



Instytut Wymiaru Sprawiedliwości



Zautomatyzowane umowy, pieczęć elektroniczna
i podpis biometryczny. Problematyka złożenia
oświadczenia woli i formy czynności prawnych

dr Nikodem Rycko



Prawo prywatne
Warszawa 2021

Spis treści

1. Przedmiot i cel opracowania	5
2. Zautomatyzowane umowy	5
2.1. Ogólne założenia technologii <i>blockchain</i>	5
2.2. Pojęcie inteligentnego kontraktu	7
2.3. Złożenie oświadczenia woli w sposób zautomatyzowany	8
2.4. Inteligentne kontrakty a forma czynności prawnych	13
3. Pieczęć elektroniczna	18
4. Podpis biometryczny	23
5. Wnioski	27
Bibliografia	29

1. Przedmiot i cel opracowania

Niniejsze opracowanie dotyczy cywilnoprawnych aspektów nowych rozwiązań technicznych, które pojawiły się w ostatnich latach w obszarze umów zawieranych drogą elektroniczną. Intensywny rozwój tych narzędzi i szerokie perspektywy ich możliwych zastosowań prowadzą do pytania o zasadność dokonania w związku z tym procesem zmian w obowiązujących przepisach prawa cywilnego. Próba rozstrzygnięcia tego zagadnienia stanowi zasadniczy cel studium. Jego zakres ograniczony został do oceny wybranych rozwiązań technicznych, tj. zautomatyzowanych umów opartych na technologii *blockchain*, pieczęci elektronicznej i podpisu biometrycznego.

W dalszej części opracowania analiza prawna poprzedzona jest skrótowym przedstawieniem poszczególnych rozwiązań technicznych – nie w celu ich wyjaśnienia, ale przedstawienia założeń, na których oparte zostały właściwe rozważania. Ocena zasadności zmiany przepisów prawnych obejmuje dwa zagadnienia: regulację złożenia oświadczenia woli oraz formy czynności prawnych.

2. Zautomatyzowane umowy

2.1. Ogólne założenia technologii *blockchain*

Pojęcie *blockchain* oznacza metodę zapisu danych w pamięci komputera. Z technicznego punktu widzenia *blockchain* jest rejestrem (bazą danych), który zawiera wpisy w kolejności chronologicznej. Baza ta składa się z informacji zapisanych w blokach pamięci, rozproszonych w sieci komputerowej. Każdy z użytkowników sieci może dodać nowy blok pamięci do rejestru, wymaga to jednak akceptacji przez pozostałe komputery tworzące sieć. W ten sposób rejestr może być uzupełniony wyłącznie zgodnie z przyjętymi na wstępie zasadami. Jednocześnie brak jest centralnego ośrodka, który sprawowałby nadzór nad poprawnością zapisów¹. Istotę technologii *blockchain* stanowią algorytmy umożliwiające zapewnienie poprawności danych przez wielu użytkowników jednocześnie, bez konieczności istnienia

¹ G.W. Peters, E. Panayi, *Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*, [online:] <https://ssrn.com/abstract=2692487>, s. 3 [dostęp: 12.11.2021].

jednego, centralnego punktu zarządzającego informacjami. Jest to rodzaj tzw. technologii rozproszonego rejestru (*Distributed Ledger Technology – DLT*)².

Praktyczne znaczenie technologii *blockchain* wynika stąd, że pomimo braku centralnego ośrodka zapewniającego poprawność danych, zapisane w pamięci komputera informacje są niezmiennie. Ich modyfikacja jest wykonalna tylko zgodnie z przyjętymi z góry regułami. Możliwe jest to dzięki weryfikowaniu kolejnych segmentów danych przez komputery należące do poszczególnych użytkowników, według określonego algorytmu³. Segmenty (*blocks*) tworzą ciąg (*chain*) składający się na zapis wszystkich kolejnych modyfikacji rejestru, wraz z oznaczeniem czasu ich dokonania⁴.

Zastosowanie technologii *blockchain* uniemożliwia kilkukrotne dodanie tych samych danych do rejestru, jak również dalsze przechowywanie w nim danych usuniętych. Jest to użyteczne przede wszystkim z perspektywy zapisów księgowych, ponieważ zapewnia, że ta sama wartość nie będzie przypisana jednocześnie do więcej niż jednej pozycji. Z tego powodu pierwszym powszechnym i nadal najważniejszym zastosowaniem omawianej technologii stały się tzw. kryptowaluty, czyli środki płatnicze występujące w postaci cyfrowej i – z ekonomicznego punktu widzenia – posiadające wszystkie cechy pieniądza⁵.

Wśród zalet *blockchain* wymienia się nieodwracalność transakcji dokonywanych przy zastosowaniu tej technologii⁶. Stwierdzenie to jest jednak nieścisłe. Rzeczywiście, większość rejestrów opartych na *blockchain*, w tym także te związane z najważniejszą z kryptowalut, czyli *bitcoin*, została zbudowana na zasadzie niezmienności przepływów danych⁷. Nie ma jednak przeszkód, aby dopuścić możliwość odwracalności transakcji, przy czym należy zaznaczyć, że zapis ponownego przepływu danych zostanie utrwalony w rejestrze. Należałoby zatem raczej stwierdzić, że zmiana zapisów w rejestrze może być dokonana tylko zgodnie z przyjętymi uprzednio regułami.

W literaturze przedmiotu zwraca się uwagę, że bazy danych stworzone na podstawie technologii *blockchain* można podzielić na:

- a) rejestry wymagające (*permissioned*) i niewymagające (*permissionless*) zgody – w zależności od tego, czy uczestniczenie w weryfikacji wpisów w rejestrze wymaga czyjejś zgody, czy jest otwarte dla każdego;

² A Report by the UK Government Chief Scientific Adviser, *Distributed Ledger Technology: beyond block chain*, Government Office for Science, 2016, [online:] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf [dostęp: 15.06.2021].

³ P.S. Bayón, *Key Legal Issues Surrounding Smart Contract Applications*, „KLRI Journal of Law and Legislation” 2019, t. 9, nr 1, s. 4–5.

⁴ H. Kakavand, N.K. De Sevres, B. Chilton, *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*, 2017, [online:] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251 [dostęp: 12.11.2021].

⁵ S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, [online:] <https://bitcoin.org/bitcoin.pdf> [dostęp: 12.11.2021]; R. Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, „Hastings Science & Technology Law Journal” 2011, nr 4, s. 165–173, [online:] <https://ssrn.com/abstract=1817857> [dostęp: 12.11.2021].

⁶ K. Gajek, *Oświadczenie woli w komunikacji elektronicznej*, Warszawa 2020, rozdz. VI, par. 1.

⁷ G.W. Peters, E. Panayi, *Understanding...*, s. 28.

- b) rejestry publiczne i prywatne – w zależności od tego, czy dostęp i możliwość dodawania wpisów do rejestru ma każdy, czy wyłącznie określone osoby.

W zasadzie rejestry prywatne są jednocześnie rejestrami wymagającymi zgody, rejestry publiczne natomiast zgody nie wymagają. Istnieją jednak wyjątki⁸.

2.2. Pojęcie inteligentnego kontraktu

Przez dłuższy czas głównym zastosowaniem technologii *blockchain* były kryptowaluty. Dalszy rozwój techniczny doprowadził jednak do powstania tzw. technologii *blockchain* drugiej generacji⁹. Nowsza forma rejestru transakcji umożliwia zapis w rejestrze opartym na *blockchain* nie tylko prostych informacji, jak w przypadku kryptowalut, ale również rozbudowanych instrukcji warunkowych, np. programu komputerowego dokonującego przelewu wirtualnych środków płatniczych w chwili spełnienia określonych przesłanek. Stało się to podstawą opracowania tzw. inteligentnych kontraktów¹⁰.

Pojęcie inteligentnego kontraktu (*smart contract*) wprowadził pod koniec ubiegłego stulecia Nick Szabo, który zaproponował automatyzację zobowiązań wyrażonych w postaci elektronicznej. Inteligentny kontrakt zdefiniował on jako zestaw takich zobowiązań, których wykonanie następuje automatycznie w razie spełnienia określonych z góry i zapisanych w postaci programu komputerowego przesłanek. Program komputerowy w celu wykonania zobowiązania musi mieć dostęp do zasobów kontrolowanych przy pomocy komunikacji elektronicznej, np. zapisów środków pieniężnych na koncie internetowym. Ustalane przez strony przesłanki mają charakter obiektywny, a wykonanie zobowiązania następuje automatycznie¹¹.

Inteligentny kontrakt w przedstawionym znaczeniu jest zatem programem komputerowym. Jego działanie polega na tym, że w razie spełnienia ustalonych warunków dochodzi do dyspozycji określonymi dobrami o wartości ekonomicznej. Cechy technologii *blockchain* – niemożność zmiany danych i brak centralnego ośrodka decyzyjnego – powodują, że rozporządzanie konkretnym dobrem na zasadach inteligentnego kontraktu jest automatyczne i nieodwołalne. W związku z tym zmiana raz ustalonych zasad wykonania umowy nie jest możliwa. Żadna ze stron nie może również wstrzymać jej wykonania – np. poprzez

⁸ Tamże, s. 5.

⁹ Tamże, s. 1.

¹⁰ Tamże, s. 2.

¹¹ P.S. Bayón, *Key Legal Issues...*, s. 3; V. Buterin, *A Next Generation Smart contract and Decentralized Application Platform*, „Ethereum White Paper” 2018, [online:] http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. [dostęp: 12.11.2021]; T. Hoser, *Blockchain basics, commercial impacts and governance challenges*, „Governance Directions” 2016, nr 68, s. 608–612; A. Walch, *The Path of the Blockchain Lexicon (and the Law)*, „Review of Banking & Finance” 2017, nr 36, s. 713, [online:] https://www.academia.edu/32573448/The_Path_of_the_Blockchain_Lexicon_and_the_Law. [dostęp: 12.11.2021].

przedstawienie okoliczności wyłączających odpowiedzialność zapisów umowy – chyba że taka możliwość została przewidziana z góry i zapisana w kodzie programu komputerowego¹².

Sam twórca pojęcia inteligentnego kontraktu stwierdza, że jest to środek zapewniający wykonanie umowy na zasadach przypominających działanie automatu do sprzedaży towarów¹³. Nick Szabo wskazuje też na szerokie możliwości zastosowania inteligentnych kontraktów dotyczące w zasadzie wszystkich dóbr, które można kontrolować cyfrowo¹⁴. Przykładem może być chociażby blokada silnika pojazdu do czasu wpływu na rachunek bankowy środków z tytułu wymagalnej raty leasingu.

Zastosowanie inteligentnego kontraktu umożliwia automatyczne wykonanie umowy bez udziału organów państwa¹⁵. Bezwzględny i nieodwołalny charakter powyższych rozwiązań jest przedstawiany jako ich zaleta, która wyraża się w obniżeniu kosztów transakcyjnych, a przez to – również cen towarów i usług¹⁶. Pomimo tego jednak trudno nie dostrzec ryzyka wystąpienia okoliczności nieprzewidzianych przez strony umowy albo możliwości świadomego wprowadzenia jednej z nich przez drugą w błąd.

2.3. Złożenie oświadczenia woli w sposób zautomatyzowany

Mając na uwadze istotę inteligentnych kontraktów z technicznego punktu widzenia, rozważenia wymaga kwalifikacja prawna postępowania osób, które korzystają z takich programów komputerowych. Zasadne wydaje się pytanie, czy inteligentny kontrakt albo wyrażenie zgody na jego zastosowanie można rozumieć jako oświadczenie woli albo element takiego oświadczenia.

