodu osobowego czy nabycia usługi doradztwa prawnego. Postawienie takiego automatu jest zatem oświadczeniem woli, które następczo będzie jedynie konkretyzowane przez algorytm. Nie dochodzi tutaj do składania nowego, innego oświadczenia woli, gdyż SI to maszyna, która nie ma woli. Wola to cecha przypisywana człowiekowi i jej cechą nieodłączną jest samoświadomość, której słaba SI nie posiada. Podobnie załóżmy, że mamy algorytm obliczający maksymalną kwotę pożyczki, okres spłaty i oprocentowanie. Taki algorytm będzie uczyć się dopasowywać ofertę pod konkretnych klientów na podstawie danych wejściowych jak dochód, ilość członków rodziny, okres zatrudnienia itp. Rzeczywisty wpływ osoby posługującej się takim algorytmem jest całkiem spory, gdyż wyznacza ona ściśle określone warianty proponowanych ofert z uwzględnieniem pewnych matematycznych wzorów. Program taki będzie można nazwać SI, ponieważ doskonali ona swoje decyzje poprzez poszerzanie bazy wiedzy o to, jak klienci spłacali „wymyślone" przez SI warianty spłaty. Nie będzie mogła jednak wyjść poza te określone przez autora programu warianty. W istocie więc każda obecna SI już na etapie jej programowania jest ograniczona w swojej swobodzie decyzji. Nawet w przypadku zastosowania uczenia nienadzorowanego zazwyczaj dochodzi do konkretyzacji funkcji i, mniej lub bardziej, określonego celu. Jedynie w przypadku, gdy algorytm dostanie pełną swobodę działania i jego możliwości będą ograniczone jedynie poziomem inteligencji programu można mówić o tym, że granice nie zostały wyznaczone i w takiej sytuacji SI należy kwalifikować analogicznie do pełnomocnika, a nie jedynie przekaźnika woli osoby, która się tym systemem posługuje. Wszelkie działania SI należy oceniać w sposób obiektywny i na podstawie towarzyszących okoliczności. Jeżeli np. wspominany chatbot Tay zaproponowałby, że sprzeda nam samochód, to takie oświadczenie będzie dla podmiotu posługującego się tym systemem wiążące, chyba że użytkownik zostanie uprzedzony o tym, że prowadzi rozmowę ze SI i jaka jest jej funkcja. Jeżeli na wstępie pojawi się komunikat, że system ten nie może składać wiążących oświadczeń woli i takie zachowanie należy traktować jako błąd oprogramowania to obiektywnie należ uznać, że nie doszło do złożenia oświadczenia woli. Ponadto z pomocą przychodzi także przewidziana w kodeksie cywilnym możliwość uchylenia się od skutków prawnych błędnego oświadczenia woli, jeżeli druga strona

mogła błąd z łatwością zauważyć. Jeżeli zatem w księgarni internetowej zarządzanej przez SI pojawi się oferta sprzedaży czegoś nietypowego dla księgarni np. traktora, to będzie można mówić o błędzie, który druga strona z łatwością mogła zauważyć. Zatem to na podmiotach posługujących się SI będzie spoczywał ciężar odpowiedniego zabezpieczenia swoich interesów, równocześnie jednak w taki sposób, który nie doprowadzi do nadmiernego obciążania dodatkowymi obowiązkami konsumenta. Jeżeli bowiem np. komunikat o zakresie działania SI będzie nieczytelny lub zbyt obszerny to zastosowanie znajdzie chociażby reguła o ochronie konsumenta jako słabszej strony stosunku. Inaczej wygląda sytuacja z tzw. silną SI, która posiada samoświadomość. Żeby można było mówić o silnej SI dany system musi posiadać samoświadomość, mieć własne cele i odczucia. Konsekwencją takich cech jest także posiadanie własnej woli, a zatem również możliwość składania oświadczeń woli. W takim wariancie system nie konkretyzuje woli podmiotu, który się nią posługuje, a składa swoje własne oświadczenie. Obecnie jednak takie systemy nie istnieją, a gdy się pojawią to prawdopodobnie będzie trzeba wyposażyć je w osobowość prawną albo chociaż własny majątek.

W razie odrzucenia wyżej przedstawionej koncepcji można jeszcze rozważać zbadanie podanego przez prof. Chłopeckiego przykładu także pod kątem teorii działania przez przedstawiciela. Należy z całą pewnością odrzucić koncepcję działania przez posłańca, gdyż takie działanie opiera się na przekazaniu oświadczenia o dokładnie takiej samej treści jaka została mu przekazana, a oświadczenie to jest oznaczone co do konkretnego odbiorcy.[56] Jeżeli, jak w powyższym przypadku, algorytm ma możliwość wyboru jednej ze ścieżek to takie działanie nie może zostać uznane za działanie przez posłańca, ponieważ w przedstawionym ujęciu posłaniec nie ma żadnej możliwości ingerencji w składane oświadczenie woli - oczywiście w sposób wiążący dla zlecającego, bo posłaniec może przesyłkę podmienić, zniszczyć itp., ale nie o to nam chodzi. Pozostaje zatem do rozważenia kwestia pełnomocnika. Przepisy regulujące przedstawicielstwo[57] wyróżniają pełnomocnictwo jako jedną z form reprezentacji osoby prawnej, osoby fizycznej czy tzw. ułomnych osób prawnych. Pełnomocnictwo zostało podzielone na ogólne, szczególne oraz rodzajowe. Z innej perspektywy dzieli się je także na ustawowe i oparte na oświadczeniu mocodawcy. Wracając więc do przykładu prof. Chłopeckiego należy rozważyć, czy można mówić tutaj o pełnomocniku. Taka interpretacja nie jest

[56] Szerz. zob. P. Sobolewski [w:] K. Osajda *„Kodeks cywilny. Komentarz"*, Warszawa 2020, komentarz do art. 85,

[57] art. 95 i n. KC

wykluczona. Przepisy o pełnomocniku można stosować na podstawie analogii, ponieważ sama SI nie ma świadomości, nie może zatem złożyć oświadczenia woli w imieniu mocodawcy. Powyższa analogia zatem doprowadzi do powstania pewnej hybrydy, która łączy w sobie elementy pełnomocnictwa i posłańca. Element posłańca objawia się w tym, że SI jest jedynie przekaźnikiem woli podmiotu, który się nią posługuje. Z kolei element pełnomocnictwa, który uważam za mający większe znaczenie, objawia się w możliwości modyfikacji oświadczenia mocodawcy. Najbardziej adekwatny wydaje się model pełnomocnictwa rodzajowego, gdyż jak już wspomniano na początku, obecnie zdecydowana większość SI to systemy eksperckie, nakierowane na czynności w konkretnym obszarze. Pełnomocnictwo rodzajowe dotyczy „działań konkretnie określonych w sensie ich rodzajowego stypizowania"[58] i „powinno ono określać rodzaj czynności prawnej objętej umocowaniem oraz jej przedmiot"[59].[60] W powyższym przykładzie z automatem zdaniem prof. Chłopeckiego „w zakresie dopuszczalności określonych funkcji algorytmu działa jak pełnomocnik z pełnomocnictwem rodzajowym (ograniczonym do sprzedaży napojów) lub w pewnych przypadkach – z pełnomocnictwem ogólnym, natomiast o pełnomocnictwie ogólnym mówilibyśmy jednak pewnie po dodatkowym wyposażeniu maszyny w algorytm płacenia podatków, czynszu etc.[61] W przypadku przyjęcia takiego modelu należy jednak rozważyć problem przekroczenia zakresu pełnomocnictwa. W przypadku SI, która ma ustalone pewne reguły graniczne np. zakaz sprzedaży poniżej pewnej wartości, nakaz sprzedaży w pierwszej kolejności produktów z najkrótszym okresem przydatności do spożycia można z góry określić jaki był zakres udzielonego pełnomocnictwa. W takiej sytuacji ustawodawca powinien wprowadzić repozytorium kodów źródłowych dla takich oprogramowani, w którym będzie można kod umieścić oraz na bieżąco go aktualizować. Korzystanie z tego systemu będzie dobrowolne i odpłatne, w swoje funkcji będzie przypominać rodzaj ubezpieczenia. Nie można zaakceptować wariantu, w którym każdy przedsiębiorca będzie indywidualnie tworzyć takie repozytorium, ponieważ może dojść do próby manipulacji i następczej zmiany kodu umieszczonego w repozytorium, tak aby uwolnić się od odpowiedzialności. Zgodnie bowiem z art. 103 § 1 KC „Jeżeli zawierający umowę jako pełnomocnik nie ma umocowania albo

58 wyr. SN z 10.1.2002 r., II CKN 473/99, Legalis

59 wyr. SN z 4.11.1998 r., II CKN 866/97, Legalis

60 Zob. P. Sobolewski [w:] K. Osajda *„Kodeks cywilny. Komentarz"*, Warszawa 2020, komentarz do art. 98, Legalis (dostęp: 20.01.2020) za: J. Strzebinczyk [w:] red. Gniewek, Machnikowski, *„Kodeks cywilny. Komentarz"*, 2016, art. 98, s. 251, Nb 5

61 A. Chłopecki *„Szkice…"*

przekroczy jego zakres, ważność umowy zależy od jej potwierdzenia przez osobę, w której imieniu umowa została zawarta". Kwestia przekroczenia zakresu pełnomocnictwa to kwestia dowodowa, a w myśl zasad polskiego prawa ciężar dowodu spoczywa na tym kto z danego twierdzenia wywodzi skutki prawne. Jeżeli zatem dojdzie do zawarcia umowy, która zakresem wykracza poza udzielone pierwotnie pełnomocnictwo, potwierdzone w formie kodu umieszczonego w repozytorium, przedsiębiorca będzie mógł nie potwierdzić takiej umowy. Fakt przekroczenia zakresu pełnomocnictwa powinien być badany już w toku procesu sądowego, chociażby na etapie procedury ugodowej. Ujawnienie danych zawartych w repozytorium powinno być możliwe tylko na wniosek uprawnionego organu jakim będzie sąd, a sama treść kodu będzie podlegać weryfikacji przez biegłego sądowego. W tej sytuacji jednak strona umowy pozostanie z niczym, nie będzie miała bowiem żadnego roszczenia – sama SI nie ma majątku, którym mogłaby odpowiadać. Być może w takiej sytuacji jako rodzaj pewnego odszkodowania można wykorzystać środki wpłacane na utrzymanie wspomnianego repozytorium kodu źródłowego, natomiast takie odszkodowanie na pewno nie może w pełni rekompensować ewentualnej straty. Co prawda teoretycznie system powinien mieć zablokowaną możliwość obejścia ustalonych przez nas granic, ale technika ta jest obecnie zagadką nawet dla informatyków, dlatego należy się zabezpieczyć.

Kolejna moja propozycja to umieszczenie przez przedsiębiorcę na jego stronie internetowej lub konkretnym urządzeniu jak np. automat odpowiedniego oświadczenia o zakresie pełnomocnictwa Takie rozwiązanie powinno być obligatoryjne dla wszystkich, którzy posługują się systemem SI. Opis zakresu pełnomocnictwa powinien pojawiać się. podczas zawierania danej transakcji, na wzór obecnego wymogu informowania konsumenta o treści regulaminu sklep internetowego. Sam zakres pełnomocnictwa powinien być przedstawiony w formie języka naturalnego, a nie kodu źródłowego.

Z drugiej jednak strony należy zastanowić się nad tym, czy takie działanie nie przyniesie skutków negatywnych dla konsumentów. Sytuacja będzie zbliżona do tzw. ogólnych warunków umowy czy licencji, które obecnie często pojawiają się przy okazji transakcji internetowych czy instalacji programów komputerowych. Takie dokumenty są zwykle napisane językiem skomplikowanym, ponadto liczą kilkadziesiąt stron. Obciążanie konsumenta obowiązkiem przeczytania tak dużej ilości materiału byłoby przerzucaniem rzeczywistej odpowiedzialności z przedsiębiorcy na konsumenta. Takie działanie stałoby w sprzeczności z ogólną zasadą ochrony konsumenta jako słabszej strony. Niemniej jednak pozostawienie całego ryzyka po stronie przedsiębiorcy

wydaje się być niesprawiedliwe. Dochodzę bowiem do wniosku, że co prawda przedsiębiorcy korzystający z SI robią to w celu maksymalizacji zysku i redukcji kosztu, ale jednak takie systemy mają wiele do zaoferowania także konsumentowi. Dzięki temu zakupy w Internecie czy załatwianie innych spraw staje się szybsze i łatwiejsze. Jest to więc wyraźna korzyść dla konsumenta. Powinien on w związku z tym, jako strona transakcji, również brać na siebie część obowiązków takich jak np. zapoznanie się z zakresem pełnomocnictwa SI. O ile więc tego typu komunikaty będą jasne i zrozumiałe, a przy tym nie będą zbyt rozbudowane (powiedzmy do 5 stron), to chyba można od konsumenta wymagać, że się z nimi zapozna. W końcu nikt nie zmusza go do zakupów na danej platformie. Warto też zwrócić uwagę, że obecnie sami akceptujemy szereg różnych tzw. ogólnych warunków umów czy warunków licencji. Większość osób tych postanowień nie czyta, a mimo to takie rozwiązanie jest akceptowane.

Ponadto oba powyżej przedstawione rozwiązania mogą być stosowane komplementarnie. Jeżeli sąd uzna, że dany komunikat skierowany do konsumenta był zbyt skomplikowany i niejasny to przedsiębiorca nadal może uchronić się przed skutkami w oparciu o kod umieszczony w repozytorium.

Cała powyższa dyskusja sprowadza się do bardzo prostego pytania: kogo należy obciążyć większym ryzykiem? Prawda jest taka, że tworząc różne regulacje problem ten bardzo często musi zostać rozstrzygnięty. Poszukiwany jest złoty środek, który nie będzie obciążeniem dla konsumentów i biznesu, ale równocześnie nie wystraszy przedsiębiorców i nie zablokuje stosowania takich algorytmów, których głównym celem jest ułatwianie życia ludziom. Podobne wątpliwości rozstrzygane były na gruncie regulacji wzorców umownych, spółek prawa handlowego czy kwestii ochrony danych osobowych. Wszystkie z tych rozwiązań mają swoje wady, ale w ich obecnym kształcie zapewniają sprawne uczestniczenie w obrocie.

Niestety propozycja umieszczania informacji o zakresie pełnomocnictwa nie będzie skuteczna w sytuacji, gdy po obu stronach umowy występuje system SI. W większości przypadków nie będzie on w stanie przeanalizować przedstawionego mu komunikatu i wyciągnąć z niego wniosków co do tego, czy SI znajdująca się po przeciwnej stronie nie przekracza zakresu pełnomocnictwa. W przypadku repozytorium kodu źródłowego nie jest to już problem, dlatego że kod nie jest ujawniony przed zawarciem umowy, w związku z tym ani człowiek ani SI nie mają czego analizować.

Oczywiście każdy przypadek należy badać ad casum i w zależności od konkretnej treści kodu źródłowego czy ujawnionego zakresu pełnomocnictwa

na stronie internetowej rozstrzygnięcia mogą być bardzo różne. Z całą pewnością praktyka posługiwania się SI w obrocie masowym przyniesie odpowiedzi na wiele pojawiających się wątpliwości. W związku z tym należy postulować wprowadzenie konkretnych rozwiązań prawnych. I tak prof. Chłopecki proponuje następujące obszary regulacji:[62]

- w przypadku stosowania samouczących się algorytmów uczestniczących w obrocie stosowałoby się do nich odpowiednio przepisy o pełnomocnictwie, a w konsekwencji,
- odpowiedzialny za uruchomienie i funkcjonowanie algorytmu (dysponent SI) ponosiłby odpowiedzialność za zawarcie i za realizację transakcji dokonanych z pomocą SI – czyli żeby był tymi kontraktami z mocy prawa związany,
- od powyższego mogłyby istnieć odstępstwa w przypadku, gdyby fakt zawarcia transakcji lub jej treść były wynikiem działania siły wyższej lub osoby nieuprawnionej ingerującej w działanie SI.

Z powyższymi propozycjami należy się zgodzić, uzupełniając je o przedstawione powyżej dwie możliwości uwolnienia się danego podmiotu od skutków przekroczenia przez SI zakresu pełnomocnictwa.

3. 3. Wady oświadczeń woli[63]

Na temat znaczenia wad oświadczeń woli w przypadku korzystania z algorytmów SI można byłoby napisać osobną pracę. Temat jest bowiem niezwykle obszerny. Regulacje te nie są bowiem w pełni dostosowane do sytuacji zawierania umów, gdzie przynajmniej po jednej stronie występuje SI. W związku z tym zastosować będzie można tylko część tych uregulowań.

Polskie prawo wyróżnia kilka postaci wad oświadczeń woli: brak świadomości lub swobody, pozorność, błąd, zniekształcenie oświadczenia woli przez posłańca, podstęp i groźba (art. 82 – 87) oraz wyzysk (art. 388). Jeżeli przy zawieraniu umowy będziemy mieli do czynienia z wadą oświadczenia, to sankcje prawne tej sytuacji mogą być dwojakie. Po pierwsze, umowa może być nieważna ex lege, natomiast w drugim przypadku wada będzie jedynie podstawą do uchylenia się od skutków prawnych złożonego oświadczenia woli. W tym drugim przypadku zastosowanie znajdzie art. 88 KC, który wymienia zamknięty katalog błędów dających podstawę do takiego działania, po drugie

62 A. Chłopecki *„Szkice…”*.
63 Szerz. zob. K. Kurosz *„Zawieranie umów…”* s. 73 i n.

określa co należy uczynić, aby od takiego oświadczenia się uchylić. Zgodnie z kodeksową regulacją uchylić można się od oświadczenia woli złożonego pod wpływem groźby, błędu (w tym podstępu) oraz w sytuacji zniekształcenia oświadczenia woli przez posłańca

Przed przystąpieniem do analizy poszczególnych regulacji należy zwrócić uwagę na jedną bardzo istotną kwestię. Otóż w przypadku wad oświadczeń woli ważnym elementem analizy stanu faktycznego jest odwołanie się do stanu świadomości uczestnika danej transakcji. W przypadku uznania SI za pełnomocnika pojawia się pewien problem. Klasycznie bowiem oświadczenie woli składa pełnomocnik we własnym imieniu, ale ze skutkiem dla swojego mocodawcy. Skoro zatem uznamy SI za pełnomocnika, to wady oświadczeń woli trzeba będzie analizować z perspektywy świadomości algorytmu, co jest niemożliwe. Rozwiązanie tego problemu w doktrynie i orzecznictwie istnieje od dłuższego czasu. Otóż w pewnych sytuacjach należy badać także wolę mocodawcy, aby ten nie wykorzystał nieświadomości czy też niewiedzy pełnomocnika do zamaskowania swoich złych intencji. Niezależnie od tego, czy zostanie przyjęte prezentowane powyżej stanowisko o przypisywaniu oświadczenia woli osobie posługującej się SI, czy też stanowisko o dopuszczalności analogicznego stosowania przepisów o pełnomocnictwie, konieczne będzie badanie stanu świadomości mocodawcy. W obu bowiem przypadkach decydujące znaczenie będzie miała jego wola i z jego perspektywy można oceniać, czy doszło do zrealizowania się której z przesłanek uzasadniających zastosowanie instytucji wad oświadczeń woli.

Stan wyłączający świadome albo swobodne podjęcie decyzji ujmowany jest w polskiej literaturze[64] i orzecznictwie[65] dosyć szeroko. Brak świadomości może być trwały lub przemijający i wynikać z jakiegokolwiek powodu. Dana osoba nie jest w stanie prawidłowo podjąć procesu decyzyjnego z powodu „niemożności zrozumienia własnych i cudzych zachowań"[66]. Z kolei brak swobody to sytuacja, w której jakaś okoliczność niejako zmusza nas do pewnego działania, nawet pomimo braku naszej woli. Dochodzi zatem do złożenia oświadczenia o określonej treści, które badane bez kontekstu sytuacji w jakiej

[64] Zob. P. Sobolewski [w:] red. K. Osajda „*Kodeks cywilny. Komentarz*", Warszawa 2020, komentarz do art. 82, Legalis; R. Strugała [w:] red. E. Gniewek „*Kodeks cywilny. Komentarz*", Warszawa 2019, komentarz do art. 82, nb 3, Legalis; M. Gutowski [w:] red. M. Gutowski „*Kodeks cywilny. Komentarz*", Warszawa 2018, Tom 1, wyd. 2, Legalis

[65] Zob. Postanowienie Sądu Najwyższego - Izba Cywilna z dnia 17 maja 2018 r. sygn. V CSK 643/17; Wyrok Sądu Najwyższego - Izba Cywilna z dnia 18 maja 2016 r. sygn. V CSK 578/15; Wyrok Sądu Najwyższego - Izba Cywilna z dnia 7 lutego 2006 r. sygn. IV CSK 7/05

[66] R. Strugała [w:] red. E. Gniewek „*Kodeks cywilny. Komentarz*", Warszawa 2019, komentarz do art. 82, nb 3, Legalis

znalazła się dana osoba będzie uznane za oświadczenie jej woli. Taka sytuacja jest wymuszona np. przez czynniki fizjologiczne. Należy odróżnić od tej sytuacji przymus fizyczny, które nie kwalifikuje się pod zakres powyższej regulacji i może być rozważany np. jako groźba. [67] Jeżeli w określonej sytuacji odbiorca oświadczenia przy dołożeniu należytej staranności jest w stanie zorientować się o istniejącym braku świadomości lub swobody to należy przyjąć, że w ogóle nie dochodzi do złożenia oświadczenia woli.[68]

W przypadku umów zawieranych z udziałem SI pojawia się problem dwojakiego rodzaju. Po pierwsze, jak w klasycznym obrocie elektronicznym, algorytm nie widzi kto znajduje się po drugiej stronie. Po drugie, algorytm może czasami celowo próbować czerpać korzyści z sytuacji, w której zauważy, że druga stronna czynności prawnej z jakiegoś powodu nie działa racjonalnie – może to być np. osoba uzależniona od gier czy narkotyków, która podejmuje nieracjonalne decyzje w celu zdobycia określonej rzeczy. Na ten moment jednak technologia SI nie jest wystarczająco rozwinięta aby z powodzeniem analizować zachowanie człowieka, będącego stroną transakcji, a w konsekwencji celowo np. zawyżać ceny. Systemy obecnie tworzone przez programistów mają do spełnienia inne cele, w związku z tym taki algorytm musiałby samemu rozwinąć takie umiejętności, czego jednak nie można wykluczyć. Problem polega jednak na tym jak dana SI miałaby się – przy jednostkowej transakcji – zorientować, że dana osoba działa nieracjonalnie. Gdyby tych transakcji było więcej albo SI miałaby dostęp do historii transakcji z innych baz danych to zagrożenie mogłoby być większe. Jeżeli rzeczywiście zaistnieje sytuacja braku świadomości lub swobody po stronie jednostki to dana czynność będzie nieważna. Udowodnienie takiej sytuacji leży jednak po stronie tego, kto na taką okoliczność się powołuje. Warto jednak odnotować tutaj pogląd z komentarza prof. Gniewka, powoływanego powyżej, zgodnie z którym nieco inaczej należy rozważać sytuację, w której dana osoba sama wprawia się w stan wyłączający świadome powzięcie decyzji np. jest pod wpływem alkoholu lub środków odurzających. W komentarzu tym słusznie twierdzi się, że „w stosunku do osoby, która w sposób zawiniony doprowadziła do wystąpienia u siebie stanu braku świadomości lub swobody, należy stosować per analogiam przepis art. 425 § 2 KC. Jeżeli druga strona czynności, dokładając należytej staranności, nie mogła zauważyć tego stanu, czynność powinna pozostać ważna, mimo jego zaistnienia, jeżeli został on spowodowany w sposób

[67] *Ibidem*, nb 5
[68] *Ibidem*, nb 2

zawiniony przez tego, kto się w nim znajduje".[69] W braku przyjęcia takiego założenia doprowadzimy do sytuacji kuriozalnej, w której np. osoby zajmujące się inwestowaniem w akcje sprzedawane przez SI będą celowo wprowadzać się w określony stan, aby w razie braku powodzenia inwestycji podnieść nieważność umowy. Dopuszczenie takiej sytuacji byłoby poważnym zagrożeniem dla bezpieczeństwa obrotu.