W doktrynie od dawna zwraca się uwagę na trudności dotyczące interpretacji oświadczeń złożonych w sposób jednostronnie albo dwustronnie zautomatyzowany¹⁷. Wydaje się, że w ramach problematyki inteligentnych kontraktów rozważenia wymagają przede wszystkim dwa zagadnienia: relacja pojęcia inteligentnego kontraktu i umowy w rozumieniu prawa cywilnego oraz kwestia przypisania podmiotowi prawa oświadczenia woli składanego w sposób zautomatyzowany.

Nie ulega wątpliwości, że z perspektywy prawa cywilnego inteligentny kontrakt sam w sobie nie jest umową. Jest rozwiązaniem technicznym zapewniającym automatyczny

¹² M. di Angelo, A. Soare, G. Salzer, *Smart Contracts in View of the Civil Code*, s. 3, [online:] https://publik.tuwien.ac.at/files/publik_278278.pdf [dostęp: 12.11.2021].

¹³ N. Szabo, *The Idea of Smart Contracts*, 1997, [online:] https://web.archive.org/web/20060615044959/http://szabo.best.vwh.net/smart_contracts_idea.html [dostęp: 12.11.2021].

¹⁴ Tamże.

¹⁵ M. Raskin, *The Law and Legality of Smart Contracts*, 2017, [online:] <https://doi.org/10.2139/ssrn.2842258> [dostęp: 12.11.2021].

¹⁶ P.S. Bayón, *Key Legal Issues...*, s. 8–10

¹⁷ W.J. Kocot, *Elektroniczna forma oświadczeń woli*, „Przegląd Prawa Handlowego” 2001, nr 3, s. 2.

transfer określonych wartości ekonomicznych w razie spełnienia ustalonych warunków. Przedstawiona wcześniej analogia do maszyny służącej do sprzedaży towarów wydaje się zatem w tym przypadku trafiona. Za słuszne możemy też uznać ustalenia nauki polskiej jeszcze z początku ubiegłego stulecia, według których zarówno wystawienie automatu do sprzedaży, jak i skorzystanie z niego można traktować jako oświadczenie woli¹⁸. Podobnie, akceptacja zasad inteligentnego kontraktu i wykonanie go może być interpretowane jako zawarcie umowy w sposób dorozumiany¹⁹. Poszczególne transakcje dokonywane w ramach inteligentnych kontraktów można z kolei rozumieć jako ofertę albo jej akceptację²⁰.

W przypadku inteligentnych kontraktów sytuacja jest jednak bardziej złożona niż w przypadku korzystania z automatów do sprzedaży. Po pierwsze, jak wskazano wyżej, inteligentny kontrakt z reguły stanowi automatyzację tylko fragmentu umowy, przez co pozostała jej treść nie znajduje wyrazu w działaniu programu komputerowego²¹. Powstaje zatem konieczność ustalenia pozostałych postanowień porozumienia. Treść umowy może być utrwalona w dowolnej formie, może też wynikać w sposób dorozumiany z zachowania stron. Po drugie, ustalenia dokonane przez strony umowy mogą pozostawać w sprzeczności z działaniem programu komputerowego, który pracuje według kodu zapisanego w określonym języku programowania. Powstaje wówczas pytanie, które postanowienia należy uznać za mające pierwszeństwo – wyrażone w języku programowania czy przedłożone w inny sposób, np. ustny albo pisemny²².

Rozwiązania pierwszego z przedstawionych zagadnień poszukiwać należy w ogólnych przepisach o wykładni oświadczeń woli. Normy kodeksu cywilnego pozostawiają szerokie możliwości ustalenia treści zawartej umowy na podstawie całokształtu zachowania stron. Komplikacje w tym zakresie mogą natomiast dotyczyć przede wszystkim kwestii dowodowych.

Znacznie trudniejsze do wytłumaczenia jest drugie z przedstawionych zagadnień. W nauce niemieckiej wyrażono pogląd, że w przypadku, gdy obie strony umowy mają świadomość znaczenia kodu, należy przyjąć, że jego treść jest rozstrzygająca. Podobnie należy postąpić w razie ustalenia, że zgodną wolą stron było zastosowanie się bez zastrzeżeń do rezultatów działania programu komputerowego²³. Pogląd ten możemy traktować jednak jako zbyt kategoryczny. Bardziej trafne wydaje się przyjęcie, że treść kodu stanowi jedną z okoliczności uwzględnianych przy dokonywaniu wykładni oświadczenia woli, zgodnie z normami wyrażonymi w art. 65 k.c. Przykładowo, uwzględnienie mechanizmu działania kodu w języku programowania nie może doprowadzić do ustalenia takiej treści umowy, której postanowienia

¹⁸ E. Till, *O znaczeniu prawnym automatu*, Lwów 1900, s. 8.

¹⁹ K. Gajek, *Oświadczenie woli...*, rozdz. VI, par. 2

²⁰ M. Kaulartz, J. Heckmann, *Smart Contracts – Anwendungen der Blockchain-Technologie*, „Computer und Recht” 2016, nr 9, s. 618–624.

²¹ P.S. Bayón, *Key Legal Issues...*, s. 11–12.

²² M. Fries, *Smart Contracts: Brauchen schlaue Verträge noch Anwälte?*, „Anwaltsblatt” 2018, nr 2, s. 86–90.

²³ M. Kaulartz, J. Heckmann, *Smart Contracts...*, s. 618–624.

byłyby wewnętrznie sprzeczne albo które pozostawałyby w sprzeczności z zasadami współżycia społecznego.

Zasady działania inteligentnego kontraktu – polegające na wystąpieniu określonego skutku w razie spełnienia ustalonych przesłanek – w gruncie rzeczy odpowiadają treści postanowienia umownego. Inteligentny kontrakt w typowym przypadku spełnia zatem dwojaką funkcję: po pierwsze – stanowi mechanizm wykonania umowy, a po drugie – jest przejawem zachowania stron, brany pod uwagę w ramach ustalania treści umowy.

Istnieje możliwość, że zasady działania inteligentnego kontraktu odbiegać będą od praw i obowiązków stron składających się na treść umowy, która jest ustalona zgodnie z regułami wykładni oświadczenia woli. Taka ewentualność występuje również wówczas, gdy mechanizm działania inteligentnego kontraktu – zapisany w postaci kodu w języku programowania – jest jedynym przejawem woli stron, który został w jakikolwiek sposób utrwalony. Zgodnie z obowiązującymi normami prawa cywilnego brak jest bowiem podstaw do przypisywania kodowi w języku programowania pierwszeństwa przed innymi sposobami wyrażenia woli. Jednocześnie nie ma przeciwwskazań, aby w okolicznościach konkretnego przypadku przyjąć, że treść kodu ma znaczenie rozstrzygające. W innych sytuacjach, np. z udziałem osoby, która kodu nie zna i nie rozumie, trafne może okazać się rozstrzygnięcie odmienne. Obowiązujące normy regulujące złożenie i wykładnię oświadczenia woli należy ocenić jako adekwatne, a ich elastyczność należy uznać za zaletę. W szczególności możemy przyjąć, że postulowanie wprowadzania szczególnych regulacji dotyczących związania stron zasadami wyrażonymi kodem w języku programowania nie jest zasadne.

Możliwy jest również przypadek, kiedy postanowienie, któremu odpowiada inteligentny kontrakt, okaże się nieważne ze względu na sprzeczność z prawem, cel zmierzający do obejścia prawa albo niezgodność z zasadami współżycia społecznego. W takim przypadku pozostawanie umowy w mocy we wtórym zakresie należy ocenić na podstawie art. 58 § 3 k.c. Wówczas należy także dokonać oceny z uwzględnieniem okoliczności danego przypadku. Nie wydaje się też trafne założenie z góry, że bez postanowienia wyrażonego w inteligentnym kontrakcie cała umowa nie zostałaby zawarta.

Przechodząc do zagadnienia przypisania podmiotowi prawa oświadczenia woli złożonego w sposób zautomatyzowany, należy wyróżnić dwa rodzaje programów komputerowych. Pierwszy z nich obejmuje te, których efekt działania jest z góry znany, przynajmniej dla osoby, która zapoznała się z treścią kodu i zna zastosowany język programowania.

Rozwój techniki komputerowej wymaga jednak wyodrębnienia również drugiej grupy programów. Od dawna w doktrynie rozważana jest dopuszczalność przypisania podmiotowi prawa skutków zachowania się komputera, które przy tworzeniu programu komputerowego nie zostały przewidziane²⁴. Obecnie problem ten nabiera znaczenia ze względu na rozwój

²⁴ A. Jędrzejewska, *Oświadczenia woli składane za pomocą komputera (w świetle doświadczeń niemieckich)*, „Państwo i Prawo” 1992, nr 11, s. 68–69.

algorytmów tzw. uczenia maszynowego, które dostosowują zawartość przekazywanych komunikatów do zachowania użytkownika. W wyniku interakcji z odbiorcą program ulega zmianie, przybierając formę nieznaną jego twórcy. W rezultacie nawet doskonała znajomość początkowej treści programu nie pozwala na ustalenie przyszłego zachowania komputera. Algorytmy tego rodzaju są obecnie powszechnie stosowane chociażby w celu ustalania treści reklamowych prezentowanych użytkownikom portali społecznościowych. Możliwości ich zastosowania są jednak znacznie szersze.

W przypadku programów należących do pierwszej grupy nie ma wątpliwości, że wystarczające są obowiązujące przepisy regulujące oświadczenia woli. Aktualne pozostają poglądy doktryny, że oświadczenie woli może być złożone w postaci elektronicznej, również w sposób zautomatyzowany, i nie wpływa to na jego moc obowiązującą²⁵.

Znacznie większe trudności wywołuje ocena sytuacji, w której treść oświadczenia składanego przez program komputerowy nie była przewidziana albo nawet nie była możliwa do przewidzenia przez osobę, która programem tym się posługuje. Pojawia się bowiem pytanie, czy można w takim przypadku stwierdzić istnienie oświadczenia woli.

Rozstrzygnięcie przedstawionej kwestii zależy od poglądu na istotę oświadczenia woli oraz przyczyny związania złożoną deklaracją. W nauce niemieckiej zagadnienie to rozważa się od dawna, odwołując się do analogii ze złożeniem własnoręcznego podpisu pod oświadczeniem *in blanco*²⁶. Wskazuje się, że osoba, która podpisała i przekazała innej osobie takie oświadczenie, będzie związana jego zawartością, chociaż w gruncie rzeczy nie miała możliwości przewidzenia, jaka treść zostanie zamieszczona powyżej podpisu. Ktoś, kto podpisuje się pod dokumentem *in blanco*, musi liczyć się z tym, że jego deklaracja będzie traktowana jako oświadczenie woli oraz że istnieje ryzyko wypełnienia dokumentu niezgodnie z wolą podpisującego²⁷.

Konsekwentnie wskazuje się, że źródłem przypisania skutków prawnych oświadczenia woli według przedstawionej koncepcji nie jest wola składającego oświadczenie, ale wywołane przez nią zaufanie u innych uczestników obrotu co do mocy wiążącej złożonego oświadczenia²⁸. Pogląd ten można wykorzystać także w odniesieniu do oświadczeń składanych w sposób zautomatyzowany. Do rozważenia pozostaje, czy oświadczenie woli należy również przypisać osobie, która przy posługiwaniu się komputerem zachowała odpowiednią staranność, a złożenie deklaracji jest wynikiem działań, na które nie miała wpływu, np. bezprawnej ingerencji osób trzecich.

²⁵ W.J. Kocot, *Elektroniczna forma...*, s. 2-3.

²⁶ H. Köhler, *Die Problematik automatisierter Rechtvorgänge, insbesondere von Willenserklärung*, „Archiv für die civilistische Praxis” 1982, nr 1-2, s. 133-134.

²⁷ A. Jędrzejewska, *Oświadczenia woli...*, s. 71.

²⁸ K. Gajek, *Oświadczenie woli...*, rozdz. VII, par. 6; A. Jędrzejewska, *Koncepcja oświadczenia woli w prawie cywilnym*, Warszawa 1992, s. 191.

W nauce niemieckiej przyjmuje się, że przypisanie oświadczenia woli następuje wyłącznie w granicach wyznaczonych przez obowiązek zachowania należytej staranności. Zachowanie tego stopnia staranności (np. stosowanie odpowiednich zabezpieczeń przed wirusami) wyklucza przypisanie oświadczenia woli, chociażby wymagała tego wspomniana ochrona zaufania innych osób. W doktrynie polskiej prezentowane jest odmienne stanowisko, zgodnie z którym przypisanie oświadczenia woli następuje na podstawie wspomnianych wyżej reguł służących ochronie zaufania uczestników obrotu²⁹. Jednocześnie wskazuje się na możliwość uchylenia się od skutków prawnych złożonego oświadczenia na podstawie używanych odpowiednio przepisów o błędzie³⁰.

Zastosowanie inteligentnych kontraktów, które umożliwiają automatyczne wykonanie zobowiązania, sprawia ponadto, że aktualna staje się kwestia ustalenia tożsamości podmiotu składającego oświadczenie woli. Ponieważ zagadnienie dotyczy umowy, można je ująć ściślej jako problem ustalenia tożsamości stron stosunku zobowiązaniowego. W wielu przypadkach osoby wyrażające zgodę na zastosowanie inteligentnego kontraktu nie ujawniają swojej tożsamości w ogóle. Konieczność identyfikacji kontrahenta staje się zbędna, jeżeli wykonanie umowy jest zapewnione przy pomocy automatycznego, a jednocześnie pewnego mechanizmu. Można wyrazić wątpliwość, czy w sytuacji, gdy osoby dokonujące czynności nie są znane, można w ogóle stwierdzić złożenie oświadczenia woli i obowiązywanie umowy w rozumieniu prawa cywilnego.

W polskich badaniach dotyczących tego zjawiska przeważa pogląd, że podmioty stosunku zobowiązaniowego muszą być oznaczone³¹. Rozbieżności dotyczą natomiast chwili, w której ich identyfikacja powinna nastąpić. Część doktryny stoi na stanowisku, że w zasadzie jest to konieczne już w chwili powstania zobowiązania, a wyjątki od tej reguły są nieliczne i wynikają z przepisów szczególnych³². W myśl odmiennego zapatrywania do powstania zobowiązania wystarczające jest stworzenie podstaw do określenia w przyszłości podmiotów występujących w charakterze wierzyciela i dłużnika³³. Treść umowy powinna zatem być taka, by w razie spełnienia się zdarzeń opisanych w jej zakresie zastosowania możliwe było ustalenie osoby zobowiązanej, nakazanego jej zachowania i osoby, na rzecz której zachowanie to ma być podjęte (osoby uprawnionej). Umowa (ewentualnie wraz z przepisami prawa – zwyczajami,

²⁹ A. Jędrzejewska, *Koncepcja oświadczenia woli...*, s. 182–191.

³⁰ M. Drozdowicz, *Błąd w elektronicznych czynnościach prawnych*, „Przegląd Prawa Handlowego” 2001, nr 9, s. 28; W.J. Kocot, *Wpływ Internetu na prawo umów*, Warszawa 2004, s. 120; M. Węsierski, *Charakterystyka prawna umów zawieranych drogą elektroniczną*, Warszawa 2020, s. 94–97.; J. Rajski, W. Kocot, K. Zaradkiewicz, *Prawo o kontraktach w obrocie gospodarczym*, Warszawa 2002, s. 81.

³¹ J. Grykiel, *Kilka uwag o nowej definicji dokumentu i formie dokumentowej*, „Monitor Prawniczy” 2016, nr 5, s. 240.

³² A. Ohanowicz, J. Górski, *Zobowiązania. Zarys według kodeksu cywilnego. Część szczegółowa*, Warszawa–Poznań 1966; S. Grzybowski, *System prawa cywilnego*, t. III, cz. 1, Wrocław 1981; W. Czachórski, A. Brzozowski, M. Safjan, E. Skowrońska-Bocian, *Zobowiązania. Zarys wykładu*, Warszawa 2009.

³³ A. Klein, *Pojęcie umowy i stosunku zobowiązaniowego kontraktacji według kodeksu cywilnego*, „Studia Cywilistyczne” 1972, t. XIX, s. 139; Z. Radwański, A. Olejniczak, *Zobowiązania. Część ogólna*, wyd. 12, Warszawa 2016, s. 12.

zasadami współżycia społecznego) musi w najmniejszym zakresie określać przynajmniej sposób, w jaki najpóźniej w chwili zaktualizowania się obowiązku dłużnika (wymagalności świadczenia) wszystkie elementy zobowiązania będą mogły być jednoznacznie wskazane przez obiektywnego obserwatora³⁴.

W odniesieniu do oświadczeń woli składanych przy pomocy środków komunikacji elektronicznej w ostatnich latach wyrażane są jednak również poglądy, że nie zawsze ustalenie tożsamości osoby składającej oświadczenie jest niezbędne do ważności umowy. Nawiązuje się przy tym do dorobku doktryny, który dotyczy umów zawieranych przy pomocy mechanicznych automatów do sprzedaży towarów³⁵.

2.4. Inteligentne kontrakty a forma czynności prawnych

Umowa zawarta z wykorzystaniem inteligentnego kontraktu podlega przepisom regulującym czynności prawne, w tym również przepisom o formie. Rozważenia wymaga kwestia, czy umowy tego rodzaju spełniają przesłanki szczególnych form czynności prawnych, uregulowanych w polskim kodeksie cywilnym. Następnie można sformułować wnioski dotyczące potrzeby zmiany przepisów kodeksu albo innych ustaw w zakresie formy czynności prawnych ze względu na pojawienie się zjawiska inteligentnych kontraktów.

Punktem wyjścia dla dalszych rozważań jest obowiązująca w polskim prawie (oraz systemach prawnych innych państw) zasada swobody formy czynności prawnych (albo, nazywanych inaczej, zachowań zmierzających do wywołania skutków prawnych w tych systemach prawnych, które pojęcia czynności prawnej nie znają)³⁶. Akt woli osoby składającej oświadczenie musi być ujawniony, ale ujawnienie to może nastąpić w różny sposób. W teorii wskazuje się, że można w tym celu posłużyć się dowolnymi znakami lub kanałami informacyjnymi. Za oczywiste uznaje się również, że oświadczenie woli może być złożone w drodze teleinformatycznego przekazu danych³⁷. Prowadzi to do wniosku, że wola zawarcia umowy może być wyrażona także poprzez opracowanie programu komputerowego nazywanego inteligentnym kontraktem oraz skutek zachowania zmierzającego do zastosowania tego kontraktu przez określone osoby w odniesieniu do ich majątku. Za element oświadczenia

³⁴ P. Machnikowski, [w:] *System Prawa Prywatnego*, t. 5: *Prawo zobowiązań – część ogólna*, red. K. Osajda, wyd. 3, Warszawa 2020, s. 567.

³⁵ K. Gajek, *Oświadczenie woli...*, rozdz. VII, par. 7.

³⁶ J. Górecki, *Forma umów obligacyjnych i rzeczowych w prawie prywatnym międzynarodowym*, Katowice 2007, s. 17–54; M. Grochowski, *Wymogi formalne w umowach konsumenckich*, Warszawa 2018, s. 110; W.J. Kocot, *Forma oświadczenia woli w dobie europeizacji polskiego prawa prywatnego*, [w:] *Rozprawy z prawa cywilnego, własności intelektualnej i prawa prywatnego międzynarodowego. Księga pamiątkowa dedykowana profesorowi Bogusławowi Gawlikowi*, red. J. Pisuliński, P. Tereszkiewicz, F. Zoll, Warszawa 2012, s. 77–79; Z. Radwański, S. Czepita, E. Drozd, Z. Kuniewicz, S. Słotwiński, *Forma czynności prawnej*, [w:] *System Prawa Prywatnego*, t. 2: *Prawo cywilne – część ogólna*, wyd. 3, Warszawa 2019, s. 173.

³⁷ W.J. Kocot, *Forma oświadczenia woli...*, s. 81.

woli uznać można również kod w języku programowania, w którym inteligentny kontrakt został wyrażony, oraz wszelkie dotyczące go komunikaty stron w dowolnej formie (ustnej, pisemnej, elektronicznej, dorozumianej).

Umowa z wykorzystaniem inteligentnego kontraktu wymagała będzie określonej formy szczególnej, jeżeli formę taką przewidziano w ustawie albo w umowie stron. Drugi z wymienionych przypadków zachodzić może przede wszystkim wtedy, gdy inteligentny kontrakt dotyczy zawartej wcześniej umowy, obejmującej postanowienia co do formy.

Nie ulega wątpliwości, że z przyczyn przedstawionych powyżej zastosowanie technologii *blockchain* umożliwia utrwalenie faktu zawarcia umowy³⁸. Co więcej, stwierdzenie tego stanu rzeczy jest znacznie trwalsze niż w przypadku, gdy oświadczenia stron zostały zawarte na piśmie albo zamieszczone w pamięci jednego tylko urządzenia elektronicznego. Ten sam stopień trwałości dotyczy momentu transferu danych, co może stanowić podstawę ustalenia chwili zawarcia umowy.

Można z tego powodu stwierdzić, że zachowanie treści oświadczenia spełnia definicję dokumentu, którym zgodnie z art. 77³ k.c. jest nośnik informacji umożliwiający zapoznanie się z jej treścią. W rozważaniach na ten temat zwraca się uwagę, że powołany przepis nie zawiera wymagania, aby przedmiotowy nośnik był trwały, przez co pojęcie dokumentu jest bardzo szerokie i obejmuje wszelkie informacje przekazywane drogą elektroniczną³⁹. Ustalenie, że zapis w technologii *blockchain* spełnia definicję dokumentu, nie wystarcza jednak do ustalenia, że spełnione zostały wymagania formy dokumentowej. Zgodnie z art. 77² k.c. do zachowania tej formy wystarcza złożenie oświadczenia woli w postaci dokumentu w sposób umożliwiający ustalenie osoby składającej oświadczenie. Można uznać, że przez ustalenie osoby należałoby rozumieć identyfikację tożsamości podmiotu prawa będącego nadawcą oświadczenia⁴⁰. Wątpliwości budzi natomiast kwestia, z czyjej perspektywy należy oceniać możliwość dokonania takiego ustalenia.