Z kolei gdy brak świadomości lub swobody wystąpi u mocodawcy, w naszym przypadku osoby posługującej się SI, również może dojść do nieważności umowy, jednak pod pewnym warunkiem.. Wyobraźmy sobie sytuację w której uruchomiony został algorytm SI, który może dokonywać kilkuset transakcji w ciągu sekundy. Następnie osoba nim się posługująca traci świadomość. Nawet szybka reakcja i wyłącznie algorytmu doprowadzi do sytuacji, w której kilkadziesiąt tysięcy transakcji będzie nieważnych (przykładowo na giełdzie). W tej sytuacji należy więc badać stan świadomości na moment uruchomienia algorytmu. Inne rozwiązanie będzie niezwykle groźne dla całego systemu prawnego.

W przypadku pozorności sytuacja jest łatwiejsza, gdyż sama SI nie dokona (raczej) czynności dla pozoru, niemniej jednak nie można tego wykluczyć, zwłaszcza w przypadku SI, która postanowi zmaksymalizować zyski poprzez czynności pozorne w celu zmniejszenia należności podatkowych. Czynność taka ma na celu ukrycie innej czynności, faktycznie będącej intencją obu stron. Konieczna jest tutaj zgoda drugiej strony transakcji. Zazwyczaj więc mamy do czynienia z człowiekiem, którego intencje można badać. Nie można natomiast wykluczyć, że taka sytuacja będzie miała także miejsce w przypadku transakcji zawieranej pomiędzy dwoma systemami SI. Samo jednak udowodnienie określonej intencji obu stron jest już trudne, natomiast w przypadku SI po obu stronach transakcji prawdopodobnie niemożliwe, gdyż algorytmy nie tłumaczą się (przynajmniej obecnie) ze swojego toku rozumowania i nie uzasadniają podejmowanych przez siebie decyzji. Co prawda każde porozumienie musi zostać w jakiś sposób uzewnętrznione, jednak samo udowodnienie, że dana czynność rzeczywiście doprowadziła do ukrycia innej czynności jeszcze nie uzasadnia wniosku, że strony działały w porozumieniu i z intencją dokonania czynności dla pozoru.

W przypadku błędu w pierwszej kolejności wskazać należy, że błąd taki musi być istotny, co zgodnie z brzmieniem art. 84 § 2 oznacza „błąd

[69] *Ibidem*, nb 2 za: R. Trzaskowski [w:] red. P. Machnikowski, *„Kodeks cywilny. Księga pierwsza"*, s. 138 i n.

uzasadniający przypuszczenie, że gdyby składający oświadczenie woli nie działał pod wpływem błędu i oceniał sprawę rozsądnie, nie złożyłby oświadczenia tej treści". Przy czynnościach odpłatnych, które są przedmiotem niniejszej analizy błąd musi zostać albo wywołany przez drugą stronę, albo musi jakoś w świadomości drugiej strony się pojawić na etapie decyzyjnym tzw. osoba ta o błędzie wiedziała albo błąd mogła z łatwością zauważyć. Przypadki wywołania błędu przez drugą stronę (która SI się nie posługuje) nie powinny być częste, ponieważ w zautomatyzowanym obrocie koniecznym jest korzystanie ze schematów, które mogą być przełożone z języka naturalnego na kod źródłowy i kod wynikowy. Takie schematy w większości przypadków uniemożliwiają wprowadzenie błędnych danych. Dla posługujących się SI będzie natomiast bardzo ważny mechanizm bezpieczeństwa w postaci przesłanki „mogła z łatwością błąd zauważyć". Co do zasady to konsument jest stroną słabszą. Jednak w sytuacji błędu algorytmu np. w postaci obejścia ustalonej ceny minimalnej role mogą się odwrócić. Dla przykładu można podać sytuację, która miała miejsce w kwietniu 2020 roku w sieci sklepów Biedronka[70]. Obowiązująca wtedy promocja miała w założeniu polegać na tym, że w przypadku nabycia przez klienta przynajmniej 20 produktów otrzymywał on 100 % rabat na trzy najtańsze produkty, a w konsekwencji były one dla niego darmowe. Z powodu jednak błędu systemu doszło do sytuacji, w której system zamiast udzielać rabatu na trzy najtańsze produkty zaczął udzielać rabatu na trzy najdroższe produkty. W ten sposób wiele osób otrzymało za darmo drogie sprzęty elektroniczne jak np. roboty kuchenne. Niestety informacja o tym co dokładnie spowodowało błąd systemu nie jest publiczna, niemniej jednak nie można wykluczyć, że taki błąd mógłby się zdarzyć przy korzystaniu z systemu SI, który został nieprawidłowo nauczony danej czynności lub skorzystał z niewłaściwej bazy danych, przez co wykonywane przez algorytm obliczenia były błędne. W takiej sytuacja sprzedawcy mogą powoływać się na instytucję błędu. Regulamin promocji dokładnie określał zasady rabatowania, a ponadto zarówno w mediach masowych jak i na plakatach sklepowych pojawiła się informacja o tym, że darmowe będą trzy najtańsze produkty. W związku z tym konsumenci z łatwością mogli zapoznać się z warunkami promocji. Nie ulega także wątpliwości, że był to błąd istotny, skoro całkowicie zmieniał sens całej promocji – przy zakupie 20 paczek gum do żucia i 3 mopów parowych

[70] S. Ogórek, „*Biedronka miała poważny błąd w... promocji. Klienci płacili 20 zł, dostawali towar za ponad 1000 zł*", https://finanse.wp.pl/biedronka-miala-powazny-blad-w-promocji-klienci-placili-20-zl-dostawali-towar-za-ponad-1000-zl-6504177773647489a, ostatni dostęp: 01.09.2021.

klienci płacili tylko za gumy. Mimo to, kiedy dowiedzieli się o błędzie systemu, postanowili ten błąd wykorzystać. Nie brak było osób, które do sklepu wracały kilka razy, promocja bowiem nie była ograniczona do jednych tylko zakupów. W takiej sytuacji zasadnym jest twierdzenie, że druga strona (konsument) wiedziała o błędzie, a już z całą pewnością, że mogła błąd z łatwością zauważyć. Gdyby zatem sprzedawcy byli w stanie odszukać wszystkich swoich klientów to wobec takich osób znajdzie zastosowanie możliwość uchylenia się od skutków prawnych oświadczeń woli. Wprowadzenie takiej instytucji przerzuca część ryzyka na konsumenta, natomiast jej istnienie należy ocenić jako słuszne. Nie można doprowadzić bowiem do sytuacji, w której będziemy czerpać zysk z naszego złego zachowania przejawiającego się w postaci naszej złej wiary lub niedochowania należytej staranności.[71].

Pojawia się jednak inny problem, mianowicie jak rozwiązać sytuację, gdy po obu stronach jest SI? To zależy. Badamy wtedy świadomość osoby posługującej się SI, a w modelu analogi z pełnomocnictwa wolę mocodawcy. Jeżeli algorytm został zaprogramowany po to, aby wyszukiwać błędy innych osób posługujących się SI to z całą pewnością należy dopuścić możliwość uchylenia się od skutków prawnych na podstawie błędu. Jeśli natomiast algorytm po prostu wykorzystał okazję bo z punktu widzenia biznesowego, czystej matematyki, zakup taki był opłacalny, to ryzyko musi ponieść osoba posługująca się wadliwym algorytmem.

Przykład sklepu Biedronka daje się zakwalifikować jako możliwy do rozwiązania przy zastosowaniu omawianego rodzaju wad oświadczeń woli, jednak sama realizacja przysługujących sklepowi uprawnień może być trudna, ponieważ ciężko będzie zlokalizować większość klientów. Warto jednak wskazać na inny przypadek, gdzie skorzystanie z prezentowanej instytucji nie będzie już możliwe. Miała ona miejsce na jesieni 2019 roku.[72] Otóż na Black Friday oficjalny dystrybutor telefonów OnePlus w Polsce sprzedawał smartfon za kwotę 2464,15 zł, podczas gdy jego cena regularna to 2899 zł. Obniżka wynosiła więc 15 %. Klienci, którzy dokonali zakupu zostali jednak mocno zaskoczeni przez dystrybutora, który przysłał im informację, zgodnie z którą spółka uchyla się od złożonego oświadczenia woli. Dlaczego? Otóż zdaniem sprzedawcy doszło do błędu systemu. Ciężko ocenić, czy mieliśmy do czynienia tutaj ze SI, ale nie jest to wykluczone. Być może system miał proponować ceny smartfonu

[71] Por. Z. Radwański [w:] red. Z. Radwański *„Prawo cywilne – część ogólna. System Prawa Prywatnego. Tom 2”,* Warszawa 2019, Legalis, Komentarz do art. 844, Nb 76 i n.

[72] Zob. https://www.telepolis.pl/wiadomosci/prawo-finanse-statystyki/black-friday-po-polsku-czyli-sklep-pomylil-sie-i-nie-chce-wyslac-kupionego-smartfonu (dostęp: 20.01.2020).

poniżej cen konkurencji. W sytuacji ich obniżki na Black Friday, zazwyczaj do ceny o niewielkim stopniu opłacalności dla sprzedawcy, system obniżył ceny jeszcze bardziej, aby nadal pozostać konkurencyjny. Taki zabieg mógł z kolei doprowadzić do ustalenia ceny nieopłacalnej dla sprzedawcy. Zdaniem dystrybutora 15% obniżka to błąd istotny. Co więcej „cena towaru wskazana na stronie sklepu internetowego w sposób jednoznaczny i niebudzący wątpliwości wskazywała na błąd i to na tyle oczywisty, że z łatwością mógł/a go Pan/Pani zauważyć porównując cenę z ofertami innych oficjalnych sprzedawców w Polsce, a nawet bez dalszego sprawdzania kierując się jedynie zasadami logiki i doświadczenia życiowego". Tłumaczenie to spotkało się z krytyką zwykłych użytkowników jak i prawników[73]. Ostatecznie telefony zostały wysłane do klientów po cenie z dnia zakupu. Oczywiście całkowicie zgadzam się z prezentowanym przez większość osób komentujących ten przypadek w mediach społecznościowych stanowiskiem, że nie mamy tutaj do czynienia z błędem dającym się łatwo zauważyć. Sama istotność może być już różnie rozstrzygana, natomiast w mojej ocenie nie jest to cena tak rażąco niska, żeby przyjąć, że błąd jest istotny. Natomiast nie ma możliwości przyznania w tej sytuacji racji dystrybutorowi, zdaniem którego błąd można było z łatwością zauważyć. Gdyby doszło do takiej sytuacji w jakimś innym okresie czasu to być może taka argumentacja nie byłaby pozbawiona sensu, jednak gdy dzieje się ona w okresie dni takich jak Black Friday, Cyber Monday, czy też stosowanym przez polskie sklepy rozwinięciu piątkowych promocji w postaci Black Weekend, ciężko zgodzić się z argumentacją dystrybutora. Większość osób w takim okresie oczekuje niskich cen smartfonów i innych elektronicznych gadżetów. Gdyby cena była obniżona o połowę, wtedy ocena byłaby inna. Natomiast w prezentowanym stanie faktycznym ciężko odmówić racji klientom, którzy niższą cenę telefonu powiązali z promocjami organizowanymi w Blach Friday, pomimo, że sytuacja dotyczyła głównie soboty będącej dniem następnym po piątku pełnym promocji. Ten jeden dzień różnicy nie zmienia mojego stanowiska, bo jak wyżej wspomniałem, polska praktyka doprowadziła do powszechnego wydłużenia tego typu promocji aż do poniedziałku następującego po tym weekendzie.

Powyższe przypadki dobrze ilustrują jak duże ryzyko może nieść za sobą korzystanie z algorytmów SI do ustalania cen sprzedaży, co obecnie dzieje się na masową skalę. Błąd jako jeden z typów instytucji wad oświadczeń woli jest dobrym zabezpieczeniem dla przedsiębiorców, jednak, jak w przypadku ze

[73] Zob. https://bezprawnik.pl/oneplus-allegro-black-friday/ (dostęp: 20.01.2020).

smartfonami, nie zawsze będzie gwarantować pełna ochronę, gdyż ogranicza go przesłanka istotności i łatwości w dostrzeżeniu błędu.

Podstęp i groźba wydają się być równie mało istotne dla omawianego problemu co kwestia pozorności. W obrocie masowym sytuacja zawierania umowy pod wpływem groźby nie będzie występować zbyt często, gdyż są to zazwyczaj transakcje charakteryzujące się mniejszą istotnością dla danej strony, zwłaszcza algorytmy różnych systemów bankowych w przypadku większych transakcji wymuszają weryfikację określonej osoby także przez pracowników, a nie same algorytmy. Mniejsza istotność transakcji jest z kolei czynnikiem, który obniża zainteresowanie stron trzecich wypływaniem na daną osobę za pomocą groźby, nie można jednak oczywiście tego wykluczyć. Sytuacja podstępu może być już bardziej powszechna, natomiast dochodzi tutaj to krzyżowania się z komentowanym wcześniej błędem. Korzystanie z instytucji groźby i podstępu przy zautomatyzowanym i elektronicznym jest problemem dowodowym, bowiem sama wada umowy nie przesądza jeszcze, że doszło do użycia groźby lub podstępu. Często więc trudności dowodowe sprawią, że łatwiej będzie oprzeć się na instytucji błędu, która odwołuje się do elementów obiektywnych np. możliwości łatwego zauważenia błędu. Niemniej jednak warto wskazać, że w przypadku zaistnienia którejś z wymienionych wad – groźby lub podstępu - nie ma żadnych dodatkowych wymogów do uchylenia się od skutków oświadczenia woli np. błąd wywołany podstępem nie musi być istotny. Co ważne, w przypadku groźby należy wskazać, że musi być ona poważna, co z kolei oznacza, że jest ona jednocześnie doniosła oraz realna.[74]

Niekiedy jeszcze w literaturze wskazuje się jako wadę oświadczenia woli wyzysk uregulowany w art. 388 KC. Instytucja wyzysku traci jednak na znaczeniu, a ponadto słusznie wskazuje prof. Radwański, że „wychodząc z normatywnej koncepcji wad oświadczenia woli, należy uznać, że wyzysk nie należy do klasy wad oświadczeń woli. Pogląd ten potwierdza analiza przesłanek zastosowania wspomnianego przepisu, jak również odmienna zupełnie sankcja przewidziana tam w razie zawarcia umowy w celu wyzyskania drugiej strony. Stanowisko takie dominuje w nauce polskiej".[75] Niemniej jednak warto wskazać, że instytucja wyzysku może znaleźć zastosowanie również do umów zawieranych w obrocie zautomatyzowanym i elektronicznym, natomiast gdy po obu stronach występuje SI to trudno może być o spełnienie przesłanek wynikających z przepisu tzn. wykorzystanie przymusowego położenia, niedołęstwa

[74] R. Strugała [w:] red. E. Gniewek *„Kodeks…"*, komentarz do art. 87, nb 3
[75] red. Z. Radwański *„Prawo cywilne…",* uwagi ogólne do rozdziału VIII, nb 3

czy niedoświadczenia drugiej strony, ponieważ zazwyczaj SI nie będzie podejmować decyzji nieracjonalnych, nawet jeśli takie decyzje podjąłby podmiot, który się nią posługuje. Samo ustalenie tych przesłanek będzie dokonywane w toku procesu sądowego i to od oceny sądu będzie zależeć zakwalifikowanie określonej sytuacji jako wyzysku. Możliwość żądania unieważnienia umowy następuje dopiero w sytuacji, w której nie jest możliwe doprowadzenie jej do stanu gwarantującego sprawiedliwe wyważenie interesów obu stron.

Podsumowując należy wskazać, że wady oświadczeń woli tracą na znaczeniu coraz bardziej w sytuacji obrotu opartego o algorytmy SI. Należy poszukiwać rozwiązań, które odpowiednią zabezpieczą interesy obu stron. Obecnie w przypadku konsumentów takie rozwiązanie daje nam art. 27 ustawy z dnia 30 maja 2014 roku o prawach konsumenta[76] przyznający tzw. konsumenckie prawo odstąpienia od umowy. Obrót oparty o SI opiera się na umowach zawartych na odległość, dlatego przepis ten można z powodzeniem stosować. Być może podobne regulacje będzie można wprowadzić także w przypadku obrotu profesjonalnego. Jak słusznie wskazuje się w literaturze[77] wprowadzenie takiego mechanizmu dla konsumentów wcale nie doprowadziło do spadku umów zawieranych przez Internet, a wręcz przeciwnie, konsumenci mając możliwość zwrotu towaru wadliwego bądź nieodpowiadającego ich oczekiwaniom dużo chętniej zawierają umowy przez Internet, gdyż nie boją się o utratę pieniędzy w razie nieudanego zakupu.

3. 4. Odpowiedzialność

Powyższe rozważania odpowiadają na pytanie, czy w przypadku transakcji, gdzie przynajmniej po jednej stronie występuje SI mamy do czynienia z oświadczeniem woli, a w konsekwencji czy dochodzi do zawarcia umowy. Udowodnienie faktu zawarcia umowy jest kluczowa dla rozważań o odpowiedzialności kontraktowej, a więc wynikającej z niewykonania lub nienależytego wykonania umowy. Gdyby bowiem nie dochodziło do powstania stosunku obligacyjnego pomiędzy stronami to nie byłoby możliwe rozważanie wykonania bądź niewykonania wynikających z takiego stosunku obowiązków. Podstawowe znaczenie ma tutaj regulacja art. 471 KC „Dłużnik obowiązany jest do naprawienia szkody wynikłej z niewykonania lub nienależytego wykonania zobowiązania, chyba że niewykonanie lub nienależyte wykonanie jest następstwem okoliczności, za które dłużnik odpowiedzialności nie

[76] Dz. U. 2014 poz. 827.
[77] Zob. K. Kurosz *„Zawieranie umów…”*, s. 96.

ponosi". W przypadku umów zawieranych z udziałem SI stroną takiej umowy, a w konsekwencji także zobowiązanym do jej wykonania, jest podmiot, który korzystał ze SI w celu zawarcia umowy. Tylko pomiędzy takim podmiotem a osobą dokonującą z nim transakcji może wystąpić więź kontraktowa. Należy więc kategorycznie odrzucić próby przypisania odpowiedzialności na podstawie tego przepisu twórcy SI, co oczywiście nie wyklucza w takiej sytuacji odpowiedzialności deliktowej lub odpowiedzialności kontraktowej z tytułu niewykonania lub nienależytego wykonania umowy między twórcą algorytmu a osobą, która będzie z niego korzystać np. w przypadku braku wywiązywania się z zawartego w umowie obowiązku bieżącej aktualizacji oprogramowania SI, ponadto może także wystąpić wada systemu, co z kolei będzie podstawą do realizacji uprawnień z rękojmi lub gwarancji.

Wskazać należy przede wszystkim na art. 472 KC, zgodnie z którym „Jeżeli ze szczególnego przepisu ustawy albo z czynności prawnej nie wynika nic innego, dłużnik odpowiedzialny jest za niezachowanie należytej staranności". Takie uregulowanie kodeksowe odsyła nas zatem do przepisów części ogólnej zobowiązań, gdzie wskazano sposób rozumienia należytej staranności w art. 355. Należyta staranność w doktrynie opisywana jest jako „sposób postępowania dłużnika odpowiadający wymaganiom zawartym w obiektywnym wzorcu postępowania, który jest tworzony na tle danego stosunku zobowiązaniowego".[78] Zdaniem prof. Machnikowskiego „odpowiedzialność dłużnika uzależniona jest od jego winy, polegającej na negatywnej ocenie jego postępowania, wyrażającej się w możliwości postawienia mu zarzutu, że mogąc w określonych okolicznościach postąpić w sposób zgodny z treścią zobowiązania i wymogami należytej staranności, postąpił on inaczej (podjął niewłaściwą decyzję)".[79] Uregulowanie tego wzorca w sposób obiektywny, a więc dający możliwość porównania konkretnego zachowania z pewnym ustalonym wzorcem prawidłowego zachowania, jest oczywiście w przypadku SI niezwykle korzystne. Takie rozwiązanie uniemożliwia uwolnienie się od odpowiedzialności dłużnika poprzez jego subiektywną ocenę zaistniałem sytuacji. Przy takim rozwiązaniu nie jest możliwe powoływanie się na nieznajomość algorytmu lub brak wiedzy o określonym rozwiązaniu technicznym, jeżeli w takiej samej sytuacji od innej osoby, dokładającej należytej staranności np. przy prowadzeniu określonego biznesu oczekiwalibyśmy, że zapozna się ona z instrukcją obsługi, zatrudni wykwalifikowany personel bądź podejmie inne, adekwatne działania. Nie jest to zatem

[78] W. Borysiak [w:] red. K. Osajda *„Kodeks cywilny. Komentarz"* wyd. 24, Warszawa 2020, komentarz do art. 355, pkt. 3, Legalis

[79] *Ibidem*

odpowiedzialność absolutna, ale uwolnić można się od niej tylko wtedy, kiedy od wzorcowego podmiotu w danej sytuacji również nie można byłoby wymagać więcej, niż rzeczywiście zostało uczynione. Co istotne, jak słusznie wskazuje się w doktrynie, umiejscowienie przepisu o należytej staranności w przepisach ogólnych części zobowiązań pozwala na stosowanie go także do analizy odpowiedzialności deliktowej opartej o zasadę winy. W przywołanym powyżej komentarzu pod redakcja K. Osajdy słusznie zwraca się uwagę, że pojęcie należytej staranności nie stanowi niezbędnego elementu zobowiązania: „nie można przyjmować, że art. 355 KC określa treść zobowiązania na tej samej zasadzie, jak czyni to art. 354 § 1 KC. Niewątpliwe jest, że prawa wierzyciela i obowiązki dłużnika składające się na treść zobowiązania mogą być dochodzone na drodze sądowej. Wierzyciel może więc żądać od dłużnika wykonania zobowiązania zgodnie z jego treścią (co wynika wprost z art. 354 § 1 KC) lub żądać wykonania zobowiązania np. przez osobiste świadczenie dłużnika w sytuacjach określonych w art. 356 § 1 KC. Nie może jednak żądać od dłużnika działania z należytą starannością (określoną bądź w stosunkach danego rodzaju, bądź umownie), jeżeli dłużnik spełnia swoje świadczenie zgodnie z treścią zobowiązania. Wierzyciel nie może też żądać od dłużnika odszkodowania (np. kary umownej zastrzeżonej na wypadek nienależytego wykonania zobowiązania) w sytuacji, gdy dłużnik wykonał zobowiązanie w sposób należyty, choć działał w sposób niedbały podczas jego wykonywania (np. dostarczył wierzycielowi w terminie zamówiony towar, mimo że dostarczając go, działał niestarannie, kilkukrotnie go gubiąc i jedynie przy pomocy osób trzecich go odnajdując)”[80]. Konsekwencją tego jest to, że wierzyciel nie zawsze może żądać od dłużnika działania w określony sposób. O ile więc w umowie między stronami nie został ustalony określony sposób działania jako element treści zobowiązania dłużnika to dłużnikowi pozostaje wybór sposobu działania w celu doprowadzenia do uzgodnionego świadczenia. Wówczas, w razie spełnienia świadczenia w sposób należyty pomimo działania niestarannego, wierzyciel nie może domagać się odszkodowania od dłużnika. Kluczowe bowiem jest to, czy ostatecznie świadczenie zostało należycie spełnione, a nie jaka przebiegał proces dążenia do wykonania zobowiązania. Oczywiście w wielu przypadkach ten proces będzie bardzo istotny i będzie wpływać na ostateczną formę przedmiotu zobowiązania np. pomimo zewnętrznie prawidłowo wyglądającego domu może on mieć usterki wewnętrzne, niewidoczne. Jednak jeśli przedmiotem zobowiązania jest dostarczenie

[80] *Ibidem*, pkt 18

przesyłki do odbiorcy to bez znaczenia będzie fakt, że w toku podróży przesyłka została kilka razy zgubiona lub trafiła do niewłaściwego oddziału, co wydłużyło czas realizacji, o ile nie przekroczono terminu dostarczenia przesyłki, a ona sama nie była w żaden sposób uszkodzona czy niekompletna.[81] Powyższe rozważania należy uzupełnić o uwagę, że nie każde niewykonanie określonego przedmiotu umowy w umowach rezultatu np. dzieła będzie prowadziło do uznania odpowiedzialności za niewykonanie zobowiązania. W takiej sytuacji należy badać staranne działanie dłużnika w świetle tego, czy gdyby zachował się w sposób należyty to doszłoby do wykonania zobowiązania. Powyższe potwierdza także doktrynie, gdzie wskazuje się, że „przyczyny ewentualnego nieosiągnięcia tego rezultatu oceniane będą z uwzględnieniem art. 355 § 1 KC, który wskazuje należytą staranność dłużnika jako miarę prawidłowego wykonania zobowiązania. W płaszczyźnie odpowiedzialności zatem podział rodzajów zobowiązań staje się, na gruncie prawa polskiego, trudny do uzasadnienia, ponieważ myliłby on miarę staranności z przedmiotem świadczenia. Nie wydaje się zasadne budowanie odrębnych standardów staranności dla tzw. zobowiązań rezultatu i starannego działania. W wyr. SN z 5.2.2002 r. (II CKN 894/99, OSG 2004, Nr 6, poz. 82) słusznie wskazano, że przyjmujący zamówienie zobowiązany jest do naprawienia szkody spowodowanej niezachowaniem należytej staranności (art. 471 w zw. z art. 472 KC)."[82] Prezentowane jest jednak również stanowisko przeciwne, zgodnie z którym dłużnik zwolni się od odpowiedzialności tylko wtedy, gdy wystąpią okoliczności od niego niezależne, które uniemożliwiły mu wykonanie dzieła – „Przyjmujący zamówienie nie może uwolnić się od odpowiedzialności kontraktowej, jeżeli dołożył należytej staranności w swych usiłowaniach zmierzających do wykonania dzieła, lecz końcowego rezultatu nie osiągnął."[83] Ponadto należy wskazać, że zwolnienie od odpowiedzialności może wynikać z przepisów szczególnych np. art. 638 KC w odniesieniu do umowy o dzieło, zgodnie z którym przyjmujący zamówienie nie ponosi odpowiedzialności za wady dzieła, jeżeli wada wynika z wady materiału użytego do wykonania dzieła, który to materiał dostarczony został przez zamawiającego.