Pierwszy pogląd zakłada, że ewentualność taką musi mieć osoba, na której sytuację prawną bezpośrednio lub pośrednio oddziałuje złożone oświadczenie woli. Najczęściej będzie to podmiot, do którego oświadczenie jest kierowane⁴¹. Według odmiennego stanowiska powyższa koncepcja jest uzasadniona celowościowo, jednak brzmienie przepisu wskazuje raczej na możliwość obiektywnej weryfikacji osoby nadawcy⁴².

Ponadto wskazuje się, że sposób ustalenia danych nadawcy może być dowolny i może wynikać chociażby z wysłania komunikatu ze skrzynki poczty elektronicznej, konta w portalu

³⁸ P.S. Bayón, *Key Legal Issues...*, s. 16

³⁹ J. Grykiel, *Kilka uwag...*, s. 237.

⁴⁰ Tamże, s. 239.

⁴¹ W.J. Kocot, *Dalsza modernizacja kodeksowej regulacji formy pisemnej czynności prawnej*, „Przegląd Prawa Handlowego” 2016, nr 10, s. 10.

⁴² J. Grykiel, *Kilka uwag...*, s. 239.

społecznościowym albo komputera oznaczonego określonym numerem IP⁴³. Wydaje się, że stanowisko to należałoby opatrzyć zastrzeżeniem, że identyfikacja nadawcy co do zasady powinna być możliwa przy zastosowaniu przeciętnych zasobów, w szczególności bez konieczności korzystania ze specjalnego oprogramowania albo zlecenia odpłatnych usług profesjonalnym podmiotom.

Zestawiając ustalenia dotyczące formy dokumentowej oraz inteligentnych kontraktów, należy zauważyć, że technologia *blockchain* nie wymaga ani nie umożliwia identyfikacji danych osób, które się nią posługują. Osoby dokonujące wpisów w rejestrze są oznaczane przy pomocy jednoznacznych i trwałych identyfikatorów, nie jest jednak wymagane powiązanie ich z określonym podmiotem prawa. Mając na uwadze, że strony umowy zawieranej przy pomocy inteligentnego kontraktu mogą znajdować się w dowolnym miejscu na świecie, trzeba stwierdzić, że w braku zastosowania dodatkowych rozwiązań technicznych mogą one pozostać anonimowe.

Nie oznacza to jednak, że technologia *blockchain* nie może zostać powiązana ze środkami identyfikacji na potrzeby komunikacji elektronicznej. W tym celu wymagane byłoby jednak zastosowanie dodatkowych rozwiązań technicznych i prawnych. Przykładowo platforma internetowa służąca do zawierania umów w oparciu o technologię *blockchain* mogłaby być dostępna wyłącznie dla osób, których identyfikator elektroniczny zostanie powiązany z ich danymi osobowymi albo oznaczeniem w rejestrze przedsiębiorców. Równolegle mogą jednak funkcjonować w praktyce platformy, które nie wymagają takiej identyfikacji, a nawet – pomagają zachować anonimowość.

Ponieważ w braku zastosowania dodatkowych rozwiązań technologia *blockchain* nie umożliwia identyfikacji podmiotu składającego oświadczenie woli, nie można uznać, aby oświadczenia tego rodzaju były składane w formie dokumentowej. Nie spełniają one również przesłanek formy elektronicznej, która zgodnie z art. 78¹ § 1 k.c. wymaga, aby oświadczenie było opatrzone kwalifikowanym podpisem elektronicznym. Chociaż najprawdopodobniej możliwe jest opracowanie sposobu łączącego podpis elektroniczny z technologią *blockchain*, to jednak – podobnie jak w przypadku identyfikacji na potrzeby formy dokumentowej – technologia ta bez dodatkowych rozwiązań podpisu takiego nie wymaga. Ponadto jest oczywiste, że inteligentny kontrakt nie spełnia również wymagań formy pisemnej.

Prowadzi to do wniosku, że umowa zawarta z wykorzystaniem inteligentnego kontraktu nie spełnia żadnej z kodeksowych form czynności prawnej. Oczywiście konkluzja ta ma sens przy założeniu, że strony nie podjęły dodatkowych działań mających na celu ich identyfikację, równoległej wymiany korespondencji w formie elektronicznej albo pisemnej czy nawet podpisania aktu notarialnego. W braku takich dodatkowych reakcji inteligentny kontrakt

⁴³ W.J. Kocot, *Dalsza modernizacja...*, s. 10.

nie spełnia wymagań formy szczególnej, a przede wszystkim – nie mogą być w ten sposób dokonane czynności, dla których ustawa zastrzega taką formę.

Przechodząc do rozważenia, czy należy dokonać zmian regulacji formy czynności prawnych ze względu na pojawienie się zjawiska inteligentnych kontraktów, należy zauważyć, że zmiany tego rodzaju mogłyby służyć większej formalizacji obrotu cywilnoprawnego albo – przeciwnie – jego odformalizowaniu poprzez wprowadzenie nowej, łagodniejszej formy czynności prawnych. Mogłyby być one połączone z rezygnacją z dotychczasowej, surowszej formuły przewidzianej dotychczas dla tych czynności⁴⁴.

Formalizacja obrotu w odniesieniu do inteligentnych kontraktów mogłaby polegać w szczególności na wprowadzeniu wymagania, aby umowy z wykorzystaniem takich rozwiązań informatycznych spełniały przesłanki określonej formy, np. dokumentowej, co umożliwiłoby identyfikację stron umowy. Należałoby wówczas przyjąć, że wymaganie to obowiązuje niezależnie od norm przewidujących formę surowszą. Z kolei odformalizowanie obrotu można by osiągnąć chociażby poprzez rezygnację z części obowiązujących wymagań formalnych tak, aby możliwe było zawarcie określonej umowy (np. leasingu) z wykorzystaniem inteligentnego kontraktu bez konieczności spełniania dodatkowych przesłanek przez strony.

Rozważenie obu przedstawionych możliwości należy poprzedzić dwoma ustaleniami. Po pierwsze, w prawie obcym w zasadzie nie występują regulacje dotyczące formy czynności prawnych odnoszące się bezpośrednio do inteligentnych kontraktów. Po drugie, w doktrynie bez większych kontrowersji przyjmuje się, że ustanowienie wymagań co do formy czynności prawnych służy realizacji następujących celów:

1. uchyleniu wątpliwości, czy oświadczenie woli zostało złożone, a więc wyraźniejszemu oddzieleniu stadiów przygotowujących dokonanie czynności prawnej od jej dokonania;
2. ułatwieniom dowodowym;
3. ochronie samych stron przed nieprzemyślanymi decyzjami;
4. jawności czynności prawnej w stosunku do osób trzecich;
5. ułatwieniu sprawowania kontroli państwa nad dokonywaniem czynności prawnych⁴⁵.

Odnosząc się, w pierwszej kolejności, do postulatu liberalizacji, warto zwrócić uwagę na fakt, że zalety inteligentnych kontraktów związane są przede wszystkim z zagwarantowaniem wykonania umowy oraz związanym z tym ograniczeniem kosztów jej zawarcia i wykonania. Jednocześnie nie ulega wątpliwości, że zastosowanie mechanizmu inteligentnego kontraktu nie umniejsza znaczenia wymienionych wyżej celów, a przeciwnie – w przypadku konieczności ochrony stron przed nieprzemyślanymi decyzjami wręcz zwiększa ich rangę. Racje

⁴⁴ J. Grykiel, *Kilka uwag...*, s. 236.

⁴⁵ K. Górską, *Zachowanie zwykłej formy pisemnej czynności prawnych*, Warszawa 2007, s. 16–20; M. Grochowski, *Wymogi formalne...*, s. 111; J. Kaspryszyn, *Podpis własnoręczny jako element zwykłej formy pisemnej czynności prawnych*, Warszawa 2007, s. 46–90; Z. Radwański, S. Czepita, E. Drozd, Z. Kuniewicz, S. Słotwiński, *Forma...*, s. 174.

leżące u podstaw wymagań co do formy w obowiązujących przepisach prawa pozostają nadal aktualne i brakuje powodów, żeby rezygnować z nich na potrzeby inteligentnych kontraktów.

Mechanizm ich działania skłaniałby raczej do rozważenia postulatu zaostrzenia wymagań formalnych, przede wszystkim w celu zagwarantowania ustalenia tożsamości stron umowy, a być może częściowo również w celu ochrony stron przed pochopnymi decyzjami. Niewątpliwie przede wszystkim postulat zapewnienia identyfikacji stron umowy jest na tyle istotny, że zasługuje na realizację. Należy jednak podać w wątpliwość skuteczność ewentualnych regulacji w tym zakresie.

Po pierwsze, praktyczne możliwości regulacji prawnej Internetu i wyegzekwowania przestrzegania wprowadzonych w tym celu norm są ograniczone⁴⁶. Dotyczy to również inteligentnych kontraktów. Po drugie, zawarcie i wykonanie umowy w Internecie sprawia, że co do zasady umowa tego rodzaju będzie obejmować tzw. elementy międzynarodowe, a zatem będzie wymagać ustalenia prawa właściwego. Podmioty korzystające z inteligentnych kontraktów mają szerokie możliwości, aby nawet w sytuacji z pozoru czysto wewnętrznej wprowadzić wyraźne powiązanie umowy z prawem w zasadzie dowolnego innego państwa.

Prawo właściwe dla wymagań formalnych umów należy ustalić na podstawie norm kolizyjnych prawa prywatnego międzynarodowego. W zakresie zobowiązujących skutków umowy zastosowanie znajdują normy rozporządzenia Rzym I o prawie właściwym dla zobowiązań umownych⁴⁷. Poza wymienionym zakresem, a więc między innymi w odniesieniu do rzeczowych skutków umowy, zastosowanie znajdują normy kolizyjne polskiej ustawy – Prawo prywatne międzynarodowe⁴⁸.

Zarówno w powołanym rozporządzeniu (art. 11), jak i w ustawie (art. 25) przyjęto stosowaną od dawna w prawie prywatnym międzynarodowym zasadę, zgodnie z którą wystarczy zachowanie formy przewidzianej w prawie państwa wskazanego przynajmniej jednym z kilku wskazanych alternatywnie łączników. Nie ulega wątpliwości, że taka konstrukcja wskazania prawa właściwego służy utrzymaniu czynności prawnej w mocy ze względu na formę, jeżeli czynność ta spełnia wymagania formalne przynajmniej jednego z systemów prawnych, z którym wykazuje dostateczny związek.

W rezultacie ze względu na treść powyższych regulacji oraz międzynarodowy charakter umów zawieranych przez Internet ustanawianie wymagań formalnych dla deklaracji zawieranych w ten sposób należy uznać za mało skuteczne. Jest bowiem bardzo prawdopodobne, że umowa okaże się ważna i skuteczna według innego prawa, z którym będzie odpowiednio związana.

⁴⁶ W.J. Kocot, *Elektroniczna forma...*, s. 4.

⁴⁷ Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 593/2008 z dnia 17 czerwca 2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I) (OJ L 177, 4.7.2008, p. 6–16).

⁴⁸ Ustawa z dnia 4 lutego 2011 r. – Prawo prywatne międzynarodowe (t.j. Dz. U. z 2015 r. poz. 1792).

Należy jednak zauważyć, że w przypadku umów konsumenckich prawem właściwym dla zobowiązujących skutków umowy jest wyłącznie prawo miejsca zwykłego pobytu konsumenta (art. 11 ust. 4 rozporządzenia Rzym I). Umożliwia to uregulowanie przez polskiego ustawodawcę formy umów zawieranych przy wykorzystaniu inteligentnych kontraktów przez konsumentów mających miejsce zwykłego pobytu w Polsce. Nadal można mieć jednak wątpliwości co do praktycznej skuteczności takich regulacji oraz co do szczegółowej ich treści.

3. Pieczęć elektroniczna

Problematyka prawna pieczęci elektronicznej została uregulowana w rozporządzeniu eIDAS⁴⁹. Według definicji legalnej, zamieszczonej w art. 3 pkt 25 tego rozporządzenia, pieczęcią elektroniczną są dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane po to, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych informacji. Pieczęć elektroniczną składa się przy pomocy urządzenia służącego do składania tego typu danych, którym zgodnie z art. 3 pkt 31 rozporządzenia eIDAS jest skonfigurowane oprogramowanie lub sprzęt wykorzystywany w tym celu.

W rozporządzeniu uregulowano dwie kwalifikowane postacie pieczęci elektronicznej. Zaawansowana pieczęć elektroniczna to taka, która spełnia następujące przesłanki:

- a) jest unikalnie przyporządkowana podmiotowi składającemu pieczęć;
- b) umożliwia ustalenie tożsamości podmiotu składającego pieczęć;
- c) jest składana przy użyciu danych służących do składania pieczęci elektronicznej, które podmiot składający pieczęć może, mając je z dużą dozą pewności pod swoją kontrolą, użyć do złożenia pieczęci elektronicznej;
- d) jest powiązana z danymi, do których się odnosi, w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna (art. 3 pkt 26 i art. 36 rozporządzenia eIDAS).

Według art. 3 pkt 24 rozporządzenia eIDAS pojęcie podmiotu składającego pieczęć elektroniczną oznacza osobę prawną, która składa pieczęć elektroniczną. Wynika stąd, że zaawansowana pieczęć elektroniczna nie musi umożliwiać ustalenia tożsamości osoby fizycznej, która się nią posługuje. Wystarczająca jest możliwość ustalenia osoby prawnej, której dane zostały oznaczone pieczęcią.

Z kolei kwalifikowana pieczęć elektroniczna została w art. 3 pkt 27 rozporządzenia eIDAS zdefiniowana jako pieczęć, która spełnia wymagania pieczęci zaawansowanej. Ponadto musi

⁴⁹ Rozporządzenie Parlamentu Europejskiego i Rady z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (OJ L 257, 28.8.2014, p. 73-14).

być ona złożona za pomocą kwalifikowanego urządzenia do składania pieczęci elektronicznej i musi opierać się na kwalifikowanym certyfikacie pieczęci elektronicznej.

Certyfikat pieczęci elektronicznej to z kolei poświadczenie elektroniczne, które łączy dane służące do walidacji pieczęci elektronicznej z osobą prawną i potwierdza nazwę tej osoby (art. 3 pkt 29 rozporządzenia eIDAS). Certyfikat jest kwalifikowany wówczas, jeżeli jest wydawany przez kwalifikowanego dostawcę usług zaufania, a ponadto zawiera (art. 3 pkt 30 i załącznik nr III do rozporządzenia eIDAS):

- a) wskazanie – co najmniej w postaci pozwalającej na automatyczne przetwarzanie – że dany certyfikat został wydany jako kwalifikowany certyfikat pieczęci elektronicznej;
- b) zestaw danych jednoznacznie reprezentujących kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane certyfikaty, obejmujący co najmniej państwo członkowskie, w którym dostawca ma siedzibę, oraz
 - i. w odniesieniu do osoby prawnej: nazwę i, w stosownym przypadku, numer rejestrowy zgodnie z oficjalnym rejestrem;
 - ii. w odniesieniu do osoby fizycznej: imię i nazwisko tej osoby;
- c) co najmniej nazwę podmiotu składającego pieczęć i, w stosownym przypadku, numer rejestrowy zgodnie z oficjalnym rejestrem;
- d) dane służące do walidacji pieczęci elektronicznej, które odpowiadają danym służącym do składania pieczęci elektronicznej;
- e) dane dotyczące początku i końca okresu ważności certyfikatu;
- f) kod identyfikacyjny certyfikatu, który musi być niepowtarzalny dla kwalifikowanego dostawcy usług zaufania;
- g) zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną wydającego kwalifikowanego dostawcy usług zaufania;
- h) miejsce, w którym nieodpłatnie dostępny jest certyfikat towarzyszący zaawansowanemu podpisowi elektronicznemu lub zaawansowanej pieczęci elektronicznej, o których mowa w lit. g);
- i) miejsce usług, z których można skorzystać w celu złożenia zapytania o status ważności kwalifikowanego certyfikatu;
- j) jeżeli dane służące do składania pieczęci elektronicznej powiązane z danymi służącymi do walidacji pieczęci elektronicznej znajdują się w kwalifikowanym urządzeniu do składania pieczęci elektronicznej, odpowiednie wskazanie tego faktu co najmniej w postaci pozwalającej na automatyczne przetwarzanie.

Natomiast urządzenie do składania pieczęci elektronicznej uznaje się za kwalifikowane, jeżeli spełnia wymagania przewidziane dla kwalifikowanego urządzenia do składania podpisu elektronicznego, obejmujące w szczególności (art. 3 pkt 32 i załącznik nr 2 rozporządzenia eIDAS):

- a) zagwarantowanie poufności użytych danych;
- b) zapewnienie jednorazowego wystąpienia użytych danych;
- c) uniemożliwienie pozyskania użytych danych oraz skuteczną ochronę przed sfałszowaniem;
- d) możliwość skutecznej ochrony danych przez używającą ich osobę przed użyciem ich przez innych;
- e) niezmiennianie danych, które mają być podpisane;
- f) zapewnienie, że dane służące do składania podpisu będą generowane lub zarządzane wyłącznie przez kwalifikowanego dostawcę usług zaufania;
- g) ograniczenie kopiowania danych służących do składania podpisu przez kwalifikowanych dostawców usług zaufania wyłącznie w celu utworzenia kopii zapasowej i z zastrzeżeniem dalszych wskazanych ograniczeń.

Przedstawione przepisy rozporządzenia regulują w zasadzie techniczne warunki poszczególnych rodzajów pieczęci elektronicznej. Wymagania te odnoszą się przede wszystkim do zapewnienia bezpieczeństwa danych, przesyłania ich wyłącznie przez uprawnione osoby oraz ograniczenia możliwości celowej albo przypadkowej utraty danych lub ich zniekształcenia. Prawodawca unijny skoncentrował się w rozporządzeniu na ustanowieniu podstaw prawnych dla bezpiecznego przesyłania danych.

Z rozbudowaną regulacją wymagań technicznych kontrastuje ograniczone unormowanie skutków prawnych zastosowania poszczególnych postaci pieczęci elektronicznych. Zaawansowana pieczęć elektroniczna występuje w przepisach rozporządzenia określających wymagania innych uregulowanych rozporządzeniem rozwiązań (art. 42 ust. 1 lit. c – kwalifikowany elektroniczny znacznik czasu, art. 44 ust. 1 lit. d – kwalifikowane usługi rejestrowanego doręczenia elektronicznego, załącznik 1 lit. g – kwalifikowany certyfikat podpisu elektronicznego, załącznik IV lit. h – kwalifikowany certyfikat uwierzytelniania witryn internetowych). Ponadto art. 37 rozporządzenia dotyczy określonej tam szczegółowo sytuacji stosowania zaawansowanej (ust. 1 i 2) oraz kwalifikowanej (ust. 3) pieczęci elektronicznej w usługach publicznych.

Treść przepisów rozporządzenia wskazuje, że pieczęć elektroniczna oraz jej kwalifikowane postaci służą do identyfikacji osób prawnych przede wszystkim na potrzeby korzystania z usług publicznych. W art. 2 ust. 3 rozporządzenia jednoznacznie wskazano, że nie ma ono wpływu na prawo krajowe ani unijne związane z zawieraniem i ważnością umów lub innych zobowiązań prawnych oraz proceduralnych, które dotyczy ich formy. Przy interpretacji tego postanowienia można się odwołać do motywu 21 preambuły rozporządzenia, zgodnie z którym nie powinno ono również obejmować aspektów związanych z zawieraniem i ważnością umów lub innych obowiązków prawnych, w przypadku gdy istnieją wymogi dotyczące formy, wprowadzone na mocy prawa krajowego lub unijnego. Dodatkowo rozporządzenie w zakresie formy nie powinno mieć wpływu na krajowe wymogi, które dotyczą rejestrów publicznych,

w szczególności rejestrów handlowych i rejestrów gruntów. W doktrynie wskazuje się, że nie ma przeszkód, aby cywilnoprawne skutki posługiwania się pieczęcią elektroniczną uregulować w prawie wewnętrznym państw członkowskich⁵⁰.

Znaczenie dla obrotu cywilnoprawnego wydają się mieć również przepisy art. 35 rozporządzenia. Na tej podstawie pieczęć elektronicznej nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że pieczęć ta ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych pieczęci elektronicznych (ust. 1). Z przepisu wynika między innymi zakaz nieuwzględnienia pieczęci elektronicznej w ramach ustalania faktów w postępowaniu cywilnym. Brakuje jednak przepisów, które wiązałyby z posłużeniem się pieczęcią elektroniczną określone skutki prawne. Wykorzystanie jej należy zatem brać pod uwagę jako jeden z faktów opiniowanych zgodnie z zasadami swobodnej oceny dowodów, stosownie do art. 233 § 1 k.p.c.

Według art. 35 ust. 2 rozporządzenia kwalifikowana pieczęć elektroniczna korzysta z domniemania integralności danych i autentyczności pochodzenia tych danych, z którymi kwalifikowana pieczęć elektroniczna jest powiązana. Zakres zastosowania tego przepisu nie został w żaden sposób ograniczony, więc zasadny jest wniosek, że ustanowione w nim domniemanie obowiązuje również w obrocie cywilnoprawnym. Jego znaczenie wydaje się jednak ograniczone. W braku tego przepisu ciężar udowodnienia, że dane opatrzone pieczęcią są niepoprawne, obciążałby również osobę, która się na to powołuje.

Z kolei według art. 35 ust. 3 rozporządzenia kwalifikowana pieczęć elektroniczna oparta na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim Unii Europejskiej jest uznawana za kwalifikowaną pieczęć elektroniczną we wszystkich pozostałych państwach członkowskich. Z przepisu tego wynika obowiązek uznawania w Polsce skutków prawnych posłużenia się pieczęcią elektroniczną, wydaną w innym państwie członkowskim. Dotyczy to zarówno skutków określonych w rozporządzeniu, jak również takich, które zostałyby przewidziane w prawie wewnętrznym.

Rozważając, czy polski ustawodawca powinien ustanowić przepisy szczególne, które dotyczyłyby składania oświadczeń woli przy pomocy pieczęci elektronicznej, należy wziąć pod uwagę, że regulacje tego rodzaju w zasadzie nie są przyjmowane w innych państwach członkowskich. Rozstrzygające znaczenie powinien mieć jednak sposób działania pieczęci elektronicznej oraz związane z tym funkcje tego rozwiązania technicznego. Według motywu 59 rozporządzenia eIDAS pieczęcie elektroniczne powinny służyć jako dowód wydania danego dokumentu elektronicznego przez daną osobę prawną, zapewniając co do pochodzenia i integralności dokumentu. Z przedstawionych powyżej regulacji rozporządzenia można wnioskować, że wymagane rozwiązania techniczne pozwalają na realizację tych celów. Z kolei w motywie 65 stwierdzono, że pieczęcie elektroniczne mogą być używane nie tylko do

⁵⁰ Ł. Goździaszek, *Identyfikacja elektroniczna i usługi zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym Unii Europejskiej. Komentarz*, Warszawa 2019, uwagi do art. 2.

poświadczenia dokumentu wydanego przez osobę prawną, lecz również do uwierzytelniania wszelkich zasobów cyfrowych osoby prawnej, takich jak kod oprogramowania lub serwery.