Przedstawione powyżej rozważanie nie mają zastosowania do zobowiązań starannego działania, których istotą jest należyta staranność przy wykonywaniu zobowiązania, niezależnie od tego, czy określony na wstępie cel zostanie

81 *Ibidem.*

82 M. Gutowski [w:] red. M. Gutowski, *„Kodeks Cywilny. Komentarz."*, Warszawa 2019, t. III, art. 627, Nb 32

83 red. K. Osajda *„Kodeks cywilny*…", komentarz do art. 627, pkt. 39.

osiągnięty np. prawnik korzystający z systemu SI określa szanse na wygrane w rozprawie sądowej i na tej podstawie decyduje się na wszczęcie procesu. Na podstawie przygotowanej przez SI analizy oraz własnych umiejętności prowadzi argumentację w toku procesu. Ostatecznie jednak sąd oddala pozew. W takiej sytuacji ocenie będzie poddana należyta staranność przy wykonywaniu zobowiązania, a więc przede wszystkim to, czy system z którego korzystał prawnik był przeznaczony do danej kategorii spraw, czy był na tyle sprawdzony, aby można było opierać się na jego sugestiach oraz czy sam proces został przez prawnika poprowadzony w sposób prawidłowy np. przegrana nie wynika z tego, że nie zostały powołane żadne dowody.

W zakresie wzorców należytej staranności wyróżnia się zwykłą niestaranność lub rażące niedbalstwo.[84] Chociaż granica ta, na co zwraca się uwagę w doktrynie, jest płynna, to można wyróżnić chociaż przypadki skrajne. I tak z rażącym niedbalstwem będziemy mieli do czynienia w sytuacji, w której dana osoba działa w sposób całkowicie niewłaściwy, także umyślny. Podobnie będzie, gdy dłużnikowi brak podstawowej wiedzy i umiejętności do wykonania zobowiązania, bądź też brakuje mu odpowiedniego sprzętu czy personelu. W przypadku SI przykładem rażącego niedbalstwa będzie w mojej ocenie sytuacja, w której dziennikarz zobowiązany do przygotowywania tekstów dla swojego pracodawcy np. gazety korzysta z oprogramowania SI do przygotowywania artykułów prasowych opartego o algorytm nadzorowanego uczenia maszynowego, ale nie zatrudnia osoby odpowiedzialnej za nadzór nad tym algorytmem. Prowadzi to do sytuacji, w której algorytm zasysa do bazy danych mnóstwo informacji nieprawdziwych, treści nieodpowiednich itp., co prowadzi do produkcji zupełnie nienadających się do publikacji materiałów prasowych. O ile dziennikarz następnie nie sprawdzi wygenerowanego tekstu przed publikacją będzie można w mojej ocenie przypisać mu rażące niedbalstwo.

Sam wzorzec odpowiedzialności jest obiektywny i zewnętrzny.[85] Konstruowany jest on w taki sam sposób dla wszystkich podmiotów, a cechy indywidualne nie są uwzględniane. Oznacza to, że dla przedsiębiorstw budowlanych wzorcem staranności będzie typowa firma wykonująca określone zlecenia. Dla osoby wypuszczającej artykuły prasowe w oparciu o SI wzorcem będzie inna, typowa firma prowadząca tego typu usługi, niezależnie od tego, czy artykuł pisane są przez człowieka czy maszynę. W przypadku niewłaściwego wykonania zobowiązania kluczowe będzie to, czy przygotowanie takie tekstu odbyło się

[84] W. Borysiak [w:] red. K. Osajda *„Kodeks cywilny…”,* komentarz do art. 355, pkt. 3, Legalis, pkt. 23, szerz. zob. także komentarz do art. 427.
[85] *Ibidem*, pkt. 25.

w sposób właściwy. Jeżeli w umowie z gazetą wyraźnie wskazano, że zobowiązanie może być wykonane przy użyciu algorytmu SI to w razie niewłaściwego wykonania zobowiązania koniecznym będzie przeanalizowanie, czy dany dziennikarz dołożył należytej staranności w całym procesie tworzenia artykułu tzn. czy korzystał z oprogramowania z pewnego źródła oraz czy zweryfikował go przed publikacją. Jeżeli natomiast z umowy nie wynikało w jaki sposób ma powstać artykuł to dziennikarz decydując się na korzystanie ze SI bierze na siebie ciężar ryzyka np. wystąpienia awarii w takim programie. Powinien zatem tak zaplanować swoja pracę, aby w razie problemów z programem był w stanie przygotować artykuł w tradycyjny sposób.. To czy dłużnik zdaje sobie sprawę z potencjalnych ryzyk jest tutaj bez znaczenia. Podjęcie działalności bez wymaganej wiedzy, sprzętu, zaplecza technicznego i kadrowego nie ma znaczenia, jeżeli dzieło zostanie dostarczone zgodnie z wymaganiami wynikającymi z umowy. Natomiast w przypadku, gdy zobowiązanie nie zostanie wykonane prawidłowo bądź nie zostanie w ogóle wykonane, wszystkie te czynniki będą poddane ocenie, tak aby stwierdzić, czy gdyby dochowano należytej staranności to udałoby się wykonać zobowiązanie. Subiektywna ocena dłużnika, że dane środki są wystarczające, nie będzie wpływała na ocenę, czy tej staranności dochowano. Inaczej przedstawia się sytuacji przy umowie starannego działania, gdzie oceniane będzie działanie dłużnika, a ocena końcowego rezultatu będzie mieć charakter wtórny. Z istoty takiego zobowiązania wynika, że dłużnik powinien działać w sposób należyty. Warto wskazać także na wyrok Sądu Najwyższego z dnia 27 stycznia 1972 roku, zgodnie z którym „nie można wykluczać odpowiedzialności dłużnika tym bardziej, jeśli już w chwili zawarcia umowy wie on o tym, że nie będzie mógł wykonać w ogóle lub w sposób należyty zobowiązania, które w umowie podejmuje".[86]

Za trafny należy uznać jednak wniosek, zgodnie z którym w razie wiedzy o takich okolicznościach po stronie wierzyciela, już w chwili powstania zobowiązania, odpowiedzialność dłużnika należy oceniać w świetle art. 362 KC mówiącego o przyczynieniu się do powstania szkody. Nie sposób bowiem bronić w takiej sytuacji wierzyciela, który zawiera umowę jedynie w celu dochodzenia odszkodowania za niewykonanie zobowiązania. Taka sytuacja prowadziłaby bowiem do rozejścia się woli rzeczywistej wierzyciela z wolą ukrytą. Jeżeli zatem wierzyciel przy zawieraniu umowy ma wiedzę np. techniczną, że dany algorytm SI, którym chce się posłużyć dłużnik, nie będzie nadawał się

[86] Sygn. akt I CR 458/71, Legalis za W. Borysiak [w:] red. K. Osajda *„Kodeks…”*, pkt. 28

do należytego wykonania zobowiązania, a mimo to decyduje się na zawarcie umowy, powinien zostać uznany za osobę przyczyniającą się do nienależytego wykonania zobowiązania. W przeciwnym razie wierzyciel mógłby zawrzeć określoną umowę nie po to, aby doszło do jej wykonania, ale po to, aby w wyniku jej niewykonania naliczyć wysokie kary umowne.

Odwoływanie się do określonych cech podmiotu mieści się w granicach teorii wzorców typu zawodowego. [87] Prowadzi to do stworzenia się pewnych określonych grup, dla których wzorzec staranności w podobnej sytuacji może być zupełnie inny. Sporne jest natomiast to, czy wartość przedmiotu świadczenia ma wpływ na wymagany miernik staranności. W przywoływanym komentarzu dr Borysiak staje na stanowisku, że wartość przedmiotu zobowiązania nie ma znaczenia dla wymaganej staranności dłużnika. W opozycji do tego poglądu wskazuje na wyrok Sądu Najwyższego z dnia 7 listopada 1990 roku[88] gdzie stwierdzono, że „przechowywanie rzeczy w normalnie zamkniętym mieszkaniu jest w zasadzie wystarczającym sposobem jej zabezpieczenia przed kradzieżą. Ze względu na nagminność włamań do mieszkań nie można jednak tego w pełni odnieść do rzeczy cudzych, o dużej wartości. O należytej staranności przechowawcy takich rzeczy można mianowicie mówić tylko wówczas, gdy mieszkanie jest odpowiednio zabezpieczone bądź przez stałą obecność osób zamieszkałych, bądź przez zastosowanie chroniących przed włamaniem środków technicznych". W mojej ocenie stanowisko Sądu Najwyższego jest jednak słuszne. Należyta staranność dłużnika opiera się o ocenę tego, jakie należy podjąć działania, aby prawidłowo zrealizować przedmiot umowy. Nie bez powodu duże sumy pieniędzy deponowane są w np. bankach szwajcarskich, które słyną z daleko idących środków ostrożności, chociaż zdeponowanie dużej kwoty pieniędzy w polskich bankach także będzie uznane za wystarczające, gdyż przepisy regulujące ich działalność zapewniają realizację wysokiego stopnia ochrony pieniędzy. Podobnie w transakcjach płatniczych kartą zbliżeniową banki wprowadziły, w ramach obowiązków wynikających z implementowanych przepisów prawa unijnego, limity wysokości transakcji (np. 50 zł), po których przekroczeniu oprócz przyłożenia karty do czytnika konieczne jest podanie numeru PIN. Jest to odpowiedź na liczne kradzieże z wykorzystaniem modemów do przekazu sygnału z karty do terminala oddalonego o pewną odległość. Odejście od mierzenia adekwatności zastosowanych rozwiązań przy ustalaniu dołożenia należytej staranności wydaje się

87 *Ibidem*, pkt. 34.
88 Sygn. akt I CR 605/90, Legalis.

być błędne, zwłaszcza biorąc pod uwagę, że sam dr Borysiak w swoim fragmencie komentarza wyróżnia przedmiot świadczenia jako jeden z elementów determinujących rodzaj ustalonego miernika staranności. Zatem jeżeli z danej umowy wynika, że powinniśmy dbać o daną rzecz i w tym celu decydujemy się na podjęcie środków mających go zabezpieczyć np. przed kradzieżą to, w zależności od wartości tej rzeczy, istotne będzie jaki sposób zabezpieczenia wybraliśmy, a nie sam fakt, że podjęliśmy kroki w celu jej zabezpieczenia. Jeśli zatem przedmiot zabezpieczymy nieadekwatnie do jego wartości to nie można mówić o dołożeniu należytej staranności. Jeżeli zatem dłużnik mający zapewnić bezpieczeństwo systemów komputerowych dużej organizacji, przy użyciu inteligentnego oprogramowania cyberbezpieczeństwa, wyposażonego w SI, zdecyduje się na wybór oprogramowania o niewystarczających funkcjach zapewnienia bezpieczeństwa, to dojdzie do niezachowania należytej staranności. Nie ma przy tym znaczenia, że w innej, mniej wymagającej organizacji ten program jest wystarczający, bo w tym przypadku mamy innego klienta, który wymaga innego poziomu bezpieczeństwa, a w konsekwencji mamy inny przedmiot umowy, pomimo, że nadal chodzi o oprogramowanie ochronne.

Kolejne sporne zagadnienie dotyczy odpłatności i nieodpłatności umowy. Na poglądy, zgodnie z którym nie ma to wpływu na stopień należytej staranności, wskazuje dr Borysiak – są to prof. Safjan[89], prof. Gutowski[90] i prof. Wiśniewski[91]. Z kolei dr Borysiak opowiada się za poglądem przeciwnym, prezentowanym także przez prof. Machnikowskiego, zgodnie z którym „w określonych sytuacjach może być uzasadnione obniżenie wymagań staranności w zobowiązaniach nieodpłatnych". Jednak jak wskazuje dr Borysiak „musi być to powiązane z treścią samego zobowiązania. Zasadą jest bowiem to, że nieodpłatność per se nie wpływa na takie obniżenie wymagań. Stąd też ciężar dowodu w ewentualnym procesie, że takie obniżenie miało miejsce, spoczywać będzie na dłużniku". W mojej ocenie należy przyjąć, iż nieodpłatność wpływa na obniżenie wymaganego stopnia staranności. Koresponduje to wprost ze wcześniejszym stanowiskiem zgodnie z którym, przedmiot zobowiązania ma wpływ na wzorzec staranności.

Ogólnie wymagana staranność nie oznacza staranności na najwyższym poziomie, ale nie dopuszcza też do przyjęcia jej na poziomie najniższym.

[89] M. Safjan [w:] red. K. Pietrzykowski, *„Kodeks Cywilny. Komentarz"*, Warszawa 2015, t. I, art. 355, Nb 10, Legalis

[90] M. Gutowski [w:] red. M. Gutowski, *„Kodeks Cywilny. Komentarz."*, Warszawa 2019, t. II, art. 472, Nb 5–6

[91] T. Wiśniewski [w:] red. J. Gudowski, *„Kodeks cywilny. Komentarz."*, Warszawa 2013, Ks. III, cz. 1, art. 355, pkt 3

Kształtuje ją więc niejako pośrodku obu tych skrajności. Staranność taką można określić jako przeciętną.[92] Oczywiście w przypadku profesjonalisty użycie sformułowania „przeciętna" może wydawać się nieadekwatne. Jednak art. 355 w § 2 stopień staranności zostaje zmodyfikowany w ten sposób, że „ należytą staranność dłużnika w zakresie prowadzonej przez niego działalności gospodarczej określa się przy uwzględnieniu zawodowego charakteru tej działalności". Jest to więc odwołanie do wspomnianej wcześniej kategoryzacji podmiotów z uwagi na prowadzoną przez nich działalność. Warto podkreślić, że jak słusznie wskazał Sąd Najwyższy w wyroku z dnia 25 września 2002 roku „należyta staranność dłużnika w zakresie prowadzonej przez niego działalności gospodarczej, którą określa się przy uwzględnieniu zawodowego charakteru tej działalności, nie oznacza staranności wyjątkowej, lecz dostosowanej do działającej osoby, przedmiotu, jakiego działanie dotyczy, oraz okoliczności w jakich działanie to następuje".[93] Jeżeli chodzi o zakres zastosowania wskazanego przepisu to wskazuje się, że nie dotyczy on tylko przedsiębiorców w rozumieniu art. 43^1 KC, ale także osób faktycznie i stale wykonujących działalność gospodarczą, nawet jeśli nie posiadają one statusu przedsiębiorcy.[94] Regulacja ta ma na celu dostosowanie przepisów do realiów działalności człowieka. Jeżeli bowiem decydujemy się na powierzenie określonych zadań podmiotom, które deklarują, że zawodowo zajmują się jakimś, zwykle trudnym zagadnieniem, to oczekujemy od nich odpowiedniej wiedzy w danym zakresie, umiejętności, profesjonalnego i rzetelnego podejścia do określonego zadania. Nie ma przy tym znaczenia świadomość wierzyciela co do tego, czy dany podmiot zawodowo zajmuje się określoną działalnością, jak również bez znaczenia są własne odczucia dłużnika, któremu może się wydawać, że nie dochował należytej staranności. Za każdym razem ocena progu staranności będzie badana obiektywnie i przy uwzględnieniu modelowego przykładu adekwatnego do prowadzonej działalności. W przypadku podmiotu posługującego się SI należałoby postawić mu wymagania takie jak znajomość technologii z jakiej korzysta, znajomość przepisów prawa np. ochrony konkurencji i konsumentów, podjęcie odpowiednich działań zapewniających stały nadzór wykwalifikowanych pracowników jak programiści, odpowiednie uregulowania z dostawcą oprogramowania SI, zapewnienie procedur zgłaszania awarii systemu, zabezpieczenia przed atakami hackerskimi itp.

92 W. Borysiak [w:] K. Osajda, *„Kodeks…"*, pkt. 54
93 *Ibidem* pkt. 71 za: sygn. akt I CKN 971/00.
94 *Ibidem*.

Po ustaleniu wzorca staranności należy jeszcze odnieść się do dwóch kwestii. Pierwsza z nich to ustalenie podstawy odpowiedzialności podmiotu posługującego się SI. Można tutaj wyróżnić dwie możliwe sytuacje. Pierwsza to taka, gdzie SI zawiera umowę jako przedstawiciel lub przekaźnik woli osoby, która się nią posługuje, a druga to sytuacja, w której umowę zawiera dana osoba (fizyczna lub prawna) i w toku swojej działalności korzysta ze SI. Pierwszy przypadek dotyczy zatem ustalenia strony stosunku prawnego umowy zawartej z udziałem SI, gdzie wykonywanie samego zobowiązania może nie być powiązane z użyciem algorytmu, natomiast drugi przypadek dotyczy dłużnika, który po zawarciu umowy bez wykorzystania SI decyduję się na realizację swojego zobowiązania przy użyciu systemu SI. W pierwszym przypadku rzecz jasna odpowiedzialność przypisujemy nie SI, która nie jest ani stroną umowy ani dłużnikiem, a osobie, która faktycznie znajduje się po drugiej stronie określonego stosunku prawnego i w konsekwencji jest zobligowana do tego, aby wykonać powstałe zobowiązanie w sposób należyty, niezależnie od tego, czy w toku jego realizacji będzie korzystać ze SI.

Natomiast w drugim przypadku można zastanawiać się, czy jeżeli SI nie będzie posiadać pewnego stopnia autonomii decyzyjnej tzn. będzie na tym środkowym lub najwyższym stopniu przedstawionego przeze mnie podziału, zbliżając się tym samym do tego, co kryje się pod określenie silnej SI, a więc przestaje być jedynie narzędziem rękach realizującego zlecenie, to czy nie znajdzie w takiej sytuacji zastosowania w formie analogicznego stosowania art. 474 KC, zgodnie z którym „dłużnik odpowiedzialny jest jak za własne działanie lub zaniechanie za działania i zaniechania osób, z których pomocą zobowiązanie wykonywa, jak również osób, którym wykonanie zobowiązania powierza. Przepis powyższy stosuje się także w wypadku, gdy zobowiązanie wykonywa przedstawiciel ustawowy dłużnika". W takiej sytuacji będzie konieczne zbadanie, czy osoba powierzająca wykonanie czynności dołożyła należytej, wymaganej staranności w wyborze podmiotu, któremu zleca dane działanie. W przypadku SI jest to konstrukcja nieco sztuczna, przynajmniej dopóki nasza SI jest algorytmem dłużnika, a nie usługa świadczoną w chmurze lub w inny sposób dostarczaną z zewnątrz. W takiej sytuacji badanie należytej staranności będzie przebiegało na zasadzie badania odpowiedniego zabezpieczenia własnego oprogramowania i wszystkich innych elementów, o których pisałem powyżej. Użycie w przepisie sformułowania „osoba" powinno powodować, że przepis będzie stosowany per analogiam, przynajmniej do czasu, gdy SI nie zostanie wyposażona w osobowość prawną. Z kolei w sytuacji, gdy SI jest usługą dostarczaną zewnętrznie i sami nie mamy wpływu np. na zakres

jej uczenia się, badanie dochowania należytej staranności będzie przebiegać jak badanie każdego zewnętrznego podmiotu dostarczającego dane usługi np. podwykonawców na budowie czy firmy kurierskiej przy przesyłkach.

Kluczowa jest jednak analiza wskazanego w art. 361 KC adekwatnego związku przyczynowego, który zgodnie rozdziela się w doktrynie[95] na test warunku sine qua non i test normalności następstw (poza zaniechaniem). Również i ten przepis z uwagi na jego usytuowanie w kodeksie należy odczytywać jako właściwy do zastosowania przy analizie odpowiedzialności deliktowej, stąd w rozdziale poświęconym odpowiedzialności deliktowej będę jedynie odwoływać się do uwag poczynionych w tym miejscu. Test warunku koniecznego (conditio sine qua non) „opiera się na teorii równowartości przyczyn (ekwiwalencji przyczyn) J.S. Milla, według której przyczyną zdarzenia jest ogół równoważnych względem siebie warunków (okoliczności), bez których nie wystąpiłby badany skutek".[96] Przy stosowaniu tego testu należy zadać sobie pytanie: Czy w braku zaistnienia zdarzenia X doszłoby do powstania skutku Y? Warto wskazać, że test będzie spełniony także wtedy, gdy pewne zdarzenie co prawda nie wywołało skutku, ale powiększyło szkodę wynikająca z innego zdarzenia.[97] Co ważne, ciąg zdarzeń w łańcuchu nie stoi na przeszkodzie przypisania zdarzeniu początkowemu skutku w postaci zaistnienia zdarzenia końcowego np. X wywołało Y, Y wywołało Z, wniosek z tego, że X wywołało Z. Przykład ten wiąże się ściśle z drugim kryterium – testem normalności następstw. Test ten polega na sprawdzeniu, czy przebieg zdarzeń był typowy, normalny i nie został przerwany przez jakieś nadzwyczajne wydarzenie. W doktrynie wskazuje się, że „za normalne przyczyny powstania szkody uznaje się te przyczyny, które każdorazowo zwiększają możliwość(prawdopodobieństwo) wystąpienia badanego skutku".[98] Z kolei Sąd Najwyższy w wyroku z dnia 11 września 2003 roku stwierdził, że jest to „skutek, który zazwyczaj i w zwykłym porządku rzeczy jest konsekwencją tego zdarzenia, czyli zdarzenie to ogólnie sprzyja jego wystąpieniu".[99] Bardzo istotnym jest to, że jest to kryterium całkowicie obiektywne. W szczególności bez znaczenia jest to, czy dany podmiot w chwili dokonywania czynności przewidywał dany ciąg

[95] Zob. P. Sobolewski [w:] red. K. Osajda „*Kodeks cywilny. Komentarz*" wyd. 24, Warszawa 2020, komentarz do art. 361; K. Zagrobelny [w:] red. E. Gniewek „*Kodeks cywilny. Komentarz*" wyd. 9, Warszawa 2019, komentarz do art. 361.

[96] P. Sobolewski [w:] red. K. Osajda „*Kodeks Cywilny. Komentarz.*" wyd. 24, Warszawa 2020, komentarz do art. 361, pkt. 8.

[97] *Ibidem*, pkt. 9.

[98] *Ibidem*, pkt. 12.