Nie ulega wątpliwości, że pieczęcią elektroniczną można opatrzyć również dokument wyrażający oświadczenie woli. Uogólniając, posłużenie się pieczęcią może stanowić zachowanie stanowiące element oświadczenia woli – zgodnie z przyjętymi regułami wykładni. Dopuszczenie składania oświadczeń woli przy pomocy pieczęci elektronicznej nie wymaga żadnych zmian w obowiązujących przepisach prawa cywilnego.

Jak wynika z wcześniejszych rozważań dotyczących inteligentnych kontraktów, oświadczenie złożone z zastosowaniem pieczęci elektronicznej może spełniać wymagania formy dokumentowej, bez potrzeby wprowadzania w tym celu dodatkowych regulacji. Jednocześnie nie spełnia ono wymagań formy pisemnej, dla zachowania której konieczne jest złożenie własnoręcznego podpisu. Uznanie oświadczenia woli opatrzonego pieczęcią elektroniczną za równoważne oświadczeniu woli złożonemu w formie pisemnej wymagałoby ustanowienia przepisu ustawy o treści zbliżonej do art. 78¹ § 2 k.c., w którym zrównano co do skutków prawnych formę pisemną i formę elektroniczną – wymagającą zaopatrzenia oświadczenia kwalifikowanego w podpis elektroniczny.

Funkcje podpisu i formy pisemnej były wielokrotnie przedmiotem wypowiedzi doktryny. Pomimo pewnych różnic między wyrażanymi poglądami, w zasadzie zgodnie przyjmuje się, że podpis ma umożliwiać identyfikację podpisującego, zapewnić integralność treści podpisywanego oświadczenia oraz wskazywać na doniosłość prawną złożenia podpisu, a tym samym chronić przed pochopnym złożeniem oświadczenia woli. W odniesieniu do funkcji identyfikacji można zauważyć, że chodzi nie tylko o wskazanie osoby składającej podpis, ale również o możliwość ustalenia – w razie wątpliwości przy wykorzystaniu wiedzy specjalistycznej z zakresu analizy porównawczej pisma ręcznego – czy oświadczenie rzeczywiście pochodzi od wskazanej osoby⁵¹. Jest to zatem identyfikacja rozumiana inaczej niż w art. 77² k.c., dotyczącym formy dokumentowej, która nie wymaga, aby możliwe było ustalenie rzeczywistej tożsamości osoby składającej oświadczenie. Przewidziane w licznych przepisach wymaganie zachowania formy pisemnej można rozumieć w ten sposób, że ustawodawca uznał za stosowne, aby w razie potrzeby istniała możliwość ustalenia rzeczywistej tożsamości składającego podpis.

Opatrzenie oświadczenia pieczęcią elektroniczną pozwala ustalić, że oświadczenie to pochodzi od określonej osoby prawnej. Nie umożliwia jednak poznania osoby fizycznej, która pieczęcią się posługuje. Użycie pieczęci nie stanowi zatem – odmiennie niż zastosowanie kwalifikowanego podpisu elektronicznego – funkcjonalnego odpowiednika własnoręcznego

⁵¹ A. Ambroziewicz, *Podpis elektroniczny – pojęcie i funkcje w obrocie*, „Przegląd Sądowy” 2001, nr 1, s. 101–102; A. Jędrzejewska, *Pisemna forma oświadczenia woli a „automatyzacja” obrotu prawnego*, „Państwo i Prawo” 1993, z. 1, s. 70; W.J. Kocot, *Elektroniczna forma...*, s. 5.

podpisu. Z tego powodu nie wydaje się zasadne uznawanie oświadczeń woli opatrzonych pieczęcią elektroniczną za równoważne oświadczeniom w formie pisemnej.

Ustalenie, że oświadczenie woli zostało skutecznie złożone przez osobę prawną, wymaga stwierdzenia, że nadawca oświadczenia nie tylko jest związany z tą osobą prawną, funkcjonuje w jej strukturze i ma faktyczną możliwość posługiwania się jej zasobami, ale również tego, że jest umocowany do złożenia danego oświadczenia. Umocowanie to może wynikać w szczególności z działania w charakterze organu osoby prawnej, współnika spółki osobowej, prokurenta lub pełnomocnika. Pełnomocnictwo może być udzielone w sposób dorozumiany. W praktyce obrotu cywilnoprawnego oświadczenia niewymagające formy szczególnej są niejednokrotnie składane przez osoby, którym nie udzielono pełnomocnictwa na piśmie. Ich umocowanie jest wówczas ustalane na podstawie okoliczności danego przypadku, zgodnie z zasadami wykładni oświadczeń woli. Jedną z okoliczności branych pod uwagę może być fakt udostępnienia danej osobie urządzeń umożliwiających posługiwanie się pieczęcią elektroniczną danej osoby prawnej. Rozważyć można przyjęcie w polskiej ustawie domniemania, że oświadczenie woli opatrzone pieczęcią elektroniczną osoby prawnej zostało złożone przez tę osobę prawną. Wydaje się jednak, że taka nowelizacja nie jest niezbędna, a podobny skutek można osiągnąć na zasadzie domniemania faktycznego.

Inną możliwością jest dopuszczenie, aby pieczęć elektroniczna zawierała informacje dotyczące reprezentacji danej osoby prawnej. Takie rozwiązanie, opatrzone zastrzeżeniem, że zasady reprezentacji powinny być wykazane kwalifikowanemu dostawcy usług zaufania, przewidziano w § 12 ust. 3 zd. 2 niemieckiej ustawy o usługach zaufania (*Vertrauensdienstegesetz*) z 18 lipca 2017 roku⁵².

4. Podpis biometryczny

Biometria jest nauką zajmującą się badaniem metod identyfikacji ludzi w oparciu o cechy fizyczne⁵³. Obecnie różne metody biometryczne są wykorzystywane w ograniczonym zakresie w niektórych dziedzinach polskiego prawa publicznego. Brak jest natomiast szczególnych regulacji poświęconych temu zagadnieniu w prawie prywatnym. Podobna sytuacja występuje również w systemach prawnych innych państw⁵⁴.

⁵² Dostępna na stronie internetowej: <https://www.gesetze-im-internet.de/vdg/BJNR274510017.html> [dostęp: 12.11.2021].

⁵³ P. Polański, *Podpisy elektroniczne w prawie polskim i wspólnotowym*, „Rejent” 2008, nr 9, s. 89.

⁵⁴ M. Maciejewska-Szałas, *Forma pisemna i elektroniczna czynności prawnych. Studium prawnoporównawcze*, Warszawa 2014, s. 7.

W art. 4 pkt 14 RODO⁵⁵ zawarto definicję legalną pojęcia *dane biometryczne*. Oznacza ono dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby. Informacje te mogą dotyczyć wizerunku twarzy lub danych daktyloskopijnych. W literaturze dotyczącej tego zagadnienia wyróżnia się biometryczne cechy fizyczne (np. tęczęwka, siatkówka oka, geometria twarzy lub dłoni, linie papilarne, barwa głosu, układ linii krwionośnych dłoni) oraz biometryczne cechy behawioralne (np. sposób mówienia, składania podpisu własnoręcznego, pisanie na klawiaturze). Ich wykorzystanie na potrzeby identyfikacji wymaga pomiaru przy pomocy urządzenia do badania właściwości biologicznych człowieka oraz zapisu w postaci danych elektronicznych⁵⁶.

Pojęcie podpisu biometrycznego nie występuje w języku prawnym. W najszerszym znaczeniu oznacza ono dowolną metodę, wykorzystującą dane biometryczne do identyfikacji osoby fizycznej, która dokonuje czynności mającej znaczenie prawne. Podpis biometryczny bywa również rozumiany jako synonim biometrycznego podpisu własnoręcznego. Jest to system, w którym na potrzeby identyfikacji osoby składającej podpis wykorzystuje się cechę biometryczną w postaci dynamiki pisma manualnego. Podpis składany jest przy pomocy specjalnego urządzenia, które składa się z elektronicznego pióra i podkładki. Maszyna ta mierzy i zapisuje cechy biometryczne pisma, takie jak: prędkość, miarowość, forma, kolejność pociągnięć, siła nacisku na podłoże. Cechy te mogą być następnie porównane z innym podpisem, pozwalając tym samym na ustalenie, czy złożyła je ta sama osoba⁵⁷. Możliwe jest również porównanie podpisu złożonego w ten sposób z podpisem złożonym w sposób tradycyjny, na papierze, przy pomocy długopisu albo innego podobnego urządzenia⁵⁸.

Według innych interpretacji podpis biometryczny jest rodzajem podpisu elektronicznego, który jest oparty na systemie szyfrowania asymetrycznego. Metoda ta zakłada, że złożenie podpisu wymaga posłużenia się dwoma kluczami (kodami) – prywatnym i publicznym – przypisanymi do danej osoby. Klucz publiczny umieszcza się w publicznym rejestrze. Umożliwia to ustalenie danych osoby, do której dany klucz należy. Z kolei klucz prywatny, aby wyeliminować złożenie podpisu przez podmiot nieuprawniony, nie powinien być udostępniany innym. Powiązanie kluczy z oznaczoną osobą następuje poprzez przyznanie tzw. certyfikatu

⁵⁵ 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) (OJ L 119, 4.5.2016, p. 1–88).

⁵⁶ L. Brazell, *Electronic Signatures Law and Regulation*, London 2004, s. 39.

⁵⁷ S. Mason, *The International Implications of Using Electronic Signatures*, „Computer and Telecommunications Law Review” 2005, nr 5, s. 160; P. Polański, *Podpisy elektroniczne...*, s. 90–91.

⁵⁸ V. Smejkal, J. Kodl, J. Kodl Jr., *Implementing Trustworthy Dynamic Biometric Signature according to the Electronic Signature Regulations*, s. 167–170, [online:] https://www.researchgate.net/publication/286759033_Implementing_trustworthy_dynamic_biometric_signature_according_to_the_electronic_signature_regulations [dostęp: 12.11.2021].

przez organ certyfikacyjny⁵⁹. W doktrynie nierzadko wskazuje się, że opisane rozwiązanie to klucz cyfrowy, który jest jedynie rodzajem klucza elektronicznego, stanowiącego pojęcie o szerszym zakresie znaczeniowym⁶⁰.

Algorytmy stosowane w podpisie elektronicznym powodują, że jakakolwiek zmiana przesyłanych danych zostaje wykryta. Zapewnia to trwałość przesłanej informacji i uniemożliwia podrobienie podpisu cyfrowego⁶¹. Możliwość złożenia podpisu przez osobę nieuprawnioną pojawia się natomiast w przypadku uzyskania dostępu do cudzego klucza prywatnego. Wykorzystanie jako klucza prywatnego danych biometrycznych zapewnia bezpieczeństwo wyższe niż w standardowej procedurze asymetrycznego szyfrowania. Unikalny klucz prywatny nie wymaga bezpiecznego przechowywania i nie istnieje ryzyko, że może wpaść w niepowołane ręce – jest on stały dla danego użytkownika, nie ma zatem możliwości jego użycia przez inną osobę⁶². W charakterze klucza prywatnego mogą zostać wykorzystane dowolne dane, które identyfikują jednoznacznie osobę fizyczną. Najczęściej wymienia się wśród nich: odcisk palca, wzór tęczy, DNA, wizerunek twarzy⁶³.