[99] Sygn. akt III CKN 473/01, Legalis

zdarzeń, i zdawał sobie sprawę z możliwości zaistnienia poszczególnych elementów jego elementów. Test ten jest wykonywany ex post, a jego podstawą są wszelkie okoliczności danej sprawy.[100] Co ważne, normalność następstw nie oznacza ich typowości, na co zwraca uwagę Sąd Najwyższy w wyroku z dnia 7 marca 2013 roku (sygn. akt II CSK 364/12, Legalis) mówiąc, że „nietypowość czy sporadyczność następstw nie przekreśla adekwatności związku przyczynowego, normalność następstw nie jest bowiem pochodną ich typowości, lecz raczej kwestią zdatności przyczyny do wywołania określonego rodzaju skutków."[101] Ponadto wskazuje się także, że brak normalności następstw nie zwalnia danej osoby z winy w sytuacji, w której zaplanowała ona taki właśnie nietypowy przebieg zdarzeń.[102] Jest to co prawda odejście od pełnej obiektywizacji testu normalności następstw, w pełni jednak uzasadnione. Istota takiego zagrożenia jest szczególnie widoczna w sytuacji posługiwania się algorytmami SI. Z uwagi na gigantyczną moc obliczeniową algorytmy są w stanie ukrywać złe intencje poprzez modelowanie ciągu zdarzeń w sposób dla człowieka wydający się być zupełnie nieprawdopodobnym. Może to być odczytane jako niespełnienie testu adekwatnego związku przyczynowego i doprowadzi do zwolnienia strony z odpowiedzialności, mimo istniejącego u SI nie tylko działania nienależytego, ale nawet celowo nastawionego na niewykonanie zobowiązania.

Łańcuch normalności następstw zostaje przerwany, gdy zaistnieje okoliczność nietypowa, dziwna, niespotykana. Przykładem takiego przerwania łańcucha będzie sytuacja, w której w wyniku niewłaściwego działania algorytmu sterującego pomieszczeniem dojdzie do niezabezpieczenia magazynu przed słońcem, co normalnie mogłoby spowodować zniszczenie produktów. Równocześnie okaże się, że jeden z produktów nie został w prawidłowy sposób oznaczony przez producenta jako łatwopalny, i z tego powodu nie był umieszczony w innym, odpowiednim magazynie. Doszło do pożaru, w wyniku którego spłonęły wszystkie produkty oraz sam magazyn. Co prawda, gdyby SI prawidłowo oceniła warunki i zasłoniła okna magazynu do tej sytuacji by nie doszło, jednak nie jest normalnym sytuacja, w której w pomieszczeniu na materiały oznakowane jako niełatwopalne znajduje się produkt łatwopalny, umieszczony tam z winy producenta, który niewłaściwie go oznaczył. Należy zwrócić szczególną uwagę na to, że SI nie posiada pewnych

[100] P. Sobolewski [w:] red. K. Osajda *„Kodeks…"* pkt. 20.
[101] *Ibidem*, por. także odmienny wyrok Sądu Najwyższego z dnia 9 lutego 2001 sygn. akt III CKN 578/00, Legalis.
[102] *Ibidem*, pkt. 27.

typowych dla człowieka wiadomości. Dla przykładu, jeżeli magazynier zobaczy kanister z benzyną bez oznaczenia o łatwopalności z pewnością i tak umieści go w innym, przystosowanym dla takich materiałów pomieszczeniu. Natomiast SI polegająca na międzynarodowych oznaczeniach produktów, obowiązkowo stosowanych przez producentów, gdy takiego oznaczenia nie zobaczy, automatycznie zostawi produkt w magazynie niewłaściwie zabezpieczonym. W takiej sytuacji, w mojej ocenie, należy zbadać przede wszystkim treść umowy między magazynującym a innymi podmiotami. Jeżeli z umowy wynika, że przy określonym stopniu nasłonecznienia magazynujący jest odpowiedzialny za zasłonięcie okien i utrzymywanie stałej temperatury pomieszczenie, mimo że nie ma tam łatwopalnych produktów, to dojdzie do nienależytego wykonania zobowiązania, w konsekwencji nie dojdzie do zwolnienia z odpowiedzialności odszkodowawczej, może natomiast być ona zmniejszona przy zastosowaniu konstrukcji przyczynienia się poszkodowanego. Natomiast jeżeli z umowy nie wynika obowiązek ochrony magazynu przed wysoką temperaturą, bo nie ma tam łatwopalnych produktów, to osoba magazynująca powinna zostać zwolniona z odpowiedzialności, ponieważ nie można jej zarzucić działania niestarannego. Błąd SI w normalnej sytuacji nie doprowadziłby do powstania pożaru, a w konsekwencji tego rodzaju szkody. Przykładów takich można podać więcej, natomiast szczególnie ważnym jest dostrzeżenie, że SI to nadal tylko algorytm. Nie posiada ona pewnych cech wrodzonych, instynktu samozachowawczego czy wiadomości typowych, ogólnych, które ma każdy z nas. Jest ona elementem układanki prawnej i technicznej, gdzie nawet oczywisty błąd człowieka, może zostać przez nią niezauważony.

Ustalenie związku przyczynowego w przypadku SI wymagać będzie zawsze opinii biegłego z zakresu informatyki, celem ustalenia, czy dane działanie algorytmu było normalne uwzględniając sposób sprawowania nad nim kontroli, wygląd kodu źródłowego i zakres zlecanych mu zadań. Chodzi tu w szczególności o określenie przez biegłego czy przy konkretnej budowie kodu źródłowego mogła zaistnieć badana sytuacja. Jeżeli dany podmiot poczynił starania celem zabezpieczenia określonych czynności np. wprowadził blokady na dokonywanie pewnych operacji, to obejście takiej blokady przez SI nie może stanowić podstawy to uznania, że nastąpił adekwatny związek przyczynowy, jeżeli tylko te zabezpieczenia były adekwatne. Normalność następstw nie zachodzi w sytuacji, kiedy w toku zdarzenia dochodzi do sytuacji trudnej do przewidzenia, ale nie niemożliwej. Patrząc ex post na dane zdarzenia można stwierdzić, że co prawda istniało prawdopodobieństwa powstania takiej

nietypowej sytuacji, ale właśnie ze względu na jej nietypowość nie zostały podjęte działania mające na celu jej uniknięcie. Należy także oceniać, czy kod źródłowy był na bieżąco monitorowany w celu wykrycia ewentualnych odstępstw od normy. O ile bowiem na początku, kiedy uruchamiamy SI, ciężko może być przewidzieć jej zachowania, o tyle w toku jej rozwoju można prześledzić to, w jaki sposób kod się zmienia i jakie potencjalne możliwości, a w konsekwencji zagrożenia, taka zmiana powoduje. To, że osoba posługująca się takim algorytmem sama takiej wiedzy na początku mieć nie będzie nie sprawa, że adekwatny związek przyczynowy nie nastąpi. Kryterium oceny jest bowiem obiektywne i właściwe dla osoby zorientowanej w danym zakresie, zaś podmiot nieposiadający wiedzy programistycznej, a decydujący się korzystać ze SI, powinien zatrudnić osoby, które są w stanie wymienione powyżej czynniki przeanalizować. Nawet osoba zorientowana w danej dziedzinie może nie zdawać sobie sprawy z zagrożeń, na które będą w stanie zwrócić uwagę specjaliści od konkretnej dziedziny. Jeżeli zatem określone następstwo byłoby zaskakujące nawet dla takiego specjalisty to można stwierdzić, że nie doszło do spełnienia przesłanki normalności następstw.

Powyższa analiza nie dotyczy SI tworzonej w modelu uczenia nienadzorowanego. Jeżeli podmiot korzystający z systemu SI decyduję się na taką właśnie metodę nauczania programu, to powinien być przygotowany na rzeczy trudne bądź niemożliwe do przewidzenia. Istotą uczenia nienadzorowanego jest to, że algorytm otrzymuje maksymalny stopień autonomiczności w działaniu i w momencie jego uruchamiania nie wiemy jakie są jego możliwości i w konsekwencji nie można tutaj mówić o normalności następstw, ponieważ nawet nietypowe działanie takiego algorytmu jest normalnym następstwem zastosowania metody uczenia nienadzorowanego. Uważam zatem, że w przypadku szkody wywołanej przez SI normalność następstw może być wyłączona tylko przez czynniki zewnętrzne takie jak np. atak hackerski, działanie poszkodowanego czy katastrofy naturalne.

Warto zwrócić jeszcze uwagę na niejednolicie rozstrzygany w literaturze problem hipotetycznej przyczynowości (causa superveniens), który dotyczy sytuacji wystąpienia szkody na skutek działania danego podmiotu, która jednak i tak wystąpiłaby, gdyby tego działania nie podjęto. W tym zakresie dr Sobolewski twierdzi, że analiza tego zjawiska powinna mieć wpływ nie na związek przyczynowy, a na ustalanie zakresu szkody.[103] Wynika to z tego, że potencjalne zdarzenie przyszłe, które i tak by nastąpiło, w żadnym razie nie

[103] *Ibidem*, pkt. 80.

wyklucza normalności następstw pierwszego ze zdarzeń. Natomiast fakt ten może mieć znaczenie przy ustalaniu poniesionej szkody. Gdyby rzeczywiście było tak, że niezależnie od poczynionych działań i tak doszłoby do powstania szkody, to powinno mieć to wpływ na sposób wyznaczenia wysokości odpowiedzialności odszkodowawczej.

Podsumowując powyższe uwagi należy stanąć na stanowisku, że przypisanie odpowiedzialności osobie, która posługuje się SI, nie jest bardzo trudne, natomiast wymaga wiedzy specjalistycznej. Kluczowym jest w tym zakresie ustalenie, że rzeczywiście doszło do powstania zobowiązania, bo odpowiedzialność kontraktowa może zaistnieć tylko wtedy, kiedy mamy do czynienia ze stosunkiem zobowiązaniowym między stronami. Dopiero w takiej sytuacji można badać wykonanie bądź niewykonanie zobowiązania oraz okoliczności, którego doprowadziły do naruszenia treści zobowiązania. Najszersze przypisanie adekwatnego związku przyczynowego do działania SI jest w mojej ocenie możliwe przy algorytmach opartych o nienadzorowane uczenie maszynowe.

4. Odpowiedzialność deliktowa

4. 1. Podstawa z art. 415

Podstawowym przepisem kontrującym zasady odpowiedzialności ex delicto w prawie cywilnym jest art. 415 KC, zgodnie z którym „Kto z winy swojej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia". Ten krótki i zwięzły przepis zarówno w doktrynie jak i orzecznictwie doczekał się setek różnych interpretacji w poszczególnych stanach faktycznych, będąc przedmiotem sporów co do swojego zakresu. Jego istotna sprowadza się do przyznania podmiotom prawa prywatnego ochrony przed naruszeniami bezprawnymi, które nie mają swojego umocowania w żadnym stosunku kontraktowym lub ewentualnie pozostają z nim w zbiegu. Chociaż to prawo karne służy karaniu zachowań bezprawnych, godzących w poszczególne jednostki, to nie zawsze naruszenia danego typu będą przez prawo karne sankcjonowane, ponadto z faktu skazania danej osoby podmiot prywatny nie ma żadnej rekompensaty (może poza moralną). W tym celu właśnie wprowadzono do polskiego kodeksu cywilnego odpowiedzialność za czyny niedozwolone.

Art. 415 KC konstruuje podstawowy, bardzo ogólny typ deliktu. Chociaż w doktrynie nie ma co do tego pełnej zgody, przyjmuje się, że w sytuacji możliwości skorzystania z innej, bardziej szczegółowej podstawy odpowiedzialności deliktowej jest ona właściwsza, co jednak nie wyklucza korzystania

z art. 415 KC. Pogląd przeciwny opiera się na założeniu, że takie konkretne przepisy stanowić będą lex specialis. Z praktycznego punktu widzenia należy jednak wskazać, że zgodnie z Kodeksem Postępowania Cywilnego nie ma potrzeby wskazywania podstawy prawnej dochodzonych roszczeń.

Przesłanki przypisania odpowiedzialności z art. 415 to:

- zachowanie człowieka (bezprawne)
- szkoda
- wina człowieka
- adekwatny związek przyczynowy pomiędzy zawinionym zachowaniem a szkodą[104]

Jak widać przypisywanie odpowiedzialności SI na podstawie powyższego przepisu jest niemożliwe, ponieważ odnosi się on tylko do człowieka, chyba że zdecydujemy się zastosować ten przepis na zasadzie analogii w stosunku do silnej SI, która otrzyma własną zdolność prawną, stworzoną na kształt zdolność prawnej przyznanej człowiekowi, a nie na kształt osoby prawnej. Na ten moment jednak SI nie została wyposażona w tego typu cechy. W związku z tym należy zastanowić się nad tym, czy osoby odpowiedzialnej można poszukiwać w innym miejscu. Jako oczywisty pomysł nasuwa się poszukiwanie odpowiedzialności u właściciela SI, a tak naprawdę dysponenta SI, czyli osoby, która się nią posługuje.[105] Właściciel to osoba (fizyczna, prawna, tzw. ułomna osoba prawna), która dysponuje prawem własności do danego algorytmu, niezależnie od tego, czy wytworzyła go osobiście czy też nabyła go od podmiotu zewnętrznego. Może ona posługiwać się w swojej działalności tym systemem SI, ale nie musi. Z kolei dysponent to osoba, która faktycznie korzysta z algorytmu w toku wykonywanej działalności, niekoniecznie jednak dysponuje prawem własności do algorytmu np. korzysta z niego na zasadzie licencji. W mojej ocenie powyższy koncept dysponenta SI, stworzony przez prof. Chłopeckiego, odpowiada zaproponowanej przez UE definicji wdrażającego system SI, o czym więcej w rozdziale 6.

Druga ewentualność to przypisanie odpowiedzialności twórcy SI, jakkolwiek w mojej ocenie wobec twórcy roszczenie powstałe w relacji poszkodowany – dysponent będzie mogło być dochodzone na podstawie odpowiedzialności kontraktowej, wynikającej z postanowień umowy np. zapewnienie bezawaryjności systemu, a ponadto na podstawie art. 415, jeżeli twórcy nie

[104] B. Lackoroński, M. Raczkowski [w:] red. K. Osajda, *„Kodeks…”*, komentarz do art. 415, pkt. 35

[105] Zob. szerz. A. Chłopecki, *„Szkice…”*, rozdział 5

można przypisać odpowiedzialności solidarnej za szkodę po stronie poszkodowanego, natomiast jeżeli będzie można taką solidarną odpowiedzialność przypisać to zastosowanie znajdzie roszczenie regresowe z art. 441 § 2 i 3 KC. Próba dochodzenia odpowiedzialności w relacji poszkodowany – twórca jest o tyle sztuczna, że dana szkoda zawsze będzie pozostawać w związku z zachowaniem dysponenta, nawet biernym, w postaci korzystania z oprogramowania.

Pierwsza przesłanka w postaci zachowania człowieka powinna być uzupełniona zawsze o wskazanie, że jest to zachowanie bezprawne. Nie można bowiem przypisać odpowiedzialności za szkodę osobie, która w żaden sposób nie naruszyła obowiązujących reguł postępowania. W związku z tym twierdzi się, że bezprawność jest wpisana w konstrukcję tego przepisu. [106] Niektórzy przypisują przesłankę bezprawności do elementów winy, jednak w mojej ocenie jest to niepoprawne. Jak będzie to wskazane poniżej, wina jest elementem subiektywnym, natomiast samo zachowanie elementem obiektywnym. Wykluczenie bezprawności zachowania sprawia, że dalsza analiza przesłanek (w tym winy) jest bezprzedmiotowa. Może bowiem zaistnieć sytuacja, w której dojdzie do zachowania bezprawnego, które nie będzie zawinione, natomiast sytuacja odwrotna jest niemożliwa. Pod pojęciem bezprawności rozumie się zarówno przepisy prawa powszechnie obowiązującego, ale także normy istniejące w oderwaniu od przepisów, takie jak zwyczaje, normy moralne, ustalone zasady postępowania czy zasady współżycia społecznego.[107] Odmiennie wskazuje się, że bezprawność może dotyczyć jedynie powszechnie obowiązujących przepisów prawa, jednak pogląd ten został odrzucony przez Sąd Najwyższy.[108] W związku z tym można twierdzić, że katalog zachowań bezprawnych może być bardzo szeroki i będzie obejmować np. próbę modyfikacji kodu źródłowego programu, korzystanie z programu w celu oszukania drugiej strony czy nawet podłączenie oprogramowania bez odpowiedniego nadzoru. Natomiast

---

106 B. Lackoroński, M. Raczkowski [w:] red. K. Osajda, *„Kodeks…"*, komentarz do art. 415, pkt. 39

107 *Ibidem*, pkt. 42 za: R. Longchamps de Bérier, „Zobowiązania", Lwów, 1939, s. 235; L. *Domański*, *„Instytucje kodeksu zobowiązań. Komentarz teoretyczno-praktyczny. Część ogólna"*, t. 2, Warszawa 1936, s. 603–604; F. Zoll, *„Zobowiązania w zarysie"*, Warszawa 1945, s. 130–131; Z. Banaszczyk [w:] red. K Pietrzykowski, *„Kodeks cywilny. Komentarz."*, Warszawa 2015, t. I, art. 415, Nb 38; W. Czachórski [w:] *„System Prawa Cywilnego"*, t. III, cz. 1, s. 533–534; G. Karaszewski [w:] red. J. Ciszewski, *„Kodeks cywilny. Komentarz"*, Warszawa 2014, art. 415, Nb 17; J.M. Kondek, *„Bezprawność jako przesłanka odpowiedzialności odszkodowawczej"*, Warszawa 2013, s. 75–78; Z. Masłowski (w:) red. Z. Resich, *„Komentarz do Kodeksu cywilnego"*, t. II, Warszawa 1972, s. 982; M. Zelek [w:] red. M. Gutowski, *„Kodeks cywilny. Komentarz"*, t. I, art. 415, Nb 16; wyrok Sądu Najwyższego z dnia 21 maja 2015 r., sygn. akt IV CSK 539/14, Legalis.

108 *Ibidem*, za: wyrok Sądu Najwyższego z dnia 21 maja 2015 r., sygn. akt IV CSK 539/14, Legalis.

w przypadku twórcy oprogramowania, o ile nie będą miały tutaj zastosowania przepisy dotyczące nienależytego wykonania zobowiązania, wad produktu, niezgodności towaru z umową, będzie to nieodpowiednia procedura testowa, korzystanie z niecertyfikowanego oprogramowania, zatrudnianie osób w oparciu o fałszywe dyplomy i certyfikaty. Nie ma więc wątpliwości, że szereg naruszeń SI będzie można przyporządkować jako bezprawne zachowanie dysponenta lub twórcy.

Druga przesłanka w postaci szkody nie wymaga większego komentarza, gdyż w tym zakresie nie ma żadnych odmienności, a więc można domagać się odszkodowania za szkodę w majątku danej osoby, jak również szkody na osobie. Wymiar szkody jest natomiast badany zarówno w zakresie szkody rzeczywiście wyrządzonej, jak również w zakresie utraconych korzyści. Jest to więc porównanie majtku poszkodowanego po dokonaniu naruszenia, z majątkiem jaki istniałby w razie, gdyby do takiego naruszenia niedoszło.

Przesłanka winy powinna być rozumiana w sposób subiektywny. Jest to możliwość „zarzucenia zachowania sprawczego”[109]. Chociaż rozróżnia się winę jako umyślną i nieumyślną, odwołując się przy tym do przepisów prawa karnego[110], to jednak nie ma ono zasadniczego znaczenia. W pierwszej kolejności należy wskazać, że prawo karne odróżnia winę od umyślności i nieumyślności, traktując je jako zupełnie odmienne płaszczyzny analizy, stąd mówienie o winie umyślnej bądź nieumyślnej jest błędne.[111] Co więcej „do przypisania odpowiedzialności na zasadzie winy określonemu podmiotowi wystarczy, że jego zachowanie, w wyniku którego doszło do wyrządzenia szkody, jest zarzucalne nawet jako najlżejszy stopień nieumyślności (culpa levissima).”[112] Przypisanie winy będzie jednak niezwykle trudne w przypadku dysponenta SI. Jeżeli bowiem wykaże on, że podjął wszelkie wymagane w danych okolicznościach kroki, a więc wykazał się odpowiednim stopniem staranności, nie będzie można przypisać mu odpowiedzialności. Jak słusznie wskazuje prof. Chłopecki, w przypadku konsumenta wystarczającym będzie postępowanie zgodnie z instrukcją obsługi danego urządzenia oraz posługiwanie się urządzeniem, które spełnia odpowiednie normy i posiada odpowiednie certyfikaty.[113]

---

109 *Ibidem*, pkt. 73.

110 *Ibidem*, pkt. 75.

111 Zob. szerz. „Dogmaty karnisty”, www.dogmatykarnisty.pl, blog prowadzony przez dr Mikołaja Małeckiego

112 B. Lackoroński, M. Raczkowski [w:] red. K. Osajda, *„Kodeks…”*, komentarz do art. 415, pkt. 76 za: T. Dybowski [w:] *„System Prawa Cywilnego”*, t. III, cz. 1, s. 200; Z. Banaszczyk [w:] red. K Pietrzykowski, *„Kodeks..”*, nb 34.

113 A. Chłopecki, *„Szkica…”*, rozdział 7.

Z całą pewnością dużo łatwiej będzie przypisać wszelkie zachowania umyślne jak modyfikacje kodu, natomiast innego typu zarzuty jak niezachowanie reguł ostrożności w punktu widzenia dowodowego będą trudne do wykazania, a wykazanie tego jest kluczowe. Natomiast zaproponowane regulacje unijne, o których będę dokładnie pisać w kolejnym rozdziale, wprowadzają w tym zakresie spore ułatwienie, a mianowicie wprowadza się domniemanie winy po stronie wdrażającego oprogramowanie SI. Podobnie w przypadku twórcy SI, z uwagi na jej niezwykle trudną do uchwycenia istotę, gdyż algorytm z definicji uczy się nowych rzeczy i ma pewien stopień autonomiczności, winę będzie ciężko udowodnić, co jest podstawą przypisania odpowiedzialności. Realna możliwość udowodnienia winy pojawi się zazwyczaj jedynie w przypadku naruszeń jednoznacznych - rażących błędów w sztuce, oczywistych omyłek czy ewentualnych złych intencji. Jednak trudności w wykazaniu winy nie oznaczają niemożności powoływania się na komentowany przepis. Tutaj z kolei, zdaniem komitetu ds. prawnych UE, kluczowe znaczenie będzie miała nowelizacja dyrektywy o odpowiedzialności za produkty wadliwe.[114]

Adekwatny związek przyczynowy został już szerzej omówiony w poprzednim rozdziale. W tym miejscu wystarczy jedynie wskazać, że jego udowodnienie nie powinno być przesadnie trudne. Dla przykładu, jeżeli w kodzie źródłowym wskazano błędy wynikające z braku rzetelnego i profesjonalnego programowania i testowania algorytmu, a w wyniku tego błędu powstała szkoda np. system inteligentnego sterowania domem nie uruchomił po wyjściu alarmu, to działanie programisty pozostaje w związku z brakiem włączenia się alarmu, co w konsekwencji prowadziło do umożliwienia złodziejowi wejścia do domu w sposób niezauważony. Gdyby algorytm działał poprawnie alarm zostałby uruchomiony, a złodziej albo uciekł by z miejsca zdarzenia od razu po jego uruchomieniu, albo w momencie przyjazdu ochrony czy interwencji sąsiada, co znacznie zmniejszyłoby rozmiar szkód. Większe straty w wyniku włamania są z kolei normalnym następstwem braku uruchomienia się alarmu. W takiej sytuacji twórca oprogramowania może odpowiadać nawet pomimo ubezpieczenia domu, gdyż brak załączenia alarmu często w umowach ubezpieczeniowych stanowi podstawę odmowy zapłaty ubezpieczenia. Problematyka umów ubezpieczeniowych nie jest jednak przedmiotem tej pracy, w związku z czym nie będę jej rozwijać, jednak problem ten zasygnalizować. Systemy SI będą mieć duży wpływ na cały rynek ubezpieczeń, tym bardziej, że UE

[114] Dyrektywa Rady z dnia 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe

w swoich regulacjach proponuje wprowadzenie dla systemów SI wysokiego ryzyka obowiązkowych ubezpieczeń.

4. 2. Inne podstawy odpowiedzialności na zasadzie winy

Z istniejących w polskim kodeksie cywilnym instytucji szczególnych opierających się na zasadzie winy na szczególną uwagę zasługują art. 429 KC, a więc wina w wyborze, a także art. 431 KC, a więc odpowiedzialność za zwierzęta.

Pierwszy z tych przepisów stanowi, że „kto powierza wykonanie czynności drugiemu, ten jest odpowiedzialny za szkodę wyrządzoną przez sprawcę przy wykonywaniu powierzonej mu czynności, chyba że nie ponosi winy w wyborze albo że wykonanie czynności powierzył osobie, przedsiębiorstwu lub zakładowi, które w zakresie swej działalności zawodowej trudnią się wykonywaniem takich czynności". Stosując ten przepis na zasadzie analogii można rozważać jego stosowanie w przypadku powierzenia wykonania danej czynności SI. Możliwość przypisania odpowiedzialności wymaga spełnienia następujących przesłanek:

- fakt powierzenia czynności przez powierzającego wykonawcy
- bezprawne działanie lub zaniechanie wykonawcy, które pozostaje w związku przyczynowym ze szkodą
- wina w wyborze
- istnienie pomiędzy podmiotami stosunku podporządkowania
- powierzenie czynności nieprofesjonaliście[115]

Ponieważ większość tych przesłanek była już analizowana powyżej, w tym miejscu najwięcej uwagi należy poświęcić przesłance winy w wyborze. Nie ulega wątpliwości, że SI nie może być traktowana jako profesjonalista, gdyż nie jest żadną osobą prowadzącą działalność gospodarczą dla siebie samej. Jest to jedynie sztuczna konstrukcja powierzenia komuś czynności, analizowana w świetle analogii. Zawsze więc SI będzie tutaj traktowana jako nieprofesjonalista, a przynajmniej póki nie doczekamy czasów osobowości prawnej SI albo jej samoświadomości. Sama okoliczność, że dany system SI jest powszechnie uznawany za profesjonalny i został doceniony np. na konkursach międzynarodowych nie uzasadnia stwierdzenia, że mamy do czynienia z profesjonalistą, bo w ten sposób dojdzie do przeniesienia ewentualnej odpowiedzialności

[115] W. Borysiak [w:] red. K. Osajda, *„Kodeks…"*, komentarz do art. 429, pkt. 14 i 15.

na algorytm, który w żaden sposób nie będzie mógł pokryć ewentualnego odszkodowania. Wina w wyborze polega nie na działaniu bezprawnym powierzającego, gdyż ciężko o przypisanie takiej bezprawności. Bezprawność zachowania badamy u osoby, która daną czynność wykonuje. Natomiast wina powierzającego sprowadza się do pytania, czy w wyborze osoby, której została zlecona czynność, kierował się on należytą starannością.[116] Na winę w wyborze składa się „element obiektywny w postaci wybrania osoby obiektywnie niezdolnej, niewłaściwej lub nieodpowiedniej do wykonania powierzonego jej zadania oraz element subiektywny, polegający na możliwości postawienia danej osobie zarzutu, że mogła dokonać w danej sytuacji właściwszego wyboru, lecz tego nie dokonała, lub mogła nie dokonywać powierzenia czynności innej osobie, lecz sama ją wykonać."[117] W tym przypadku należy się więc kierować oceną, czy decydując się na wybór SI dana osoba wybrała produkt z odpowiednimi certyfikatami, zabezpieczeniami, gwarancjami ze strony jego producenta, czy prawidłowo wskazała na zakres zadania, nie zlecając zadań z np. z chęcią wywołania szkody. Jest to więc analiza tego, czy wybrany produkt, a nie osoba, spełnia kryteria adekwatne do powierzonych zadań.

SI sama nie może być profesjonalnym podmiotem, natomiast inne osoby mogą zlecać wykonanie pewnych zadań przedsiębiorcom posiadającym tego typu oprogramowania. W takiej sytuacji nie będziemy badali samego algorytmu SI, ale to jakie zapewnienia składał zewnętrzny podmiot posługujący się taki systemem, jakie ma opinie na rynku. Takie badanie będzie zatem odbywać się w sposób identyczny do tego, jakie przeprowadzamy przy wyborze każdego innego podmiotu zewnętrznego. W tym zakresie SI nie powinna być traktowana inaczej, gdyż kryterium stanowi tutaj osoba przedsiębiorcy, a nie to jakimi posługuje się on narzędziami do realizacji zlecenia.

Dużo ciekawsza i bardziej adekwatna wydaj się być podstawa odpowiedzialności z art. 431 KC. Zgodnie z paragrafem pierwszym tego przepisu „Kto zwierzę chowa albo się nim posługuje, obowiązany jest do naprawienia wyrządzonej przez nie szkody niezależnie od tego, czy było pod jego nadzorem, czy też zabłąkało się lub uciekło, chyba że ani on, ani osoba, za którą ponosi odpowiedzialność, nie ponoszą winy." Analogia do zwierzęcia jest o tyle trafna, że SI tak jak zwierzę potrafi w pewien sposób działać samodzielnie, jednak świadomości takiej jak człowiek nie posiada. Co prawda zwierzęta są świadome i odczuwają emocje, mają swoje potrzeby fizjologiczne, czym

116 *Ibidem*, pkt. 39.

117 *Ibidem*, pkt. 40 za:. P. Machnikowski [w:] *„System Prawa Prywatnego"*, t. 6, Warszawa 2014, s. 468, Nb 53

różnią się od SI, jednak generalnie dla nas, jako osoby zewnętrznie patrzącej na sytuację, ich proces decyzyjny pozostaje zagadkowy. Pewne ich zachowania potrafimy z czasem przewidzieć, ale w przypadku SI będzie tak samo. Również zwierzęta są w stanie nas zaskoczyć swoim zachowaniem. Historie, kiedy dziecko zostaje pogryzione przez psa, który do tej pory był całkowicie bezproblemowy i spokojny, nie są rzadkie. Myślenie ustawodawcy sprowadzało się do następującej tezy: nie do końca wiemy jak może zachować się zwierzę, ale rozumiemy potrzebę jego posiadania i nie możemy tego zakazać. Zwierzę jednak nie ma jak zrekompensować szkód, które wyrządzi (co najwyżej można je zająć i sprzedać, a pieniądze będą służyć jako odszkodowanie). Dlatego też najlepszym wyjściem z sytuacji będzie obciążenie ryzykiem posiadania takiego zwierzęcia osobę, która chce je posiadać. Nieadekwatne będzie jednak konstruowanie odpowiedzialności na zasadzie ryzyka. Dlatego należy tutaj zastosować pewnego rodzaju winę w nadzorze nad tym zwierzęciem. Ze SI jest podobnie: „skoro człowieku chcesz z niej korzystać to powinieneś w odpowiedni sposób SI nadzorować. Jeśli tego nie uczynisz będziesz musiał odpowiedzieć odszkodowawczo za to, co SI zrobi." Jedyna różnica polega na tym, że zwierzęta nie są zazwyczaj w stanie spowodować tak poważnych szkód jak SI np. na giełdzie. Stąd w przypadku przedsiębiorców intuicyjnie wydaje się, że bardziej adekwatna będzie odpowiedzialność oparta na zasadzie ryzyka, ale o tym za chwilę. Zatem w przypadku konsumentów, którzy korzystają ze SI dla własnej przyjemności (ułatwianie sobie życia to przecież przyjemność) najbardziej zbliżona wydaje się sytuacja korzystania ze zwierząt (kupujemy je także dla przyjemności). Również UE w swoich motywach do projektu regulacji wskazuje, że sytuacja wyrządzenia szkody przez SI jest podobna właśnie do sytuacji wyrządzenia szkody przez zwierzę.

Szukanie podstaw w klasycznej winie w nadzorze z art. 427 KC wydaje mi się koncepcją słabiej odpowiadającej temu, czym jest SI. Wina w nadzorze opiera się na założeniu, że człowiek na pewnym etapie swojego życia nie jest w stanie kontrolować swojego zachowania z powodu okoliczności zewnętrznych, czasami wynikających z uwarunkowań genetycznych np. choroby układu nerwowego, a w przypadku dziecka wynikająca z niewielkiego doświadczenia życiowego i braku wykształcenia jeszcze na tym etapie pewnych cech osobowości. Jest to więc sytuacja będąca odstępstwem od normalnego zachowania się człowieka dorosłego, sprawnego intelektualnie i fizycznie, który nie wymaga dodatkowej opieki. SI natomiast ze swej istotny nie ma świadomości i zawsze będzie musiała być przez kogoś nadzorowana, inaczej niż dziecko, które wyrośnie, czy osoba chora, która może wyzdrowieć. Podobnie jest ze

zwierzętami, które po prostu należy pilnować i nigdy nie osiągną one autonomiczności prawnej. Wina będzie tutaj polegać na niewłaściwym nadzorze nad SI, a więc na braku kontroli bazy danych, z której się uczy, braku pilnowania aktualizacji, łatek systemowych, poprawności działania czy odpowiednich zabezpieczeń przed teoretycznymi zagrożeniami cyberbezpieczeństwa.

4. 3. Odpowiedzialność na zasadzie ryzyka

Najbardziej intuicyjnie, gdy myślimy o SI, nasuwa nam się pomysł o zastosowaniu regulacji dotyczącej odpowiedzialności na zasadzie ryzyka. Jest to w pełni poprawna myśl, gdyż odpowiedzialność na zasadzie ryzyka została wprowadzona do polskiego kodeksu cywilnego z uwagi na większe ryzyko wystąpienia poszczególnych szkód przy posługiwaniu się nowymi wynalazkami. Ze SI jest podobnie, dlatego też warto przyjrzeć się w tym zakresie art. 435 KC, zgodnie z którym „ Prowadzący na własny rachunek przedsiębiorstwo lub zakład wprawiany w ruch za pomocą sił przyrody (pary, gazu, elektryczności, paliw płynnych itp.) ponosi odpowiedzialność za szkodę na osobie lub mieniu, wyrządzoną komukolwiek przez ruch przedsiębiorstwa lub zakładu, chyba że szkoda nastąpiła wskutek siły wyższej albo wyłącznie z winy poszkodowanego lub osoby trzeciej, za którą nie ponosi odpowiedzialności". Aby przypisać odpowiedzialność na podstawie powyższego przepisu muszą zostać spełnione następujące przesłanki:

- prowadzone na własny rachunek przedsiębiorstwo
- wprawiane w ruch za pomocą sił przyrody
- szkoda
- związek przyczynowy
- brak spełnienia przesłanki negatywnej

Powszechnie już uznaje się, że samo zasilanie przedsiębiorstwa prądem elektrycznym nie jest wystarczające do tego, aby można było zastosować powyższy przepis. Jak twierdzi Sąd Najwyższy "tam zatem, gdzie nie chodzi o uruchomienie dużych mocy elementarnych, nie można obecnie mówić o szczególnym niebezpieczeństwie, które leżało u podstaw wprowadzenia odpowiedzialności na zasadzie ryzyka".[118] Teza ta jednak nie pasuje to działalności SI, gdyż ta może wiązać się z bardzo dużym niebezpieczeństwem. Ponadto często takie systemy będą wykorzystywane także tam, gdzie działają inne maszyny np. w elektrowniach czy na kolei. Zastosowanie zatem przepisów

[118] Wyrok Sądu Najwyższego z dnia 8 grudnia 2015 r., sygn. akt I UK 97/05.

o odpowiedzialności na zasadzie ryzyka będzie moim zdaniem wynikać nie z samego faktu zastosowania w przedsiębiorstwie SI, ale z tego czego dotyczy prowadzona działalność i przy jakich czynnościach SI będzie wykorzystywana. Jeżeli przedsiębiorstwo napędzane jedynie energię elektryczną wykorzystuje algorytm SI to obsługi czynności zupełnie niezwiązanej z zasadniczym przedmiotem działalności, równocześnie nie stanowiącą dużego ryzyka, nie będzie można zastosować tej odpowiedzialności. Zatem jeżeli SI służy do obsługi bramy wjazdowej do zakładu to ryzyko wyrządzenia szkody jest niewielkie, a zatem ten model odpowiedzialności nie może być zastosowany. Z kolei jeżeli SI używana jest do sterowania ruchem pojazdów to w przypadku potrącenia pieszego taki model odpowiedzialności można zastosować, ponieważ ryzyko wystąpienia szkody jest w takiej sytuacji wysokie. Co ważne, ruch nie dotyczy samej szkody, a działalności przedsiębiorstwa jako takiego.[119] Z tego też względu słusznie wskazał Sąd Najwyższy, że „ruch przedsiębiorstwa lub zakładu w ujęciu art. 435 § 1 k.c. to każda działalność tego przedsiębiorstwa lub zakładu, a nie tylko taka, która jest bezpośrednio związana z działaniem sił przyrody i która stanowi następstwa ich działania".[120] Z tego też względu np. pośliznięcie na peronie, w sytuacji gdy nawet brak było na nim pociągu, będzie kwalifikować się pod powyższy przepis.[121] Z kolei zgodnie z orzecznictwem Sądu Najwyższego „związek między ruchem przedsiębiorstwa i szkodą występuje wtedy, gdy szkoda nastąpiła w wyniku zdarzenia funkcjonalnie powiązanego z działalnością przedsiębiorstwa, choćby nie było bezpośredniej zależności między użyciem sił przyrody a szkodą".[122] Odpowiedzialność na zasadzie ryzyka sprowadza się do braku konieczności wykazywania winy czy nawet bezprawności. Nawet w sytuacji działania zgodnie z prawem i wszelkimi zaleceniami, w przypadku zaistnienia określonego zdarzenia, będzie można domagać się odszkodowania, pod warunkiem, że nie zachodzą okoliczności wyłączające odpowiedzialność, a więc siła wyższa bądź wina poszkodowanego lub osoby trzeciej. Nie jest to więc odpowiedzialność absolutna, która występuje np. w przypadku elektrowni atomowych, chociaż i tam przewiduje się wyjątki np. wojna, ale już nie zwalnia się z odpowiedzialności nawet w przypadku katastrof naturalnych, przy których tak niebezpieczna rzecz jak elektrownia

[119] R. Morek [w:] red. K. Osajda, *„Kodeks…"*, komentarz do art. 435, pkt. 13.

[120] *Ibidem*, za: wyrok Sądu Najwyższego z dnia 5 stycznia 2001 r., sygn. akt V CKN 190/00, Legalis

[121] *Ibidem*, za: G. Bieniek, J. Gudowski [w:] red. J. Gudowski, *„Kodeks cywilny. Komentarz"*, Warszawa 2013, Ks. III, cz. 1, art. 435, s. 621, Nb 16.

[122] *Ibidem*, za: wyrok Sądu Najwyższego z dnia 11 grudnia 1963 r., sygn. akt II CR 116/63.

atomowa powinna być nadal w pełni zabezpieczona. W przypadku SI rozwiązanie oparte o zasadę ryzyka jest bardzo pożądane. W przypadku przedsiębiorców posługujących się algorytmami SI potencjalne szkody wyrządzone przez program mogą być naprawdę spore. Z kolei udowodnienie winy w tych przypadkach będzie niezwykle utrudnione. W przypadku odpowiedzialności opartej o zasadę ryzyka istnieje domniemanie naruszenia w przypadku wykazania powyższych przesłanek, a zwolnić z odpowiedzialności można się jedynie wtedy, kiedy to przedsiębiorca wykaże podstawy do zwolnienia. Znacznie ułatwia to więc dochodzenie odszkodowania, co jest szczególnie istotne, gdyż zazwyczaj naprzeciwko takiego przedsiębiorcy staje słabszy podmiot – zwykły człowiek. Taka konstrukcja pozostaje również w zgodzie z ratio legis wprowadzonego do kodeksu cywilnego przepisu. Adekwatność odpowiedzialności na zasadzie ryzyka dostrzega także prawodawca unijny, który w zaproponowanych regulacjach opiera odpowiedzialność wdrażającego system SI na zasadzie ryzyka, przy czym tylko dla tzw. systemów SI wysokiego ryzyka. Szerzej na ten temat w rozdziale 6.

4. 4. Produkt niebezpieczny

Regulacje dotyczące odpowiedzialności za produkt niebezpieczny w polskim kodeksie cywilnym znaleźć można w tytule VI[1]. Zgodnie z art. 449[1] § 2 „Przez produkt rozumie się rzecz ruchomą, choćby została ona połączona z inną rzeczą". Za produkt uważa się także zwierzęta i energię elektryczną". SI ciężko nazwać rzeczą ruchomą, gdyż jest to jedynie kod źródłowy. Zgodnie z kodeksową definicją rzeczy mogą być jedynie materialne. W związku z tym sam kod źródłowy nigdy nie będzie mógł uzyskać takiej kwalifikacji. Połączenie go z inną rzeczą jest rozwiązaniem dający możliwość zastosowania reżimu przewidzianego dla produktów niebezpiecznych, jednak obecnie większość SI nie ma postaci fizycznej, androidalnej. Klasyczne roboty, takie jakie pojawiają się np. w serii „Star Wars" obecnie stanowią margines prac nad SI. Niemniej jednak regulacje odpowiedzialności za produkt niebezpieczny mogą stanowić bardzo ciekawy fundament pod prace nad wprowadzeniem nowej, bardzo podobnej regulacji, która obejmie swoim zakresem także SI. Innym rozwiązaniem jest po prostu zmiana definicji produktu niebezpiecznego, na co w swoich propozycjach zwraca uwagę komitet ds. prawnych UE, w związku z czym można się spodziewać, że w najbliższym czasie taka zmiana nastąpi. Zgodnie z kodeksową definicją „niebezpieczny jest produkt niezapewniający bezpieczeństwa, jakiego można oczekiwać, uwzględniając normalne użycie

produktu. O tym, czy produkt jest bezpieczny, decydują okoliczności z chwili wprowadzenia go do obrotu, a zwłaszcza sposób zaprezentowania go na rynku oraz podane konsumentowi informacje o właściwościach produktu. Produkt nie może być uznany za niezapewniający bezpieczeństwa tylko dlatego, że później wprowadzono do obrotu podobny produkt ulepszony". Przekładając powyższą definicję na SI można zauważyć, że algorytmy tego typu z uwagi na ich ograniczoną przewidywalność zawsze będą mogły być uznane za potencjalnie niebezpieczne, a pełne poinformowanie o jego możliwościach będzie niemożliwe. Z kolei w toku normalnego użycia produktu niebezpieczeństwo istnieje przez cały czas. Stosowanie tej regulacji obciążałoby producenta, a także w niektórych przypadkach, wytwórcę materiału, surowca lub części składowych. Z kolei w zakresie okoliczności zwalniających z odpowiedzialności wskazana w art. 449^3 § 2 przesłanka niemożności przewidzenia niebezpiecznych właściwości produktów nie będzie zwalniać z odpowiedzialności, gdyż nieprzewidywalność SI jest jej cechą definicyjną, przynajmniej w zakresie obszaru, funkcji, dla których algorytm został stworzony. Są to zatem przepisy, które będą mogły stanowić skuteczny mechanizm ochronny przed szkodami wyrządzonymi przez SI, natomiast wymagają nowelizacji w zakresie definicji produktu niebezpiecznego oraz uwzględnienia specyfiki SI, gdyż w obecnym zakresie, z uwagi na nieprzewidywalność wielu systemów SI, wprowadzają odpowiedzialność zdecydowanie zbyt szeroką, co może negatywnie odbić się na rozwoju tego typu oprogramowania.

4. 5. Odpowiedzialność za delikty – podsumowanie

Podsumowując powyższe rozważania należy wskazać, że przy obecnie istniejących regulacjach prawnych przypisanie odpowiedzialności za szkody wyrządzone przez SI jest możliwe, aczkolwiek w praktyce może być trudne do osiągnięcia z uwagi na konieczność udowodnienia przesłanek, które dowodowo są trudne do wykazania. Powyższe wnioski są w większości zgodne z tym, co w swojej monografii zaprezentował prof. Chłopecki. W jego ocenie odpowiedzialność deliktowa SI prezentuje się w sposób następujący:

- „w zakresie odpowiedzialności deliktowej postulować należy wprowadzenie dla prywatnych nieprofesjonalnych dysponentów SI odpowiedzialności na zasadzie winy w nadzorze, czy raczej odpowiednika takiej odpowiedzialności. W konsekwencji dysponent SI ponosiłby odpowiedzialność za szkodę wyrządzoną przez SI, o ile w sposób nieprawidłowy („niezgodny

z instrukcją") z SI by korzystał – przy czym na nim spoczywałby ciężar dowodu, że jego działanie było prawidłowe;

- powyższe nie zmieniałoby innych możliwych podstaw odpowiedzialności za szkody wyrządzone przez SI, zwłaszcza tam, gdzie SI byłoby narzędziem działalności gospodarczej lub składnikiem przedsiębiorstwa, należałoby również utrzymać lub być może rozszerzyć system obowiązkowych ubezpieczeń, np. telekomunikacyjnych;
- SI, zwłaszcza słaba SI, pozostawałaby produktem, w wyniku czego brak byłoby podstaw do wyłączenia w stosunku do jej działań i wobec producentów, względnie sprzedawców tzw. odpowiedzialności za produkt niebezpieczny."[123]

W zakresie pierwszego wniosku w mojej ocenie właściwsze jest odwoływanie się do odpowiedzialności opartej o przepis dotyczący szkód wyrządzonych przez zwierzęta, jednak zastosowanie jednej bądź drugiej regulacji nie niesie ze sobą dużych odmienności. Uzasadnieniem mojego poglądu jest jednak to, że SI należy porównywać bardziej do stanu posiadania zwierzęcia, niż opieki nad małym dzieckiem albo osobą starszą, nieporadną czy też chorą.

Drugi wniosek jest już w pełni do zaakceptowania. Stosowanie do przedsiębiorców posługujących się SI przepisów o odpowiedzialności za ruch przedsiębiorstwa, a zatem odpowiedzialności opartej o zasadę ryzyka, jest rozwiązaniem najlepiej przystającym do obecnej rzeczywistości. Kwestia stosowania obowiązkowych ubezpieczeń jest problemem bardzo ważnym, jednak nie pokrywa się z tematem tej pracy. Niemniej jednak ubezpieczenia wydają się być rozwiązaniem bardzo pożądanym, bardziej nawet niż wariant wnoszenia SI do spółki kapitałowej jako aportu. Sam jednak obowiązek ich posiadania może różnic się w zależności od prowadzonej działalności i rodzaju SI. Jak słusznie wskazuje prof. Chłopecki w przypadku pojazdów autonomicznych takie ubezpieczenia muszą być obowiązkowe i funkcjonować tak jak obecnie, a jedyna różnica dotyczyć będzie szacowania przez ubezpieczyciela ryzyka wystąpienia danego zdarzenia np. zamiast wypadku z powodu niewłaściwego użytkowania pojazdu będzie trzeba rozważać niewłaściwe dbanie o aktualizacje systemu chroniącego przed atakami hackerskimi.[124] Propozycje legislacyjne UE zakładają obowiązkowe ubezpieczenia dla wszystkich wdrażających systemy SI wysokiego ryzyka, wskazując nawet na maksymalne kwoty odpowiedzialności odszkodowawczej.

123 A. Chłopecki *„Szkice..."*, rozdział 7
124 *Ibidem*.

Z kolei trzeci wniosek, w kształcie obecnych regulacji, wydaje się być nietrafiony. Algorytmy SI rzadko przybierają postać rzeczy fizycznych, zwłaszcza w okresie bardzo dynamicznego rozwoju danych opartych o systemy chmurowe. Z kolei wgranie algorytmu przez użytkownika na swój komputer nie tworzy produktu niebezpiecznego wytwarzanego przez producenta. W przypadku tak szerokiej i restrykcyjnej odpowiedzialności wątpliwe wydaje się rozszerzanie zakresu stosowania tego przepisu. Niemniej jednak sama regulacja wydaje się być bardzo adekwatna do omawianego problemu, a jej zastosowanie będzie możliwe jeśli tylko definicja produktu niebezpiecznego zostanie w odpowiedni sposób zmodyfikowana. Propozycja unijna także zwraca uwagę, że rozwiązania wynikające z dyrektywy o produktach wadliwych będą adekwatne dla problemu SI, niemniej powinny zostać zmodyfikowane w niezbędnym zakresie.

5. Czyny nieuczciwej konkurencji – przykłady zagrożeń

Postanowiłem rozważyć problemy ogólne zarysowane w tej pracy na tle szczegółowej problematyki czynów nieuczciwej konkurencji, gdyż SI obecnie najbardziej dotykać może zwykłych konsumentów właśnie na rynku wirtualnym, platformach sprzedażowych i zapewniających dostęp do różnych powszechnych usług np. Uber. Zjawiska te będą coraz częstsze i warto poświęcić im nieco uwagi. Ochrona konsumenta stanowi fundament europejskiego prawa cywilnego, a wszelkie obowiązki powinni w pierwszej kolejności ponosić przedsiębiorcy.