Problematyka podpisu biometrycznego nie jest przedmiotem specjalnych regulacji w ustawodawstwie poszczególnych państw. Również w doktrynie wprowadzenie takich przepisów nie jest szerzej proponowane. W tym zakresie rozważane jest raczej zagadnienie, czy podpis biometryczny spełnia przesłanki formy pisemnej – w znaczeniu przyjętym w poszczególnych systemach prawnych – lub przesłanki podpisu elektronicznego w rozumieniu rozporządzenia eIDAS⁶⁴.

Na podstawie obowiązującego prawa polskiego oświadczenie woli opatrzone podpisem biometrycznym spełnia wymagania formy dokumentowej, nie spełnia natomiast wymagań formy pisemnej lub elektronicznej. Podobna sytuacja występuje między innymi w prawie niemieckim⁶⁵. Natomiast w prawie francuskim funkcjonujące tam pojęcie dowodu na piśmie obejmuje zarówno informację zapisaną w dokumencie papierowym, jak i elektronicznym, jeżeli pozwala na ustalenie tożsamości autora i gwarantuje integralność treści. Przedstawiona norma została wprowadzona nowelizacją kodeksu cywilnego francuskiego z 2000 roku, która potwierdziła wcześniejsze orzecznictwo⁶⁶. Podobne rozumienie wymagań formy pisemnej,

⁵⁹ J. Jacyszyn, *Elektroniczne czynności prawne*, „Przegląd Prawa Handlowego” 1999, nr 7, s. 31; W.J. Kocot, *Elektroniczna forma...*, s. 6–7.

⁶⁰ Ł. Neuman, M. Świerczyński, *Podpis elektroniczny – prawne i techniczne objaśnienie pojęć*, „Monitor Prawniczy” 2001, nr 11, s. 590.

⁶¹ Tamże, s. 591.

⁶² L. Brazell, *Electronic Signatures...*, s. 40; M. Marucha-Jaworska, *Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym*, Warszawa 2015, s. 179–182; K.J. Pawan, M.Y. Siyal, *Novel Biometric Digital Signatures for Internet Based Applications*, „Information Management & Computer Security” 2001, nr 9, s. 205–212.

⁶³ M. Bromby, *Identification, trust and privacy: How biometrics can aid certification of digital signatures*, „International Review of Law, Computers & Technology” 2010, t. 24, nr 1, March 2010, s. 136.

⁶⁴ V. Smejkal, J. Kodl, J. Kodl Jr., *Implementing...*, s. 165–167.

⁶⁵ M. Maciejewska-Szałas, *Forma pisemna...*, s. 293–302.

⁶⁶ A. Krasuski, *Status prawny sztucznego agenta. Podstawy prawne zastosowania sztucznej inteligencji*, Warszawa 2021, par. 1; M. Maciejewska-Szałas, *Forma pisemna...*, s. 426–428;

odwołujące się do argumentów funkcjonalnych, proponowano również w regulacji polskiej⁶⁷. W doktrynie i orzecznictwie przeważa jednak pogląd, że niezbędnym elementem formy pisemnej jest własnoręczny podpis⁶⁸, a to wyklucza spełnienie wymagań tej formy przez jakikolwiek przekaz danych drogą elektroniczną, w tym również przy pomocy omawianego tu podpisu biometrycznego.

W związku z tym pojawia się pytanie, czy skutki prawne podpisu biometrycznego należy zrównać ze skutkami podpisu własnoręcznego *de lege ferenda*. Jak wskazano wyżej, podpis biometryczny umożliwia jednoznaczną identyfikację składającej go osoby⁶⁹. Wydaje się, że przy odpowiednim uregulowaniu technicznego sposobu składania takiego podpisu możliwe byłoby zachowanie również pozostałych funkcji podpisu tradycyjnego.

Zrównanie skutków prawnych podpisu elektronicznego i tradycyjnego wymagałoby ponadto uwzględnienia negatywnych konsekwencji korzystania z danych biometrycznych. Wśród wad podpisu biometrycznego wymienia się między innymi brak zapewnienia integralności danych oraz możliwość ich utraty lub bezprawnego ujawnienia⁷⁰. Znaczenie tych okoliczności jest jednak uwarunkowane technicznie, a zatem zmienne, a przy tym – trudne do oceny dla osób, które nie posiadają specjalistycznej wiedzy. Niezależnie od rzeczywistego zagrożenia można jednak spodziewać się, że wprowadzenie podpisu biometrycznego będzie związane z obawami potencjalnych użytkowników, dotyczącymi naruszenia prywatności lub bezprawnego wykorzystania danych biometrycznych⁷¹.

W doktrynie wyrażono stanowisko, że prawne rozumienie podpisu powinno być wyznaczone jego funkcją, natomiast sposób złożenia podpisu powinien być uregulowany w sposób technologicznie neutralny⁷². Pogląd ten można podawać jako uzasadnienie postulatu zmiany przepisów regulujących formę pisemną czynności prawnych, w szczególności art. 78 § 1 k.c., w taki sposób, aby możliwe było jej zachowanie przy pomocy podpisów różnego rodzaju. Byłaby to daleko idąca zmiana dotycząca podstawowych regulacji polskiego prawa cywilnego. Rozwiązaniem alternatywnym mogłoby być uregulowanie podpisu biometrycznego w odrębnym akcie prawnym oraz ustanowienie przepisu zrównującego skutki prawne oświadczenia woli opatrzonego takim podpisem z oświadczeniem woli w formie pisemnej.

W opracowaniach dotyczących kwestii identyfikacji elektronicznej wskazuje się, że wprowadzenie podpisu biometrycznego wymaga rozstrzygnięcia i uregulowania szeregu zagadnień szczegółowych. Na uwagę zasługuje pogląd, że dla powstania automatycznego systemu uwierzytelniania lub identyfikacji określonej osoby potrzebne są:

⁶⁷ W.J. Kocot, *Forma oświadczenia woli...*, s. 86–87.

⁶⁸ Z. Radwański, *Uwagi ogólne o zakresie stosowania formy elektronicznej w prawie cywilnym*, [w:] *Rozprawy prawnicze. Księga pamiątkowa Profesora Maksymiliana Pazdana*, red. L. Ogiełło, W. Popiołek, M. Szpunar, Kraków 2005, s. 1297.

⁶⁹ M. Marucha-Jaworska, *Podpisy elektroniczne...*, s. 179.

⁷⁰ M. Maciejewska-Szałas, *Forma pisemna...*, s. 7–8.

⁷¹ Tamże, s. 8.

⁷² W.J. Kocot, *Elektroniczna forma...*, s. 5.

1. odpowiednia cecha biometryczna;
2. naukowe rozpoznanie tej cechy;
3. możliwości techniczne dla zbudowania detektora danej cechy;
4. odpowiednie metody informatyczne do szybkiej analizy i porównywania danych biometrycznych;
5. właściwa implementacja systemu;
6. biometryczna baza danych⁷³.

Wydaje się, że powyższy wykaz jest aktualny zarówno w przypadku opracowywania projektu regulacji w prawie powszechnie obowiązującym, jak również w odniesieniu do projektowania systemu podpisu biometrycznego przez dowolną jednostkę organizacyjną na wewnętrzne potrzeby, w ramach obowiązującego prawa. Zagadnieniem wymagającym rozstrzygnięcia w pierwszej kolejności jest dobór odpowiedniej cechy (cech) biometrycznej używanej na potrzeby identyfikacji. Wskazuje się, że powinna ona mieć następujące właściwości:

1. uniwersalność – każda osoba powinna posiadać daną cechę biometryczną;
2. jednoznaczność – powinna istnieć możliwość rozróżnienia każdej z dwóch osób na podstawie danej cechy biometrycznej;
3. trwałość – niezmiennność danej cechy biometrycznej w czasie;
4. mierzalność – możliwość nieinwazyjnego zmierzenia danej cechy biometrycznej;
5. akceptowalność – pomiar danej cechy biometrycznej powinien być akceptowany społecznie⁷⁴.

Wśród cech biometrycznych stosowanych na potrzeby podpisu biometrycznego na uwagę zasługuje elektroniczne utrwalanie dynamiki pisma ręcznego. Zakładając techniczną możliwość wdrożenia rozwiązania tego rodzaju, zachowuje ono zalety pozostałych metod identyfikacji biometrycznej. Jednocześnie odpowiada zakorzenionej głęboko społecznej świadomości funkcji i doniosłości własnoręcznego podpisu. Wydaje się też, że gromadzenie i przetwarzanie danych o dynamice pisma ręcznego jest społecznie bardziej akceptowalne niż w przypadku wielu innych cech biometrycznych.

5. Wnioski

Sformułowanie wniosków dotyczących celowości nowelizacji przepisów prawa cywilnego w związku z pojawieniem się przedstawionych rozwiązań technicznych należy poprze-
dzić przytoczeniem nadal aktualnego stanowiska, że nowych zjawisk nie należy w prawie

⁷³ M. Marucha-Jaworska, *Podpisy elektroniczne...*, s. 171.

⁷⁴ R. Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, „Information Technology & People” 1994, t. 7, nr 4, s. 6–37.

cywilnym normować zbyt szybko. Pogląd ten uzasadniany jest rozmaicie. Wskazuje się, że trudno jest ocenić z góry zasięg i znaczenie nowych wynalazków⁷⁵, a ich pochopna regulacja mogłaby niepotrzebnie ograniczyć rozwój praktyki obrotu⁷⁶. Podzielając te argumenty, należy również zauważyć, że elastyczność i abstrakcyjny charakter norm prawa cywilnego w wielu przypadkach pozwalają na rozstrzyganie problemów prawnych dotyczących nowych zjawisk. Można w tym przypadku opowiedzieć się po stronie stanowiska, że w odniesieniu do nowelizacji materialnego prawa cywilnego, a przede wszystkim – jego regulacji ogólnych, do których należy problematyka oświadczenia woli i formy czynności prawnych, należy zachować ostrożność.

Powyższy pogląd w niejednakowym stopniu dotyczy poszczególnych rozwiązań, które zostały przeanalizowane w niniejszej pracy. Bez zastrzeżeń można go zaakceptować w odniesieniu do inteligentnych kontraktów. Jest to nowe rozwiązanie techniczne, którego znaczenie w praktyce obrotu cywilnoprawnego trudno przewidzieć⁷⁷. W prawie obcym w zasadzie brak jest szczególnych regulacji dotyczących inteligentnych kontraktów⁷⁸. Jednocześnie obowiązujące prawo polskie zdaje się stanowić odpowiednią podstawę do rozstrzygania zagadnień związanych z przypisaniem oświadczenia woli, ustaleniem treści umowy lub skutkami błędnego działania programu komputerowego. Z kolei skuteczność regulacji formy czynności prawnych wydaje się ograniczona zarówno ze względu na praktyczne uwarunkowania działania Internetu, jak i z uwagi na treść obowiązujących norm kolizyjnych prawa prywatnego międzynarodowego. Odmienne wnioski można z kolei sformułować w odniesieniu do inteligentnych kontraktów, które byłyby dostępne wyłącznie dla ograniczonego kręgu zidentyfikowanych użytkowników, np. w ramach platformy elektronicznej przeznaczonej do zawierania umów określonego rodzaju. Wówczas można by rozważyć chociażby przypisanie rozstrzygającego charakteru treści kodu w języku programowania przy wykładni oświadczenia woli lub ustalenie szczególnych wymagań co do formy czynności prawnych. Konkretna treść możliwych zmian wymagałaby jednak znajomości założeń funkcjonowania takiego systemu.