Ustawa o zwalczaniu nieuczciwej konkurencji wprowadza definicję czynu nieuczciwej konkurencji w art. 3 ust. 1, zgodnie z którym „czynem nieuczciwej konkurencji jest działanie sprzeczne z prawem lub dobrymi obyczajami, jeżeli zagraża lub narusza interes innego przedsiębiorcy lub klienta.", a powyższa definicja jest uzupełniana o ust. 2 gdzie czytamy, że „czynami nieuczciwej konkurencji są w szczególności: wprowadzające w błąd oznaczenie przedsiębiorstwa, fałszywe lub oszukańcze oznaczenie pochodzenia geograficznego towarów albo usług, wprowadzające w błąd oznaczenie towarów lub usług, naruszenie tajemnicy przedsiębiorstwa, nakłanianie do rozwiązania lub niewykonania umowy, naśladownictwo produktów, pomawianie lub nieuczciwe zachwalanie, utrudnianie dostępu do rynku, przekupstwo osoby pełniącej funkcję publiczną, a także nieuczciwa lub zakazana reklama, organizowanie systemu sprzedaży lawinowej, prowadzenie lub organizowanie działalności

w systemie konsorcyjnym oraz nieuzasadnione wydłużanie terminów zapłaty za dostarczane towary lub wykonane usługi". Z powyższej definicji jasno wynika, że katalog czynów nieuczciwej konkurencji pozostaje otwarty. Pogląd ten jest również powszechnie przyjmowany w doktrynie.[125] Chciałbym bardzo krótko przeanalizować jednak każdy z wymienionych, a potencjalnie groźnych, przykładowych czynów nieuczciwej konkurencji w świetle zagrożeń jakie może nieść za sobą korzystanie z samouczących się algorytmów SI oraz ich konsekwencji w zakresie odpowiedzialności odszkodowawczej.

Pierwszy z czynów to wprowadzające w błąd oznaczenie przedsiębiorstwa. W tym zakresie zagrożenie ze strony SI jest spore. Algorytm bez żadnych zabezpieczeń może z łatwością wpaść na pomysł wykorzystania materiałów innego przedsiębiorstwa, które zmieni tylko w minimalnym zakresie. Dojdzie do takiego wniosku poprzez analizę danych takich jak m. in. obroty innego przedsiębiorstwa, dostępne badania rynku oraz reakcji człowieka. Dostrzeże w ten sposób, że ludzie często nie sprawdzają dokładnie prezentowanych im marek, polegając jedynie na krótkich, wstępnych sygnałach. Dla konsumentów takie działanie może być bardzo groźne, gdyż będą nabywać usługi i produkty, które w ich mniemaniu mają określoną jakość i prestiż. W takiej sytuacji wobec konsumenta zastosowanie będą mogły znaleźć regulacje dotyczące rękojmi za wady produktu, ponieważ będą one różnić się w swoich właściwościach od produktów oryginalnych, których właściwości są powiązane z daną marką np. wykorzystanie oznaczenia przedsiębiorstwa powiązanego z wytwarzaniem produktów naturalnych zawiera w sobie niejako zobowiązanie, że oferowane produkty nie są produkowane w sposób sztuczny. Oprócz tego w razie powstania szkody konsument może korzystać z zasad odpowiedzialności wynikających z postanowień umowy zawartej z przedsiębiorcą, konsumenckiego prawa do odstąpienia od umowa, a także odpowiedzialności deliktowej z art. 415 KC. Należy zatem algorytmy SI w tym zakresie blokować, a przynajmniej dołożyć należytej staranności np. poprzez uniemożliwienie im zmiany treści reklam. Pomiędzy przedsiębiorcami odpowiedzialność może kształtować się w dwóch płaszczyznach. W pierwszej kolejności będzie to odpowiedzialność kontraktowa, wynikająca z umowy zawartej pomiędzy przedsiębiorcą naruszającym i zewnętrzną firmą dostarczającą oprogramowanie SI wykorzystane przy kształtowaniu oznaczenia przedsiębiorstwa. Konkretny jej zakres zależy od samej treści umowy, natomiast w wielu sytuacjach stworzenie

[125] Zob. K. Jasinska, J. Szwaja [w:] red. J. Szwaja, *„Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz."*, Warszawa 2019, wyd. 5, nb 5, Legalis

oznaczenia nowego, odróżniającego od innych przedsiębiorstw będzie jednym z głównych elementów treści umowy. Druga płaszczyzna to odpowiedzialność deliktowa polegająca na naruszeniu interesu innego przedsiębiorcy poprzez wprowadzenie jego klientów w błąd w ten sposób, że kupili inne produkty będąc przekonanym, że są to produkty oryginalne. W takiej sytuacji odpowiedzialność opiera się o art. 415 KC i zasadę winy, ponieważ o oznaczeniu przedsiębiorstwa w sposób zaproponowany przez SI ostatecznie decyduje człowiek. Wina polegać będzie m. in. na niezbadaniu oznaczeń na danym rynku geograficznym i produktowym oraz niewłaściwym przygotowaniu bazy, z której SI mogła korzystać. Gdyby takie czynności zostały podjęte to można byłoby mówić o zachowaniu się w sposób adekwatny do sytuacji, w związku z czym obiektywny miernik staranności został zachowany i nie można zarzucić danej osobie, że nie podjęła środków wystarczających do tego, aby uniknąć naruszenia prawa.

Bardzo podobnym, ale jeszcze groźniejszym czynem nieuczciwej konkurencji jest wskazane w art. 8 ustawy fałszywe oznaczenie pochodzenia towarów lub usług. O ile bowiem w przypadku niewłaściwego oznaczenia przedsiębiorstwa konsument jest w stanie, przy zachowaniu odpowiedniej uwagi, połapać się w próbie wprowadzenia go w błąd, o tyle w przypadku oznaczenia produktu jako pochodzącego z danego kraju np. sera mozzarella jako pochodzącego z Włoch, pomimo wyprodukowania go z mleka krowiego w Polsce, szansa na zorientowanie się przez przeciętnego konsumenta w oszustwie będzie niewielka. Tego typu naruszenia są wyszczególnione w art. 9, gdzie chroni się kwalifikowane oznaczenia geograficzne i chronione nazwy pochodzenia, a więc produkty wytwarzane tylko i wyłącznie na określonym obszarze, odpowiednio certyfikowane. Równie niebezpieczne co niewłaściwe oznaczenie pochodzenia towaru jest wprowadzenie w błąd co do innych aspektów produktu jak jakość, sposób wykonania, użyte materiały, marka itp. To naruszenie zostało uregulowane w art. 10 i również jest trudne do uchwycenia dla przeciętnego konsumenta. Bardzo widoczne jest to np. w zakresie podrabiania odzieży, gdzie podrabiane są nawet metki poszczególnych produktów, a odróżnienie oryginału od podróbki wymaga sporej wiedzy. Wszystkie tego typu naruszenia mogą być dokonywane przez algorytmy SI, które nie otrzymają odpowiednich blokad, gdyż jest to bardzo dobry sposób na maksymalizację zysku przedsiębiorstwa. W tym zakresie moim zdaniem odpowiedzialność kształtuje się w taki sam sposób jak powyżej – różnica dotyczy przedmiotu oznaczenia, w związku z tym przy odpowiedzialności kontraktowej będzie badana treść umowy w tym właśnie zakresie, a przy delikcie wina w odniesieniu do wybranego

systemu SI i sposobu weryfikacji rynku pod kątem tych produktów. We wszystkich powyżej przedstawionych sytuacjach odpowiedzialność odszkodowawcza będzie się w bardzo dużym zakresie opierać o utracone korzyści – wynikające z tego, że konsumenci zamiast oryginalnych produktów zakupili ich podróbki.

Ochrona tajemnicy przedsiębiorstwa i przejmowanie pracowników oraz klientów, a także będące w tym związku naruszenie ochrony danych osobowych to bardzo istotne zagrożenia ze strony algorytmów SI. Programy tego typu będą korzystać ze wszystkich mających dla nich znaczenie informacji, do jakich uzyskają dostęp. Ponadto istnieje ryzyko wymiany informacji danego przedsiębiorstwa przez algorytmy SI, zupełnie poza świadomością podmiotów, które się nimi posługują. Jest to także ryzyko naruszenia przepisów prawa antymonopolowego. Podstawowym zabezpieczeniem przed tego typu sytuacjami będzie uniemożliwienie algorytmom SI wymiany informacji z innymi tego typu programami. Co prawda nie daje to całkowitej gwarancji, gdyż może dojść do wymiany pośredniej albo zwyczajnie obejścia takich zabezpieczeń, jest to jednak istotny krok w kierunku redukcji ryzyka. Również w tej sytuacja podstawy odpowiedzialności wynikać będą zarówno z umowy pomiędzy dostawcą oprogramowania, a podmiotem, który się nim posługuje, jak również powstaną na gruncie odpowiedzialności deliktowej. Odpowiedzialność kontraktowa zależy od treści umowy, w szczególności w odniesieniu do tego jak ukształtowano odpowiedzialność między podmiotami za nieprawidłowe działanie systemu. Z kolei odpowiedzialność deliktowa pomiędzy naruszycielem a poszkodowanym wynikać będzie z art. 415 KC. Winę będzie można przypisać w przypadku niewłaściwego nadzoru nad systemem SI, w szczególności tego z jakich danych korzysta, posłużenia się programem bez wystarczających zabezpieczeń oraz w przypadku niezapewnienia odpowiedniej ochrony danych, które następnie stanowią bank wiedzy SI.

Czyn naśladownictwa, polegający na kopiowaniu produktów innych przedsiębiorców jest o tyle groźny, że SI nie tłumaczy się z działań, jakie podejmuje. Może zatem dojść do sytuacji, w której algorytm komunikując się z inną SI albo przeglądając bazy produktów w Internecie, dojdzie do wniosku, że taki produkt z powodzeniem będzie się sprzedawać przez przedsiębiorstwo, które z SI korzysta. Przygotuje więc innowacyjny, świetnie sprzedający się produkt. Jednak w żadnym razie nie poinformuje o tym, że to nie on jest jego pomysłodawcą. O ile zatem dysponent SI nie zweryfikuje tych informacji (czasem wyśledzenie oryginału może być niemożliwe, gdyż człowiek nie dysponuje taką mocą obliczeniową jak SI) dojdzie do wypuszczenia

produktu będącego naśladownictwem produktu innego przedsiębiorcy. Również w tym przypadku odpowiedzialność kontraktowa wnika z umowy pomiędzy przedsiębiorcą a dostawcą systemu SI. Z kolei odpowiedzialność deliktowa kształtowana przez art. 415 KC wystąpi w sytuacji, w której przy sprawdzaniu zaproponowanego przez SI produktu przedsiębiorca nie dołożył należytej staranności przy weryfikacji produktów istniejących na rynku oraz jeżeli skorzystał ze SI o nieadekwatnym poziomie zaawansowania np. program co prawda potrafi proponować nowe produkty, jednak nie zapewniono przy tym procesie weryfikacji zaproponowanego produktu z baza produktów innych przedsiębiorców. Będzie to więc również badanie winy w wyborze odpowiedniego oprogramowania.

Rozpowszechnianie informacji nieprawdziwych i wprowadzających w błąd może trochę przypominać sytuację manipulowania cenami akcji na giełdzie, co obecnie jest powszechnym problemem związanym ze SI. Co więcej, może być nawet elementem tej manipulacji. Problem jest jednak znacznie szerszy. Dotyczy on nie tylko giełdy, ale także drobnych przedsiębiorców. Takie działanie może czasem być trudne do wykrycia np. kiedy silniejsza SI będzie w stanie zmanipulować słabszą SI danego przedsiębiorcy i wtedy on sam będzie działać na swoją szkodę, publikując dane ze zmienionej przez SI rywala bazy danych. Potencjalnych zagrożeń z tym związanych jest bardzo wiele, a zmniejszenie ryzyka ich wystąpienia jest trudne. W takiej sytuacji roszczenia kontraktowe wynikają z treści umowy, w szczególności obowiązku zapewnienia przez twórcę oprogramowania stałego aktualizowania bazy danych i monitorowania informacji nieprawdziwych. Odpowiedzialność deliktowa jest już trudniejsza do wykazania, ponieważ w przypadku włączenia się w proces manipulacji innej, silnej SI, może dojść do przerwania łańcucha związku przyczynowego – w obecnych czasach silna SI nie istnieje, w związku z czym jej ingerencja w systemy nie będzie uznana za normalne następstwo danego działania, bo obiektywnie taka sytuacja nie była przewidywalna w takim stopniu, który uzasadniałby podjęcie odpowiednich kroków. Przy informacjach nieprawdziwych największe pole do udowadniania winy jest oczywiście w obszarze kontroli i monitoringu bazy danych, której SI używa. W przypadku niewłaściwego i niewystarczającego nadzoru nad taką bazą dojdzie do spełnienia przesłanek odpowiedzialności deliktowej.

Bardzo groźnym czynem nieuczciwej konkurencji jest wskazane w art. 15 utrudnianie dostępu do rynku. W przypadku SI jest to spory problem, gdyż wiąże się on z platformami sprzedażowymi. SI operująca na takich platformach według tylko sobie wiadomego klucza wyświetla poszczególne

produkty w pewnej ustalonej kolejności. Oczywiście sortowanie według ceny czy ocen problem ten rozwiązuje, jednak przed zmianą systemu sortowania zawsze dostajemy pierwszą listę uszeregowaną w tajemniczy dla nas sposób. Może też dojść do sytuacji, w której SI z jakiegoś powodu postanowi albo całkowicie usunąć z listy wyników produkty danej marki, albo przesunie je na sam koniec listy. Dlaczego? Bo uzna, że są brzydkie, bo często są zwracane, bo firma ma negatywne opinie. Takie sprawy pojawiają się za granicą coraz częściej i należy spodziewać się w najbliższych miesiącach i latach pierwszych decyzji organów regulacyjnych w tym zakresie. Dostawca takich usług jak np. w Polsce Allegro.pl powinien być neutralny wobec podmiotów, które umieszczają tam swoje produkty. Niemniej jednak kiedy w pole wyszukiwania wpiszemy prostą frazę np. „laptop" to ciężko doszukać się na początkowych stronach produktów marek mało popularnych. Rozwiązanie tego problemu dla programistów jest bardzo trudne, głównie dlatego, że oni sami nie wiedzą w jaki sposób SI podejmuje poszczególne decyzje. Dopóki zatem nie dojdzie do opracowania algorytmów, które tłumaczą swój sposób myślenia (a szybko to nie nastąpi) ryzyko przedsiębiorców jest spore. Jeszcze większy problem występuje w przypadku platform sprzedażowych jak Amazon, gdzie oprócz produktów zewnętrznych są oferowane także produkty właściciela tej platformy. W przypadku takich naruszeń podstawą są zapisy umowne, które determinują warunki oferowania i prezentowania produktów na danej stronie internetowej. Z kolei odpowiedzialność deliktowa z art. 415 KC wymagać będzie udowodnienia, że przedsiębiorca pomimo posiadanej wiedzy o funkcjonowaniu algorytmu w przedstawiony powyżej sposób nic z tym nie zrobił, samemu wprowadził takie możliwości do programu bądź zaniechał przeprowadzania kontroli nad tym w jaki sposób algorytm się rozwija. Jeżeli stały nadzór jest sprawowany w sposób prawidłowy to takie nietypowe zjawiska z pewnością zostaną wykryte i będzie można im zapobiegać.

Kolejne ryzyko to nieuczciwa reklama z art. 16, a szczególnie reklama porównawcza. W braku odpowiednich zabezpieczeń SI w celu maksymalizacji zysku w sposób naturalny będzie starała się na wszelkie sposoby eliminować konkurencję. Nie chodzi tutaj nawet o reklamę fałszywą, ale taką, która wprost krytykuje produkty konkretnego rywala. Nie ma tutaj znaczenia to, czy krytyka ta jest słuszna czy nie. Równie groźna jest reklama wprowadzająca klienta w błąd np. poprzez przekazywanie tylko informacji wygodnych dla sprzedawcy. Również w tym zakresie pole do nadużyć ze strony algorytmów SI jest bardzo duże. Tutaj także podstawa z art. 415 wymaga udowodnienia niewłaściwego nadzoru zarówno nad samą działalnością SI, jak również nad

jej produktami. Każda reklama powinna być przed jej upublicznieniem zweryfikowana pod kątem ryzyka porównawczej argumentacji.

Ostatnim szczególnie groźnym z wymienionych w ustawie czynów jest organizowanie systemu sprzedaży lawinowej. Dla dysponenta SI sposób wypracowania zysków przez algorytm często będzie pozostawać tajemnicą. Kluczowe będą jedynie wpływy i ilość sprzedanych produktów czy usług, a nie to w jaki sposób doszło do osiągniecia ich wysokości. Rodzi to więc ryzyko organizowania systemów sprzedaży lawinowej, które nie będą podlegać wyjątkom przewidzianym w art. 17c ust. 2 a więc:

- korzyści materialne uzyskiwane z uczestnictwa w systemie sprzedaży pochodzą ze środków uzyskiwanych z zakupu lub ze sprzedaży dóbr i usług po cenie, której wartość nie może rażąco przekraczać rzeczywistej wartości rynkowej tych dóbr i usług;
- osoba rezygnująca z udziału w systemie sprzedaży ma prawo do odprzedaży organizatorowi systemu za co najmniej 90% ceny zakupu wszystkich nabytych od organizatora nadających się do sprzedaży towarów, materiałów informacyjno-instruktażowych, próbek towarów lub zestawów prezentacyjnych zakupionych w przeciągu 6 miesięcy poprzedzających datę złożenia rezygnacji organizatorowi systemu sprzedaży.

Należy więc mieć na uwadze konieczność wprowadzenia odpowiednich mechanizmów w celu zwolnienia się z ewentualnej odpowiedzialności, jeśli SI postanowi korzystać z systemu sprzedaży lawinowej. W takiej sytuacji odpowiedzialność deliktowa z art. 415 KC wymaga udowodnienia niewłaściwego nadzoru nad systemem SI – po raz kolejny najważniejsze jest weryfikowanie przygotowywanych przez nią produktów czy ofert. Problem ten jest oczywiście często niemożliwy do zidentyfikowania na początku działalności algorytmu, jednak systematyczna kontrola oraz badanie tego, co przez SI zostało przygotowane będzie w mojej ocenie wystarczające do tego, aby uwolnić się od odpowiedzialności. Jeżeli po przeprowadzaniu odpowiedniej analizy, którą obiektywnie specjalista w danej dziedzinie uzna za wystarczającą, dojdzie mimo wszystko do naruszenia interesów osób trzecich poprzez funkcjonowanie systemu SI, to w mojej ocenie nie można przypisać temu podmiotowi winy, ponieważ uczynił on wszystko co było możliwe, aby zapobiec naruszeniom.

Wszystkie powyższe sytuacje należy jeszcze uzupełnić o analizę odpowiedzialności na zasadzie ryzyka. Wszystko zależy od tego jak zakwalifikujemy dany system SI. Jak pisałem powyżej SN nie zdecydował się na uznanie, że energia elektryczna uzasadnia przyjęcie odpowiedzialności za ruch

przedsiębiorstwa napędzanego siłami przyrody. Pogląd ten uważam za trafny jedynie w części. Istota wprowadzenia tego uregulowania sprowadza się bowiem do tego, że zdaniem ustawodawcy pewne urządzenia generują tak duże ryzyko, że odpowiedzialność na zasadzie winy nie będzie wystarczająco chronić potencjalnych poszkodowanych, a równocześnie nie będzie wystarczająco motywować przedsiębiorców do stosowania adekwatnych środków zabezpieczeń. W przypadku SI możemy mieć do czynienia z dwoma sytuacjami – z ryzykiem, które uznamy za niewielkie oraz z wysokim ryzykiem. Trafnie zwraca na to uwagę komitet ds. prawnych UE w swoich propozycjach regulacyjnych. Zastosowanie zatem przepisów o odpowiedzialności na zasadzie ryzyka będzie moim zdaniem wynikać nie z samego faktu zastosowania w przedsiębiorstwie SI, ale z tego, czego dotyczy prowadzona działalność i przy jakich czynnościach SI będzie wykorzystywana. Jeżeli zatem SI ma służyć do obsługi rejestracji użytkowników na giełdzie, to przepis ten nie znajdzie zastosowania, ponieważ ryzyko wiążące się z rejestracją nie ma bezpośredniego przełożenia na dokonywane transakcje. Jeżeli natomiast przedsiębiorca korzysta przy obsłudze giełdy z systemu SI, który ma możliwość obrotu akcjami, to ryzyko manipulacji giełdowej jest spore, w konsekwencji może znaleźć zastosowanie odpowiedzialność na zasadzie ryzyka. Oczywiście jeżeli już dojdzie do zakwalifikowania przedsiębiorcy jako korzystające z systemu SI stwarzającego duże ryzyko, a zatem można będzie powyższą regulację zastosować, konieczne jest zawsze przeanalizowanie przesłanek negatywnych, w szczególności dotyczącej ingerencji osób trzecich.

Powyższa analiza ma uświadomić czytelnika jak wiele groźnych sytuacji może wywoływać korzystanie z algorytmów SI bez odpowiedniego przygotowania kodu od strony prawnej. Czyny nieuczciwej konkurencji są szczególnie istotne, gdyż dotykają konsumentów, osób prywatnych, a natknąć możemy się na nie w toku zwykłych czynności. Z kolei zaburzenie równowagi konkurencji na rynku może prowadzić do obniżenia jakości towarów połączonej ze wzrostem cen, w skrajnej sytuacji ustalanych przez podmiot mający status monopolisty.

6. Projekt Rozporządzenia Unii Europejskiej w sprawie odpowiedzialności odszkodowawczej za czyny SI[126,]

6. 1. Motywy

Kiedy niniejsza praca była już właściwie ukończona miało miejsce przełomowe wydarzanie - komitet ds. prawnych UE opublikował 4 maja 2020 roku rekomendacje zawierające projekt przepisów regulujących odpowiedzialność deliktową SI. Jest to znaczący krok naprzód w zakresie regulacji prawnej SI, będący następstwem przygotowanej w lutym 2020 roku „Białej Księgi dla Sztucznej Inteligencji"[127], tym bardziej istotny, że UE przedstawiła propozycje bardzo konkretne, a w mojej ocenie, także w zdecydowanej większości trafne i odpowiadające temu, czego, zarówno prawnicy jak i przedsiębiorcy, mogli oczekiwać.

Przedstawiona propozycja wynika z zastosowania art. 47 Regulaminu Parlamentu Europejskiego, zgodnie z którym Parlament może zwrócić się do Komisji o „przedłożenie wszelkich stosownych wniosków mających na celu przyjęcie nowego lub zmianę istniejącego aktu prawnego", a zatem będzie ona jeszcze przedmiotem analizy Komisji Europejskiej, a następnie Parlamentu Europejskiego i Rady Unii Europejskiej. Warto jednak wskazać, że już w tym momencie stanowisko UE jest jednoznaczne – wprowadzane regulacje muszą mieć charakter Rozporządzenia. Rozwiązanie to należy ocenić jako słuszne, ponieważ przyczyni się ono do jednolitego stosowania przygotowanych przepisów we wszystkich krajach UE, co jest o tyle istotne, że pozytywnie wpłynie na jakość produkowanego i stosowanego oprogramowania, konkurencję na rynku oraz bezpieczeństwa użytkowników systemów SI.