Pieczęć elektroniczna jest przedmiotem szczegółowych regulacji na poziomie prawa Unii Europejskiej. W rozporządzeniu eIDAS unormowano wymagania techniczne pieczęci elektronicznych oraz niektóre skutki posługiwania się nimi. Prawa prywatnego regulacje te dotyczą w bardzo ograniczonym zakresie. Pieczęć elektroniczna pozwala na wskazanie osoby prawnej, od której pochodzi określone oświadczenie woli, nie identyfikuje jednak osoby fizycznej, która się nią posługuje. Z tego względu niezasadne byłoby zrównanie skutków prawnych pieczęci elektronicznej i własnoręcznego podpisu. W związku z tym rozważyć

⁷⁵ E. Till, *O prawem...*, s. 3.

⁷⁶ K. Gajek, *Oświadczenie woli...*, rozdz. VI, par. 4.

⁷⁷ P.S. Bayón, *Key Legal Issues...*, s. 25–26.

⁷⁸ M. di Angelo, A. Soare, G. Salzer, *Smart Contracts...*, s. 1.

można ustanowienie domniemania, że oświadczenie woli opatrzone pieczęcią elektroniczną, albo którąś z jej kwalifikowanych postaci, zostało złożone przez osobę prawną. Nowelizacja tego rodzaju nie wydaje się jednak konieczna, gdyż podobne wnioski można przyjąć również na podstawie domniemania faktycznego.

Z kolei podpis biometryczny wydaje się stanowić bardzo perspektywiczne rozwiązanie, mogące znacząco ułatwić praktykę obrotu elektronicznego. Wprowadzenie regulacji prawnych w tym zakresie wydaje się nie tyle konieczne, co przydatne. Podpis biometryczny mógłby stanowić metodę identyfikacji osób fizycznych na potrzeby dokonywania czynności prawnych, która stanowiłaby surogat tradycyjnego podpisu. Wprowadzenie podpisu tego rodzaju wymagałoby jednak uregulowania szeregu przedstawionych wyżej zagadnień w oparciu o wybrane wcześniej założenia, począwszy od doboru stosowanej cechy biometrycznej. Wśród proponowanych cech interesującą perspektywą z punktu widzenia obrotu cywilnoprawnego wydaje się wykorzystanie dynamiki pisma ręcznego.

Bibliografia

- A Report by the UK Government Chief Scientific Adviser, Distributed Ledger Technology: beyond block chain*, Government Office for Science, 2016, [online:] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf [dostęp: 15.06.2021].
- Ambroziewicz A., *Podpis elektroniczny – pojęcie i funkcje w obrocie*, „Przegląd Sądowy” 2001, nr 1.
- di Angelo M., Soare A., Salzer G., *Smart Contracts in View of the Civil Code*, [online:] https://publik.tuwien.ac.at/files/publik_278278.pdf [dostęp: 12.11.2021].
- Bayón P.S., *Key Legal Issues Surrounding Smart Contract Applications*, „KLRI Journal of Law and Legislation” 2019, t. 9, nr 1.
- Brazell L., *Electronic Signatures Law and Regulation*, London 2004.
- Bromby M., *Identification, trust and privacy: How biometrics can aid certification of digital signatures*, „International Review of Law, Computers & Technology” 2010, t. 24, nr 1.
- Buterin V., *A Next Generation Smart contract and Decentralized Application Platform*, „Ethereum White Paper” 2018, [online:] http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [dostęp: 12.11.2021].
- Clarke R., *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, „Information Technology & People” 1994, t. 7, nr 4.
- Czachórski W., Brzozowski A., Safjan M., Skowrońska-Bocian E., *Zobowiązania. Zarys wykładu*, Warszawa 2009.
- Drozdowicz M., *Błąd w elektronicznych czynnościach prawnych*, „Przegląd Prawa Handlowego” 2001, nr 9.
- Fries M., *Smart Contracts: Brauchen schlaue Verträge noch Anwälte?*, „Anwaltsblatt” 2018, nr 2.
- Gajek K., *Oświadczenie woli w komunikacji elektronicznej*, Warszawa 2020.
- Goździaszek Ł., *Identyfikacja elektroniczna i usługi zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym Unii Europejskiej. Komentarz*, Warszawa 2019.
- Górecki J., *Forma umów obligacyjnych i rzeczowych w prawie prywatnym międzynarodowym*, Katowice 2007.
- Górska K., *Zachowanie zwykłej formy pisemnej czynności prawnych*, Warszawa 2007.

- Grinberg R., *Bitcoin: An Innovative Alternative Digital Currency*, „Hastings Science & Technology Law Journal” 2011, nr 4, [online:] <https://ssrn.com/abstract=1817857> [dostęp: 12.11.2021].
- Grochowski M., *Wymogi formalne w umowach konsumenckich*, Warszawa 2018.
- Grykiel J., *Kilka uwag o nowej definicji dokumentu i formie dokumentowej*, „Monitor Prawniczy” 2016, nr 5.
- Grzybowski S., *System prawa cywilnego*, t. III, cz. 1, Wrocław 1981.
- Hoser T., *Blockchain basics, commercial impacts and governance challenges*, „Governance Directions” 2016, nr 68.
- Jacyszyn J., *Elektroniczne czynności prawne*, „Przegląd Prawa Handlowego” 1999, nr 7.
- Jędrzejewska A., *Koncepcja oświadczenia woli w prawie cywilnym*, Warszawa 1992.
- Jędrzejewska A., *Oświadczenia woli składane za pomocą komputera (w świetle doświadczeń niemieckich)*, „Państwo i Prawo” 1992, nr 11.
- Jędrzejewska A., *Pisemna forma oświadczenia woli a „automatyzacja” obrotu prawnego*, „Państwo i Prawo” 1993, z. 1.
- Kakavand H., De Sevres N.K., Chilton B., *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*, 2017, [online:] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251 [dostęp: 12.11.2021].
- Kaspryszyn J., *Podpis własnoręczny jako element zwykłej formy pisemnej czynności prawnych*, Warszawa 2007.
- Klein A., *Pojęcie umowy i stosunku zobowiązaniowego kontraktacji według kodeksu cywilnego*, „Studia Cywilistyczne” 1972, t. XIX.
- Kocot W.J., *Dalsza modernizacja kodeksowej regulacji formy pisemnej czynności prawnej*, „Przegląd Prawa Handlowego” 2016, nr 10.
- Kocot W.J., *Elektroniczna forma oświadczeń woli*, „Przegląd Prawa Handlowego” 2001, nr 3.
- Kocot W.J., *Forma oświadczenia woli w dobie europeizacji polskiego prawa prywatnego*, [w:] *Rozprawy z prawa cywilnego, własności intelektualnej i prawa prywatnego międzynarodowego. Księga pamiątkowa dedykowana profesorowi Bogusławowi Gawlikowi*, red. J. Pisuliński, P. Tereszkievicz, F. Zoll, Warszawa 2012.
- Kocot W.J., *Wpływ Internetu na prawo umów*, Warszawa 2004.
- Köhler H., *Die Problematik automatisierter Rechtvorgänge, insbesondere von Willenserklärung*, „Archiv für die civilistische Praxis” 1982, nr 1-2.
- Krasuski A., *Status prawny sztucznego agenta. Podstawy prawne zastosowania sztucznej inteligencji*, Warszawa 2021.
- Machnikowski P., [w:] *System Prawa Prywatnego*, t. 5: *Prawo zobowiązań – część ogólna*, red. K. Osajda, wyd. 3, Warszawa 2020.
- Maciejewska-Szałas M., *Forma pisemna i elektroniczna czynności prawnych. Studium prawnoporównawcze*, Warszawa 2014.
- Marucha-Jaworska M., *Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym*, Warszawa 2015.
- Mason S., *The International Implications of Using Electronic Signatures*, „Computer and Telecommunications Law Review” 2005, nr 5.
- Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, [online:] <https://bitcoin.org/bitcoin.pdf> [dostęp: 12.11.2021].
- Neuman Ł., Świerczyński M., *Podpis elektroniczny – prawne i techniczne objaśnienie pojęć*, „Monitor Prawniczy” 2001, nr 11.
- Ohanowicz A., Górski J., *Zobowiązania. Zarys według kodeksu cywilnego. Część szczegółowa*, Warszawa-Poznań 1966.
- Pawan K.J., Siyal M.Y., *Novel Biometric Digital Signatures for Internet Based Applications*, „Information Management & Computer Security” 2001, nr 9.
- Peters G.W., Panayi E., *Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*, [online:] <https://ssrn.com/abstract=2692487> [dostęp: 12.11.2021].
- Polański P., *Podpisy elektroniczne w prawie polskim i wspólnotowym*, „Rejent” 2008, nr 9.

- Radwański Z., *Uwagi ogólne o zakresie stosowania formy elektronicznej w prawie cywilnym*, [w:] *Rozprawy prawnicze. Księga pamiątkowa Profesora Maksymiliana Pazdana*, red. L. Ogiełło, W. Popiołek, M. Szpunar, Kraków 2005.
- Radwański Z., Olejniczak A., *Zobowiązania. Część ogólna*, wyd. 12, Warszawa 2016.
- Radwański Z., Czepita S., Drozd E., Kuniewicz Z., Słotwiński S., *Forma czynności prawnej*, [w:] *System Prawa Prywatnego*, t. 2: *Prawo cywilne – część ogólna*, wyd. 3, Warszawa 2019.
- Rajski J., [w:] Kocot W., Zaradkiewicz K., *Prawo o kontraktach w obrocie gospodarczym*, Warszawa 2002.
- Raskin M., *The Law and Legality of Smart Contracts*, 2017, [online:] <https://doi.org/10.2139/ssrn.2842258> [dostęp: 12.11.2021].
- Szabo N., *The Idea of Smart Contracts*, 1997, [online:] https://web.archive.org/web/20060615044959/http://szabo.best.vwh.net/smart_contracts_idea.html [dostęp: 12.11.2021].
- Smejkal V., Kodl J., Kodl J. Jr., *Implementing Trustworthy Dynamic Biometric Signature according to the Electronic Signature Regulations*, [online:] https://www.researchgate.net/publication/286759033_Implementing_trustworthy_dynamic_biometric_signature_according_to_the_electronic_signature_regulations [dostęp: 12.11.2021].
- Till E., *O znaczeniu prawnem automatu*, Lwów 1900.
- Kaulartz M., Heckmann J., *Smart Contracts – Anwendungen der Blockchain-Technologie*, „Computer und Recht” 2016, nr 9.
- Walch A., *The Path of the Blockchain Lexicon (and the Law)*, „Review of Banking & Finance” 2017, nr 36, [online:] https://www.academia.edu/32573448/The_Path_of_the_Blockchain_Lexicon_and_the_Law [dostęp: 12.11.2021].
- Węgierski M., *Charakterystyka prawna umów zawieranych drogą elektroniczną*, Warszawa 2020.