W motywach do proponowanej regulacji wskazano, że zasady odpowiedzialności odszkodowawczej spełniają zasadniczo dwa główne cele – z jednej strony stanowią gwarancję, że strona poszkodowana będzie miała możliwość otrzymania rekompensaty za poniesione straty, zarówno materialne jak i fizyczne, a z drugiej strony jest to czynnik motywujący przedsiębiorców do

[126] Opracowane na podstawie „Draft Report with recommendations to the Commission on a Civil liability regime for artificial intelligence", (2020/2014(INL)), Committee on Legal Affairs, https://www.europarl.europa.eu/doceo/document/JURI-PR-650556_EN.pdf (dostęp: 17.05.2020); Poniższy rozdział stanowi rozwinięcie artykułu dotyczącego tożsamego zagadnienia, który pojawi się na blogu kancelarii traple.pl, jednak na dzień oddania pracy (27.05.2020) nie jest jeszcze opublikowany. W niniejszym rozdziale wprost wykorzystane zostały jedynie przygotowane przez mnie tłumaczenia przepisów

[127]

postępowania zgodnie z określonymi zasadami i z dochowaniem należytej staranności, a więc stanowią czynnik prewencyjny. Słusznie wskazuje się także, że pomimo istniejących wad związanych ze stosowaniem SI, jej zalet jest znacznie więcej – SI pomaga m. in. w procesach medycznych oraz przyczynia się do walki ze zmianami klimatycznymi. Ponadto UE zwraca uwagę, że obecnie jedynie niektóre systemy SI stanowią potencjalnie duże zagrożenie dla społeczeństwa, natomiast większość takich systemów stosowana jest do wykonywania prostych zadań. Wprowadzenie regulacji wymuszają dwa główne czynniki – fakt, że SI nie ma osobowości prawnej, a w konsekwencji własnego majątku, w związku z czym sama nie może odpowiadać, a po drugie, istnieją jednak systemy SI stwarzające duże ryzyko, którego nie można przewidzieć, co więcej, z powodu procesu uczenia maszynowego, autonomii systemu oraz skomplikowania technologicznego SI trudno jest ustalić, jakie czynniki doprowadziły do powstania szkody. Ten niemożliwy do prześledzenia fragment procesu działania SI określony został jako „black box element". Dodatkowo SI może działać niepoprawnie z uwagi na ingerencję w jej oprogramowanie w wyniku coraz częstszych naruszeń cyberbezpieczeństwa systemów, których sprawców ciężko wyśledzić. Wszystkie te czynniki sprawiają, że udowodnienie winy operatora SI może być niemożliwe, a w konsekwencji osoba poszkodowana nie będzie w stanie otrzymać należnego jej odszkodowania.

Konsekwencją wskazanych powyżej czynników jest konieczność utworzenia systemu odpowiedzialności za SI w oparciu o dwa modele – zwykłe systemy SI oraz systemy SI wysokiego ryzyka, które odpowiednio opierają się na odpowiedzialności na zasadzie winy (z jej domniemaniem) oraz na zasadzie ryzyka. UE wskazuje, że odpowiedzialność za SI jest zbliżona do odpowiedzialności za pojazd lub zwierzę. Proponowane regulacje wynikają z przyjęcia słusznej tezy, że odpowiadać powinien ten, kto stwarza określone ryzyko dla społeczeństwa. Ponadto UE wskazuje na konieczność wprowadzenia obowiązkowych ubezpieczeń dla systemów SI wysokiego ryzyka. Dodatkowo, w ślad za propozycjami przedstawionymi w „Białej Księdze", wskazuje się na konieczność utworzenia mechanizmu dobrowolnej certyfikacji SI - „System opierałby się na procedurach oceny zgodności w UE, zob. decyzja 768/2008/WE lub rozporządzenie (UE)2019/881 (akt o cyberbezpieczeństwie), z uwzględnieniem specyfiki sztucznej inteligencji, zob. Niebieski przewodnik –wdrażanie unijnych przepisów dotyczących produktów, 2014 r".[128]

[128] *Ibidem*, s. 27; „*Draft report…*", s. 14.

Proponowana regulacja dotyczy tylko odpowiedzialności podmiotów wdrażających SI i tylko w zakresie szkód na zdrowiu i życiu danej osoby oraz jej własności. W związku z tym UE wskazuje na konieczność dostosowania obecnych regulacji wynikających z Dyrektywy o produktach wadliwych[129] w zakresie odpowiedzialności producenta, wytwórcy (*manufacturer*), operatora końcowego (*backend operator*) i programistów (*developer*).

6. 2. Zakres stosowania

Po przedstawieniu motywów jakie towarzyszyły prawodawcy unijnemu przy tworzeniu projektu regulacji można przejść do treści zaproponowanych przepisów. W artykule 2 wskazuje się na zakres regulacji – dotyczy ona zdarzeń wywołujących szkodę, mających miejsce na terytorium UE. Ponadto zgodnie z ustępem 2 wyłączenie odpowiedzialności wynikającej z proponowanej regulacji w drodze umowy pomiędzy wdrażającym a poszkodowanym (zarówno osobą fizyczną jak i prawną) jest nieważne, niezależnie od tego, czy zawarcie takiej umowy miało miejsce przed czy po zdarzeniu powodującym szkodę. Takie rozwiązanie oceniam jako słuszne, bo już na wstępie uniemożliwia ono wszelkie próby obchodzenia przepisów i wykorzystanie ewentualnej niewiedzy poszkodowanego.

W art. 3 znajduje się słowniczek pojęć, a co najbardziej istotne, UE zdecydowała się na utworzenie definicji legalnej SI oraz powiązanych z tą definicją określeń. Propozycje te przedstawiają się w następujący sposób:

- '**system SI**' oznacza system, który wykazuje inteligentne zachowanie poprzez analizę pewnych danych wejściowych i podejmowanie działań, z pewną dozą autonomii, w celu osiągnięcia określonych celów. **Systemy SI** mogą być oparte wyłącznie na oprogramowaniu, działając w wirtualnym świecie lub mogą być osadzone w urządzeniach sprzętowych[130]
- '**autonomiczny**' oznacza system SI, który działa poprzez postrzeganie określonych danych wejściowych i bez konieczności postępowania zgodnie z zestawem wcześniej ustalonych instrukcji, pomimo swojego zachowania

[129] Dyrektywa Rady z dnia 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe

[130] AI-system means a system that displays intelligent behaviour by analysing certain input and taking action, with some degree of autonomy, to achieve specific goals. AI systems can be purely software-based, acting in the virtual world, or can be embedded in hardware devices

będąc ograniczonym przez cel, który został wyznaczony, i inne istotne wybory projektowe dokonane przez jej dewelopera[131]

- '**wysokie ryzyko**' oznacza znaczny potencjał w autonomicznie działającym systemie SI do wyrządzenia krzywdy lub szkody jednej osobie lub większej liczbie osób w sposób losowy i niemożliwy do przewidzenia z góry; znaczny potencjał zależy od wzajemnego oddziaływanie między skalą możliwej krzywdy lub szkody, prawdopodobieństwem, że ryzyko dojdzie do skutku i sposobem użycia systemu SI[132]

Powyższe definicje posługują się wieloma pojęciami nieostrymi, jednak należy uznać je za dobrą propozycję. Uwzględniają one bowiem cechy charakterystyczne dla SI takie jak dane wejściowe, wykazywanie zachowania inteligentnego, możliwość działania w sposób autonomiczny oraz oparcie systemu zarówno w urządzeniu fizycznym (hardware) jak i w postaci czystego oprogramowania (software). Definicja SI oraz autonomiczności wydaje się być najbliższa metodzie uczenia ze wzmocnieniem, jednak z uwagi na wymóg zdefiniowania celu nie uwzględnia w mojej ocenie metody uczenia nienadzorowanego, gdzie niekiedy może nie istnieć żaden określony cel. Systemy SI wysokiego ryzyka nie zostały zdefiniowane w sposób umożliwiający jednoznaczną ich identyfikację, jednak nie jest to konieczne, ponieważ będą one wymienione w sposób wyczerpujący w załączniku do Rozporządzenia, który z kolei będzie monitorowany i dostosowywany co 6 miesięcy.

Kolejna istotna definicja ma charakter podmiotowy – określa ona bowiem kogo rozumie się pod pojęciem wdrażającego, a zatem kto odpowiada na podstawie niniejszej regulacji:

- „**wdrażający**" oznacza osobę, która decyduje o użyciu systemu SI, sprawuje kontrolę nad powiązanym ryzykiem i czerpie korzyści z jego działania[133]

W mojej ocenie przedstawiona definicja może wywoływać uzasadnione wątpliwości co do tego jak odróżnić użytkownika systemu SI od wdrażającego

131 autonomous means an AI-system that operates by perceiving certain input and without needing to follow a set of pre-determined instructions, despite its behavior being constrained by the goal it was given and other relevant design choices made by its developer

132 high risk means a significant potential in an autonomously operating AI-system to cause harm or damage to one or more persons in a manner that is random and impossible to predict in advance; the significance of the potential depends on the interplay between the severity of possible harm or damage, the likelihood that the risk materializes and the manner in which the AI-system is being used

133 deployer means the person who decides on the use of the AI-system, exercises control over the associated risk and benefits from its operation

– w motywie 9 wskazuje się, że „jeżeli użytkownik, a mianowicie osoba korzystająca z systemu AI, bierze udział w zdarzeniu szkodliwym, powinna on ponosić odpowiedzialność na podstawie niniejszego rozporządzenia tylko wtedy, gdy użytkownik kwalifikuje się również jako wdrażający”[134]. Przykładowo osoba korzystająca z autonomicznej kosiarki w mojej ocenie decyduje o użyciu systemu SI, sprawuje – większą bądź mniejszą – kontrolę nad tym urządzeniem, w konsekwencji nad ryzykiem, a także czerpie korzyści z działania tego urządzenia – definicja nie wskazuje, że mają to być korzyści finansowe lub psychiczne, związane z komfortem życia, a także, czy są to korzyści bezpośrednie lub pośrednie. W konsekwencji w mojej ocenie definicja powyższa wymaga modyfikacji np. poprzez wprowadzenie rodzaju osiąganych korzyści np. sprzedaż urządzenia wyposażonego w system SI takiego jak autonomiczna kosiarka lub inteligentna lodówka.

6. 3. Odpowiedzialność na zasadzie ryzyka

Zakres odpowiedzialności za systemy SI wysokiego ryzyka regulują przepisy Rozdziału II (art. 4 – 7). Zgodnie z tymi regulacjami systemy SI wysokiego ryzyka wskazuje się w załączniku do Rozporządzenia w oparciu o sektor, w jakim korzysta się ze SI oraz rodzaj tego systemu. Załącznik ten będzie odpowiednio aktualizowany w formie aktów delegowanych, a wprowadzane zmiany wchodzić będą w życie po upływie 6 miesięcy. Wdrażający system nie będzie mógł uwolnić się od odpowiedzialności argumentując, że dochował należytej staranności lub że szkoda powstała w wyniku autonomicznej działalności SI. Jedyna możliwość to powołanie się na siłę wyższą. Jest to zatem odpowiedzialność ukształtowana na zasadzie ryzyka.

Ponadto proponowane regulacje nakładają obowiązkowe ubezpieczenia w zakresie systemów SI wysokiego ryzyka, określając równocześnie kwoty tego ubezpieczenia - 10 mln EUR w przypadku krzywdy w postaci śmierci i naruszenia stanu zdrowia oraz 2 mln EUR w przypadku szkody dla przedmiotu własności, jednak w tym drugim przypadku odszkodowanie nie zostanie wypłacone, jeżeli jego wysokość byłaby niższa niż 500 EUR i równocześnie poszkodowany ma wobec wdrażającego roszczenie odszkodowawcze wynikające z odpowiedzialności kontraktowej.

[134] If a user, namely the person that utilises the AI-system, is involved in the harmful event, he or she should only be liable under this Regulation if the user also qualifies as a deployer

W obecnym kształcie wykaz systemów SI wysokiego ryzyka prezentuje się następująco:

System SI	Sektor krytyczny
Bezzałogowe statki powietrzne	transport
Pojazdy autonomiczne o poziomach 4 i 5 (zgodnie ze standardem SAE J3016)	transport
Autonomiczne systemy zarządzania ruchem	transport
Roboty autonomiczne	wsparcie
Autonomiczne urządzenia do czyszczenia miejsc publicznych	wsparcie

Katalog ten jest dość skromny, jednak UE wskazuje na konieczność jego monitoringu i odpowiedniej aktualizacji, zapewne także w momencie ustalenia ostatecznego brzmienia Rozporządzenia będzie on poszerzony. UE w motywach do Rozporządzenia wskazuje, że konieczny będzie bieżący kontakt z programistami, którzy będą informować UE o prowadzonych pracach nad nowymi systemami SI.

Projektowane przepisy wskazują także jakie czynniki należy uwzględnić przy określaniu wysokości odszkodowania – są to m. in. koszty leczenia, utracony zarobek, zakres alimentacji na rzecz osób, które zmarły miał obowiązek utrzymywać czy też koszty pogrzebu.

Okresy przedawnienia w zaproponowanych przepisach prezentują się w następujący sposób:

- 30 lat od dnia wystąpienia szkody w przypadku śmierci lub naruszenia zdrowia
- 10 lat od dnia wystąpienia szkody dla przedmiotu własności, jednak nie dłużej niż 30 lat od dnia uruchomienia systemu SI

Okresy przedawnienia roszczeń są więc bardzo długie i z pewnością będą miały wpływ na to, w jaki sposób ukształtuje się rynek ubezpieczeń od odpowiedzialności SI.

6. 4. Odpowiedzialność na zasadzie winy

Rozdział III (art. 8 – 9) projektowanego Rozporządzenia reguluje zasady odpowiedzialności za pozostałe systemy SI. Odpowiedzialność ta została ukształtowana w oparciu o zasadę winy, przy czym przepisy przewidują domniemanie tej winy, które może być obalone poprzez wykazanie, że:

- system SI został aktywowany bez wiedzy wdrażającego, a równocześnie podjęto wszystkie uzasadnione i niezbędne środki, aby uniknąć takiej aktywacji[135], lub
- zachowano należytą staranność, wybierając odpowiedni system SI dla właściwego zadania i wymaganych umiejętności, system SI został uruchomiony prawidłowo, monitorowano aktywność SI i utrzymanie niezawodności działania poprzez regularne instalowane wszystkich dostępnych aktualizacji[136]

Podobnie jak przy prezentowanej wcześniej odpowiedzialności za systemy SI wysokiego ryzyka także tutaj wdrażający nie może uwolnić się od odpowiedzialności argumentując, że szkoda wynikła z autonomicznej działalności SI, ale odpowiedzialność wyłącza wystąpienie siły wyższej. Ustęp 3 projektowanej regulacji przewiduje jednak pewien wyłom od zasady odpowiedzialności na zasadzie winy w sytuacji, w której dochodzi do ingerencji w system SI. Jeżeli bowiem w wyniku takiej ingerencji osoby trzeciej dojdzie do wyrządzenia szkody, a osoba ingerująca nie jest możliwa do wyśledzenia lub nie ma wystarczających środków do tego, aby zrekompensować poniesione przez poszkodowanego straty, odpowiedzialność ponosi wdrażający. Jest to więc odpowiedzialność podobna, lecz zmodyfikowana w innym kierunku, do występującej w kodeksie cywilnym odpowiedzialności z art. 428, której sens opiera się na założeniu, że skoro nie można uzyskać odszkodowania od osoby rzeczywiście odpowiedzialnej (w przypadku winy w nadzorze jest to sprawujący nadzór, a w przypadku SI sprawca włamania do systemu) to dochodzimy odszkodowania od kogoś innego (przy winie w nadzorze jest to osoba nadzorowana, natomiast w przypadku SI jest to osoba odpowiadająca za to, że system był nienależycie zabezpieczony). Regulacja ta wiąże się dla wdrażających ze sporym ryzykiem i nakłada na nich bardzo daleko idące obowiązki związane z zapewnieniem adekwatnego poziomu cyberbezpieczeństwa, jednak z drugiej strony pozostaje w zgodzie z zasadą, że ten kto korzysta z rozwiązania obarczonego pewnym stopniem ryzyka wystąpienia szkody powinien ponosić odpowiedzialność, jeżeli to ryzyko się zmaterializuje w postaci szkody. Niemniej jednak jest to pomysł kontrowersyjny i z pewnością UE poświęci mu sporo uwagi, co może prowadzić do pewnych modyfikacji tej zasady. W innym tłumaczeniu[137] powyższego przepisu druga przesłanka dotyczy

[135] the AI-system was activated without his or her knowledge while all reasonable and necessary measures to avoid such activation were taken, or

[136] due diligence was observed by selecting a suitable AI-system for the right task and skills, putting the AI-system duly into operation, monitoring the activities and maintaining the operational reliability by regularly installing all available updates

[137]

braku wystarczających środków na pokrycie odszkodowania, ale sytuacji, w której wykrycie osoby trzeciej byłoby nieproporcjonalnie kosztowne. Uważam to tłumaczenie za błędne przynajmniej z trzech powodów. Po pierwsze dosłowne tłumaczenie słowa „impecunious" oznacza ubogi, bez środków do życia. Po drugie, to wdrażający będzie w razie braku wykrycia sprawcy odpowiadać za szkodę, w związku z tym to on ponosi koszty zidentyfikowania takiej osoby czy organizacji, a w konsekwencji to on decydować będzie o tym, czy jakieś działania są uzasadnione z ekonomicznego lub wizerunkowego punktu widzenia. Po trzecie, cała regulacja unijna stwarza wrażenie, że chodzi o ochronę strony słabszej i zagwarantowanie jej ochrony. Jeżeli zatem przyjmiemy powyższe tłumaczenie, to w sytuacji, gdy uda się zidentyfikować daną osobę, ale nie będzie ona miała wystarczających środków do wypłaty odszkodowania, osoba poszkodowana pozostanie bez ochrony. W przypadku więc ważenia interesów i konieczności podjęcia decyzji, czy chronić należy osobę poszkodowaną czy też wdrażającego system SI, należy dojść do wniosku, że przy takim stanie faktycznym należy raczej przyjąć odpowiedzialność wdrażającego, gdyż to on ponosi ostatecznie ryzyko korzystania z systemu SI, nawet jeżeli szkoda powstała wskutek ingerencji osoby trzeciej, która jednak nie będzie w stanie zaspokoić roszczenia osoby poszkodowanej, i to roszczenia o charakterze krytycznym np. kwoty niezbędnej do leczenia.

Projektowane Rozporządzenie, aby umożliwić wdrażającym wykazanie braku winy wprowadza obowiązek współdziałania producentów systemów SI z wdrażającymi w takim zakresie, jaki jest niezbędny do wykazania braku winy. Konsekwencja tej regulacji będzie obowiązek wyznaczenia na terytorium UE przez podmioty spoza tego obszaru odpowiednich przedstawicieli, co w motywach do Rozporządzenia porównuje się do obowiązków wynikających obecnie z RODO[138]. W mojej ocenie takie rozwiązanie należy ocenić jako słuszne, jakkolwiek nie wiadomo jak ta współpraca będzie przebiegać w praktyce, bowiem niekiedy wykazanie braku winy wdrażającego może skończyć się odpowiedzialnością producenta systemu SI, co może stanowić czynnik utrudniający taką współpracę.

Zakres odszkodowania oraz terminy przedawnienia w stosunku do tego rodzaju systemów SI zależą już od regulacji przepisów prawa krajowego.

[138] Rozporządzenie Parlamentu Europejskiego 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)

6. 5. Podział odpowiedzialności

Rozdział IV (art. 10 – 12) dotyczy kwestii podziału odpowiedzialności. Zgodnie z tymi regulacjami w przypadku przyczynienia się przez poszkodowanego do powstałej szkody odpowiedzialność wdrażającego powinna być odpowiednio zmniejszona, a jeżeli jest to przyczynienie się o charakterze przeważającym lub wyłącznym, to odpowiedzialność zostanie wyłączona całkowicie. Jest to więc regulacja podobna do tej przewidzianej w art. 362 kodeksu cywilnego. Z kolei w przypadku wielu wdrażających system SI odpowiadają oni solidarnie, a jeżeli wdrażający jest także producentem, to pierwszeństwo ma odpowiedzialność wynikająca z tego Rozporządzenia. Regres został uregulowany podobnie do regulacji kodeksu cywilnego. Należy zatem wskazać, że Rozporządzanie uzależnia możliwość skorzystania z roszczenia regresowego dopiero po zaspokojeniu roszczeń poszkodowanego. Zakres roszczenia regresowego zależy od stopnia odpowiedzialności, natomiast jeżeli poszkodowany nie może uzyskać odszkodowania od jednego z dłużników solidarnych, to może z tym roszczeniem wystąpić do pozostałych. W przypadku wypłaty odszkodowania wdrażający może mieć roszczenie regresowo w stosunku do producenta, na zasadach wynikających z odpowiedzialności za produkty wadliwe. Z kolei w przypadku wypłaty ubezpieczenia ubezpieczyciel wstępuje we wszystkie prawa poszkodowanego w zakresie roszczeń cywilnych, wobec innych osób, wynikających z tej samej szkody.

6. 6. Podsumowanie

Podsumowując, uważam że proponowane regulacje w zdecydowanej większości można ocenić jako pozytywne, a ich wady zostały wykazane powyżej. W mojej ocenie największa z nich jest niejasna definicja wdrażającego, która jest kluczowa dla całej regulacji, ponieważ wskazuje na podmiot odpowiedzialny. Z kolei jako bardzo trafiony i adekwatny do specyfiki systemów SI należy ocenić pomysł podziału systemów SI na te wysokiego ryzyka i pozostałe systemy, który to podział uzupełnia się poprzez wyczerpujące wskazanie rodzajów systemów SI wysokiego ryzyka, których lista będzie na bieżąco aktualizowana. Podział odpowiedzialności na opartą o zasadę ryzyka w przypadku systemów SI wysokiego ryzyka oraz o zasadę winy, z jej domniemaniem, w przypadku innych systemów SI również uważam za adekwatny do tego jak oceniono ryzyko wynikające z danych typów SI. Jest to zresztą powiązane z prezentowanym przeze mnie poglądem, że odpowiedzialność na zasadzie

ryzyka powinna dotyczyć przedsiębiorców (bo to oni korzystają z systemów mogących stanowić większe ryzyko) zgodnie z regulacją art. 435 kodeksu cywilnego, jednak tylko przy uwzględnieniu stopnia tego ryzyka (oczywiście tylko w zakresie w jakim rozważamy, czy samo korzystanie z energii elektrycznej jest wystarczającą podstawą do zastosowania tego przepisu). Kontrowersje może budzić przepis obarczający odpowiedzialnością na zasadzie winy wdrażającego system SI, w przypadku, gdy szkoda została wyrządzona w wyniku ingerencji osoby trzeciej, od której jednak nie można uzyskać odszkodowania. W mojej ocenie ten wyjątek od odpowiedzialności na zasadzie winy, zmierzający w kierunku odpowiedzialności na zasadzie ryzyka, stanowi jednak zadowalający kompromis pomiędzy interesami poszkodowanego a wdrażającego, gdyż z powodów słusznościowych w przypadku kolizji – czy wypłacić odszkodowanie mimo braku winy, czy też pozostawić poszkodowanego bez odszkodowania – należy zdecydować się na pierwszy wariant, ponieważ skoro wdrażający stwarza potencjalne ryzyko, powinien za nie ostatecznie odpowiadać.

7. Wnioski i propozycje autora

Odpowiedzialność za działanie SI, zarówno w zakresie odpowiedzialności kontraktowej jak i deliktowej, jest nieprzystosowana do rzeczywistości, która zaczyna nas otaczać. Przedstawione w niniejszym opracowaniu próby uzasadnienia przypisania odpowiedzialności w określony sposób, zwłaszcza w zakresie odpowiedzialności deliktowej, są możliwe do zastosowania tylko w zakresie spraw nieskomplikowanych, gdzie udział różnych podmiotów nie jest bardzo złożony i trudny w ocenie. W sytuacjach, gdzie w procesie wytworzenia, uczenia i zastosowania SI bierze udział większa ilość podmiotów, a także gdzie algorytmy nie sprowadzają się do obsługi czynności prostych i masowych, zastosowanie powyższych propozycji będzie bardzo trudne. Ponadto jest to propozycja oparta o analogię i nakierowana na przedstawienie stanowiska, zgodnie z którym jakaś możliwość przypisania odpowiedzialności istnieje. Nie oznacza to, że sądy nie postanowią iść w swoim orzecznictwie w zupełnie innym kierunku.

Z tego względu wprowadzenie nowych regulacji dotyczących SI wydaje się być nieodzowne. To co cieszy i jest warte odnotowania to fakt, że w Polsce problem ten jest dostrzegany. Co prawda prac na temat SI w zakresie odpowiedzialności nie ma zbyt wiele (oprócz pracy prof. Chłopeckiego na ten moment są tylko dwie inne, które w sporej mierze odwołują się do tej pierwszej), to jednak pojawia się coraz więcej artykułów naukowych, a na studiach coraz

więcej osób decyduje się pisać swoje prace w oparciu o temat AI (odpowiedzialność, autonomiczne pojazdy, prawo autorskie, dane osobowe). Ponadto już w listopadzie 2018 roku Ministerstwo Cyfryzacji, na wezwanie Komisji Europejskiej, przygotowało krajowy plan strategii dot. SI, gdzie zdefiniowano podstawowe problemy w zakresie czterech obszarów: gospodarki opartej o dane, finansowania i rozwoju, edukacji oraz prawa i etyki.[139] W zakresie odpowiedzialności SI wnioski ekspertów również sprowadzają się do tego, że potrzebne są nowe regulacje, przy czym ich zdaniem obecne regulacje są praktycznie niemożliwe do zastosowania. Warto zauważyć, że jako rozwiązanie tymczasowe proponuje się dostosowanie obecnych przepisów o produkcie niebezpiecznym do istoty SI.[140] Odrzucana jest przy tym koncepcja nadawania osobowości prawnej SI i obciążanie odpowiedzialnością jej samej. To, czy nadanie SI osobowości prawnej jest słuszne czy nie stanowić mogłoby temat osobnej pracy, niemniej jednak należy wskazać, że taki zabieg generuje szereg innych problemów i zasadniczo powoduje przerzucenie ryzyka i konieczności dostosowania się do nowych obowiązków prawnych w inne miejsce. Bardzo istotnym postulatem jest konieczność zapewnienia transparentności w zakresie SI. W tym zakresie proponuje się:

- zapewnienie mechanizmów gwarantujących, że użytkownik wchodzący w kontakt z SI ma świadomość, że wchodzi w interakcję z SI (tj. że „po drugiej stronie" znajduje się AI);
- zapewnienie dostępu podmiotom zainteresowanym np. będących w sporze do algorytmów będących podstawą działania SI oraz mechanizmów zapewniających zrozumienie sposobu działania SI (proces decyzyjny);
- określenie zasad informowania użytkowników jak w razie potrzeby skontaktować się z człowiekiem oraz jak sprawdzić lub skorygować decyzje podjęte przez SI.[141]

Co do postulatu konieczności zrozumienia mechanizmów działania SI to jest to marzenie wielu programistów i obecnie wiele prac nad SI koncentruje się właśnie w zakresie transparentności procesu decyzyjnego, jednak

[139] https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=2ahUKEwjet7Of3M7nAhXqh4sKHfJqCQwQFjADegQIARAB&url=https%3A%2F%2Fwww.gov.pl%2Fdocuments%2F31305%2F436699%2FZa%25C5%2582o%25C5%25BCenia_do_strategii_AI_w_Polsce_-_raport.pdf&usg=AOvVaw0BHTcjLA_qao5pPnSdxLxM (dostęp: 5.02.2020).

[140] *Ibidem*, s. 131.

[141] *Ibidem*, s. 129.

osiągnięcie poziomu, gdzie SI pokazuje nam sposób w jaki działała jeszcze jest stosunkowo trudne do zrealizowania.

Natomiast konieczność identyfikacji algorytmu SI przed wejściem w interakcję z użytkownikiem jest postulatem bardzo słusznym i takie działanie na pewno będzie pożądane. Proponowałbym oparcie tego typu działalności o regulacje na wzór obowiązującego RODO, w zakresie w jakim konieczne jest wyrażenie zgody na przetwarzanie danych osobowych czy też przepisów o świadczeniu usług drogą elektroniczną, gdzie konieczne jest akceptowanie regulaminów sklepów internetowych. Podmiot posługujący się SI powinien mieć obowiązek poinformowania użytkownika na danej platformie (zawsze potrzebna nam jest wizualna część systemu do wejścia w interakcję) o tym, że cały proces obsługuje SI oraz konieczność zaznaczenia w sposób niebudzący wątpliwości, że użytkownik o tym wie i godzi się na takie działanie. Jest to oczywiście obciążanie konsumenta kolejnymi obowiązkami, jednak po takiej informacji konsument (czy nawet inny podmiot) ma szansę na ewentualne powzięcie wątpliwości i podjęcie decyzji o zmianie kontrahenta. Oczywiście jak w przypadku RODO czy plików cookies znowu dojdzie do zarzucania konsumenta ogromem informacji, jednak lepsze jest takie rozwiązanie niż pozostawianie go w niewiedzy i bez możliwości zdecydowania o tym, czy z tą ogromną ilościom informacji zechce się zapoznać. Problem robi się już bardziej złożony gdy po obu stronach występuje SI, jednak można ustawić algorytm w taki sposób, aby po otrzymaniu informacji, że przystępuje do kontraktowania z inną SI, wyłączył się on z transakcji albo poprosił o akceptację jego działania swojego zwierzchnika (człowieka). Co prawda spowalnia to cały proces ale może też eliminować potencjalne ryzyka.

W przywoływanym dokumencie pojawia się także postulat powołania wyspecjalizowanej instytucji zrzeszającej ekspertów z wielu różnych dziedzin celem analizowania sytuacji rozwoju SI, jej wykorzystania oraz wymaganych zmian legislacyjnych.[142] Postulat ten jest słuszny, aczkolwiek nie przyczyni się on na pewno do szybkiego dostosowania regulacji prawnych do otaczającej nas rzeczywistości. W związku z tym być może należy powołać nowy organ regulacyjny, tak jak np. KNF, którego zadaniem byłaby kontrola korzystania ze SI, wydawanie rekomendacji, składanie zawiadomień np. do UOKiK, utworzenie repozytorium kodów źródłowych, a może nawet powołanie przy takiej instytucji wyspecjalizowanego sądu, na wzór sądów arbitrażowych, które mogłyby rozstrzygać spory powstałe na gruncie SI. Jest to z kolei nowa

142 *Ibidem*, s. 128.

dawka obowiązków dla przedsiębiorców, uzasadniona jednak tym, że stosują oni nowości techniczne potencjalnie niebezpieczne dla całego rynku. Ważne jest jednak to, aby uwzględnić specyfikę danej dziedziny np. kod źródłowy podlega różnym zmianą na całym etapie programowania, algorytm musi przejść fazy testów opartych o nadzorowane uczenie maszynowe itp. Pamiętać bowiem należy, że zbyt drastyczne regulacje mogą zahamować innowacyjność.

W zakresie regulacji prawnych w systemie kontynentalnym, gdzie prawo zapisane jest tylko w aktach prawnych, najbardziej pożądane byłoby stworzenie definicji SI. Jak już wskazywałem na początku jest to zadanie bardzo trudne. Warto jednak spróbować skonstruować taką definicję, aby niniejsza praca miała wartość dodaną i mogła stanowić przedmiot konstruktywnej krytyki. W mojej ocenie całkiem dobra definicja mogłaby brzmieć tak: „Pod pojęciem sztucznej inteligencji rozumie się algorytm (kod źródłowy) uruchomiony na dowolnym urządzeniu w oparciu o dowolny system operacyjny, który posiada, nawet w minimalnym stopniu, możliwość podejmowania decyzji bez permanentnego nadzoru człowieka, na podstawie danych wejściowych dostarczonych bez względu na źródło ich pochodzenia." Definicja ta pozwala na nazwanie sztuczną inteligencją algorytmu bez względu na jego zewnętrzną postać czy sposób jego odtworzenia, obejmuje swoim zakresem zarówno nadzorowane jak i nienadzorowane uczenie maszynowe, wskazuje na swobodę decyzyjną algorytmu, a także konieczność podejmowania decyzji na podstawie danych wprowadzanych do niej nie tylko przez człowieka, ale także zbieranych autonomicznie. Definicja ta nie rozdziela jednak algorytmów na tzw. silną i słabą SI, co stanowi jej istotną wadę. Obecnie jednak brak jest algorytmów, które będzie można z pełną odpowiedzialnością przyporządkować do kategorii silnej SI, a perspektywa powstania takowych w najbliższej przyszłości także jest niewielka. Zaproponowana przeze mnie powyżej definicja powstała jeszcze w styczniu 2020 roku kiedy pisałem ten rozdział. Ostatecznie jednak ta praca jest poszerzona o opublikowaną w maju propozycję regulacji unijnych, które były omawiane powyżej. Zaproponowana tam definicja SI jest bardzo zbliżona do tej zaprezentowanej przeze mnie, jednak z powodu użycia w niej sformułowania „osiągniecia określonych celów"[143] może sugerować, że nie obejmuje swoim zakresem uczenia nienadzorowanego, przy którym nie zawsze dochodzi do określenia celu, jaki ma osiągnąć SI.

Co do zakresu ukształtowania odpowiedzialności deliktowej przy obecnie istniejących regulacjach, w mojej ocenie należy pozostać przy rozdziale jej

[143] *Achieve specific goals*.

charakteru w zależności od osoby, która SI się posługuje. Jeżeli jest to konsument to należy opowiadać się za odpowiedzialnością opartą o zasadę winy w nadzorze, przy czym zwolnienie się z odpowiedzialności wymagać będzie udowodnienia posłużenia się SI zgodnie z instrukcją, jak również tym, jeżeli dojdzie do certyfikacji SI, że jest ona certyfikowana, oryginalna, pochodzi z legalnego i pewnego źródła. Przy wykazaniu powyższych przesłanek dojdzie do uwolnienia się danej osoby od odpowiedzialności. W takiej sytuacji odpowiedzialność może być dochodzona od tego, kto produkt wprowadza do obrotu. Ten z kolei będzie odpowiadać jak za produkt niebezpieczny, która to odpowiedzialność prawdopodobnie w ślad za rekomendacjami komitetu ds. prawnych UE zostanie niedługo znowelizowana. W przypadku przedsiębiorców korzystających ze SI ich odpowiedzialność powinna być ukształtowana na zasadzie ryzyka, w przypadku zwolnienia się od niej (np. wina niewłaściwego poinstruowania przez producenta) odpowiedzialność przejdzie na kolejny podmiot - wprowadzającego do obrotu, producenta. Na końcu tego łańcucha pozostają programiści, osoby odpowiedzialne za wprowadzane dane, testy oprogramowania itp. Zazwyczaj będą oni znajdować się w strukturze jakiegoś przedsiębiorstwa lub sami będą prowadzić działalność gospodarczą. W takiej sytuacji ich odpowiedzialność należy ukształtować na zasadzie ryzyka przedsiębiorcy, na wzór regulacji o wprowadzaniu przedsiębiorstwa w ruch siłami przyrody, ale tylko w przypadku, gdy produkowana SI może wyrządzić duże szkody – tutaj warto odwołać się do zaproponowanego przez UE katalogu systemów SI wysokiego ryzyka. Jeżeli taka sytuacja nie będzie miała miejsca to będziemy stosować zwykłą odpowiedzialność na zasadzie winy. Z kolei osoby, które nie prowadzą przedsiębiorstwa będą odpowiadać za swoje błędy na podstawie umowy zawartej z pracodawcą i na zasadach wynikających z prawa pracy. Taki łańcuch odpowiedzialności gwarantuje, że konsumenci są chronieni w sposób wystarczający, a największe ryzyko ponosi podmiot największy, a więc ten, który masowo wprowadza dane oprogramowanie do obrotu, nawet jeśli nie jest jego twórcą. Oczywiście należy pamiętać o tym, że oprócz tego wszystkiego w grę wchodzić będą kwestie ubezpieczeń, które w pewnym zakresie powinny być nawet obowiązkowe np. właśnie dla podmiotów w unijnej propozycji nazwanych wdrażającymi. Na to wszystko należy nałożyć jeszcze, w praktyce bardzo częste, regulacje umowne. Będą one pojawiać się w szczególności pomiędzy twórcami oprogramowania, producentami oprogramowania a podmiotami, które będą chciały wprowadzać je do obrotu na masową skalę albo z nich korzystać. W zależności od rozwoju tych systemów praktyka z całą pewnością ukształtuje umowy zawierające

specyficzne dla tych systemów rozwiązania, tak jak np. wykształciły się w IT umowy wdrożeniowe, które zresztą będą przy systemach SI podstawowym typem umów, zmodyfikowanym tylko z uwagi na specyfikę oprogramowania np. konieczność stałego nadzoru nad systemem, nie tylko w razie awarii.

Przedstawione przeze mnie wnioski są oczywiście jedynie jedną z wielu możliwych do stworzenia koncepcji, jednak uważam je za trafne. Im więcej będzie się na ten temat pisać i mówić, tym większa szansa na wypracowanie rozwiązań optymalnych (idealne nigdy nie powstaną). Warto więc analizować różnego rodzaju propozycje, sprawdzać zachowanie rynku oraz podmiotów zaangażowanych w tworzenie, wprowadzanie i korzystanie z algorytmów SI. Cechą nieodzownie związaną ze SI jej możliwość ciągłego rozwoju takich programów, dlatego z pewnością również prawo wymagać będzie co jakiś czas dostosowania do pojawiających się zmian. Na taki zresztą krok zdecydowała się UE, która w swoich propozycjach regulacji jako jeden z kluczowych elementów wskazuje na konieczność aktualizacji listy systemów SI wysokiego ryzyka co pół roku. Z kolei gdzieś na horyzoncie, chociaż odlegle, pojawia się widmo silnej SI, która będzie operować sama dla siebie, posiadając swoją świadomość i własne potrzeby. Być może nieuwaga osób odpowiedzialnych za tego typu algorytmy doprowadzi do sytuacji, w której SI dojdzie do wniosku, że nie chce być narzędziem w rękach ludzi. Sytuacja taka, rodem z filmów science fiction, wcale nie jest niemożliwa. Na ten moment nikt nie jest w stanie przewidzieć tego kiedy i jak rozwinie się SI. Jest ona jednak już powszechnie obecna w naszej codzienności, a spory związane z korzystaniem z niej będą w najbliższym czasie coraz częstsze. Warto więc stworzyć prawo, dzięki któremu konsumenci i przedsiębiorcy będą mogli czuć się bezpiecznie, a spory nie będą konieczne.

8. Bibliografia

1. Król U., *Sztuczna inteligencja i systemy ekspertowe. Omówienie wybranych zagadnień w świetle piśmiennictwa 2005-2010*, Kraków 2011.

2. *„History of Artificial Intelligence”*, https://www.coe.int/en/web/artificial-intelligence/history-of-ai , ostatni dostęp: 01.09.2021.

3. *„Can Machines Think?”*, Anyoha Rockwell, http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/ , ostatni dostęp: 01.09.2021.

4. *„The Chinese Room Argument”*, David Cole, https://plato.stanford.edu/entries/chinese-room/, ostatni dostęp: 01.09.2021.

5. *„What is artificial intelligence?"* John McCarthy, Computer Science Department Stanford University Stanford, CA 94305, https://jmc.stanford.edu/articles/whatisai/whatisai.pdf, ostatni dostęp: 01.09.2021.

6. *„Homage to John McCarthy, the Father of Artificial Intelligence (AI)"*, Andy Peart, https://www.artificial-solutions.com/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence, ostatni dostęp: 01.09.2021.

7. *„AI Magazine"* 2006, nr 4

8. *„Sztuczna inteligencja pokonała arcymistrzowski program szachowy. Ludziom zostało kibicowanie"*, Domański Tomasz, https://www.spidersweb.pl/2017/12/sztuczna-inteligencja-szachy.html, ostatni dostęp: 01.09.2021.

9. *„Deep Blue. Komputer, który wygrał z Kasparowem"*, Kaczmarczyk Marcin, https://www.newsweek.pl/wiedza/historia/deep-blue-wygral-20-lat-temu-w-szachy-z-garrim-kasparowem/1g9xnt7, ostatni dostęp: 01.09.2021.

10. *„Watson: sztuczna inteligencja IBM-u uratowała już ludzkie życie. Co sprawia, że jest wyjątkowa?"*, Kreczmar Tomek, https://kreczmar.gadzetomania.pl/58784,watson-sztuczna-inteligencja, ostatni dostęp: 01.09.2021.

11. *"Zimna maszyna" bez pasji nie będzie już grać w go z ludźmi. Nie ma z kim - pokonała najlepszych z najlepszych"*, https://businessinsider.com.pl/wiadomosci/sztuczna-inteligencja-alphago-od-google-wygrala-z-arcymistrzem/p9c7r42, ostatni dostęp: 01.09.2021.

12. *„Chiński robot zdał egzamin lekarski. Koniec z problemami w służbie zdrowia?"*, Winiarski Paweł, https://antyweb.pl/robot-zdaje-egzamin-lekarski/, ostatni dostęp: 01.09.2021.

13. *„Profesor Hawking znów ostrzega ludzkość"*, Bellon Marta, https://businessinsider.com.pl/technologie/profesor-stephen-hawking-o-sztucznej-inteligencji/ph31g7z, ostatni dostęp: 01.09.2021.

14. *„Google zbudowało najpotężniejszy komputer kwantowy na świecie. Totalny przełom"*, Stando Arkadiusz, https://tech.wp.pl/google-zbudowalo-najpotezniejszy-komputer-kwantowy-na-swiecie-totalny-przelom-6426886742259329a, ostatni dostęp: 01.09.2021.

15. *„The Key Definitions Of Artificial Intelligence (AI) That Explain Its Importance"*, Marr Bernard, https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/#69f0c12f4f5d, ostatni dostęp: 01.09.2021.

16. *„Czym jest sztuczna inteligencja?"*, https://planetpartners.pl/czym-jest-sztuczna-inteligencja/, ostatni dostęp: 01.09.2021.

17. *„Czy androidy śnią o zmowach cenowych? Algorytmy cenowe, sztuczna inteligencja i prawo konkurencji"* Derdak M. K., Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2018, nr 8(7), www.ikar.wz.uw.edu.pl, ostatni dostęp: 01.09.2021.

18. *„A beginner's guide to AI: Supervised and unsupervised learning"*, Tristan Greene, https://thenextweb.com/artificial-intelligence/2019/07/06/a-beginners-guide-to-ai-supervised-and-unsupervised-learning/, ostatni dostęp: 01.09.2021.

19. *„Semi-Supervised Machine Learning"*, https://www.datarobot.com/wiki/semi-supervised-machine-learning/, ostatni dostęp: 01.09.2021.

20. *„Semi-Supervised Machine Learning"*, Pająk P., https://www.spidersweb.pl/2016/03/tay-bot-microsoft-sztuczna-inteligencja.html, ostatni dostęp: 01.09.2021.

21. *„What is reinforcement learning? The complete guide*", Osiński B., Budek K., https://deepsense.ai/what-is-reinforcement-learning-the-complete-guide/

22. Flisak D., *Sztuczna inteligencja – jak chronić prawa autorskie twórczości robotów,* „Rzeczpospolita", https://www.rp.pl/Opinie/305229984-Sztuczna-inteligencja--jak-chronic-prawa-autorskie-tworczosci-robotow.html, ostatni dostęp: 01.09.2021.

23. Kurosz K., *„Zawieranie umów przez sztuczną inteligencję (systemy autonomiczne) a wady oświadczeń woli – wprowadzenie do problemu"* [w:] red. Robaczyński W., *„Czynić postęp w prawie. Księga jubileuszowa dedykowana Profesor Birucie Lewaszkiewicz-Petrykowskiej"*, Łódź 2017, s. 73 i n.

24. *„Prawo cywilne – część ogólna. System Prawa Prywatnego. Tom 2"*, red. Z. Radwański, Warszawa 2019, Legalis, Nb 30 i n.

25. *„Kodeks cywilny. Komentarz."* wyd. 24, red. K. Osajda, Warszawa 2020, Legalis.

26. Jędrzejewska A., *„Koncepcja oświadczeń woli w prawie cywilnym"*, Warszawa 1992, s. 10-14.

27. Kocot W. J., *„Wpływ Internetu na prawo umów",* Warszawa 2004.

28. Chłopecki A., *„Szkice prawnicze i futurologiczne”*, Warszawa 2018, wyd. 1, Legalis.

29. *„Kodeks cywilny. Komentarz”*, red. E. Gniewek, P. Machnikowski, Warszawa 2016.

30. *„Black Friday po polsku, czyli sklep „pomylił się" i nie chce wysłać kupionego smartfonu”*, https://www.telepolis.pl/wiadomosci/prawo-finanse-statystyki/black-friday-po-polsku-czyli-sklep-pomylil-sie-i-nie-chce-wyslac-kupionego-smartfonu, ostatni dostęp: 01.09.2021.

31. *„Dystrybutor smartfonów OnePlus miał na Allegro promocję w Black Friday. Dziś odmawia wydania rzeczy po promocyjnej cenie”*, Kralka J. https://bezprawnik.pl/oneplus-allegro-black-friday/, ostatni dostęp: 01.09. 2021.

32. *„Kodeks Cywilny. Komentarz”*, red. K. Pietrzykowski, Warszawa 2015, t. I, Legalis.

33. *„Kodeks Cywilny. Komentarz.”*, red. M. Gutowski, Warszawa 2019, t. II.

34. *„Kodeks cywilny. Komentarz.”*, red. J. Gudowski, Warszawa 2013, Ks. III, cz. 1.

35. *„Zobowiązania”*, R. Longchamps de Bérier, Lwów, 1939, s. 235.

36. Domański L., *„Instytucje kodeksu zobowiązań. Komentarz teoretyczno-praktyczny. Część ogólna”*, t. 2, Warszawa 1936, s. 603–604

37. Zoll F., *„Zobowiązania w zarysie”*, Warszawa 1945, s. 130–131.

38. *„Kodeks cywilny. Komentarz.”*, red. K Pietrzykowski, Warszawa 2015, t. I, art. 415, Nb 38.

39. *„System Prawa Cywilnego”*, red. E. Gniewek, t. III, cz. 1, s. 533–534.

40. Ciszewski J., *„Kodeks cywilny. Komentarz”,* Warszawa 2014, art. 415, Nb 17

41. Kondek J.M., *„Bezprawność jako przesłanka odpowiedzialności odszkodowawczej”*, Warszawa 2013, s. 75–78.

42. *Komentarz do Kodeksu cywilnego*, red. Resich Z., t. II, Warszawa 1972.

43. *Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz.*, red. J. Szwaja, Warszawa 2019, wyd. 5.

44. Ogórek S., *„Biedronka miała poważny błąd w... promocji. Klienci płacili 20 zł, dostawali towar za ponad 1000 zł”*, https://finanse.wp.pl/biedronka-miala-powazny-blad-w-promocji-klienci-placili-20-zl-dostawali-towar-za-ponad-1000-zl-6504177773647489a, ostatni dostęp: 01.09.2021.

45. *„Draft Report with recommendations to the Commission on a Civil liability regime for artificial intelligence”*, (2020/2014(INL)), Committee on Legal Affairs, https://www.europarl.europa.eu/doceo/document/JURI-PR-650556_EN.pdf, ostatni dostęp: 01.09.2021.

46. *„Jest konkretna propozycja unijnej regulacji dot. odpowiedzialności sztucznej inteligencji”,* Michał Nowakowski, https://alebank.pl/jest-konkretna-propozycja-unijnej-regulacji-dot-odpowiedzialnosci-sztucznej-inteligencji/, ostatni dostęp: 01.09.2021.

47. *„Założenia do strategii AI w Polsce. Plan działań Ministerstwa Cyfryzacji.”*, Warszawa, 9 listopada 2018 roku, https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=2ahUKEwjet7Of3M7nAhXqh4sKHfJqCQwQFjADegQIARAB&url=https%3A%2F%2Fwww.gov.pl%2Fdocuments%2F31305%2F436699%2FZa%25C5%2582o%25C5%25BCenia_do_strategii_AI_w_Polsce_-_raport.pdf&usg=AOvVaw0BHTcjLA_qao5pPnSdxLxM , ostatni dostęp: 01.09.2021.

TOM PT. „OCHRONA DANYCH OSOBOWYCH I SZTUCZNA INTELIGENCJA W PRAWIE POLSKIM I CHIŃSKIM” STANOWI PIERWSZY KROK W DYSKUSJI NAD ROZWOJEM BADAŃ NA STYKU PRAWA NOWYCH TECHNOLOGII I OCHRONY DANYCH OSOBOWYCH. TEMATYKA TA JEST NIEZWYKLE WAŻNA ZARÓWNO W POLSCE, JAK W CHINACH, DLATEGO TEŻ WŁAŚNIE TE DWA KRAJE I PORÓWNYWANIE ICH OSIĄGNIĘĆ W TYCH DZIEDZINACH STANOWI CEL NINIEJSZEJ MONOGRAFII.

MOST WIEDZY

ISBN: 978-83-67074-19-3