01

20 listopada 2019

KONCEPCJA ROZSZERZENIA ZNACZENIA PRAWNEGO PIECZĘCI ELEKTRONICZNEJ

Ministerstwo Cyfryzacji, Grupa robocza
ds. rejestrów rozproszonych i blockchain

Dokument przygotowany w ramach grupy roboczej ds. rejestrów rozproszonych i blockchain wyraża poglądy ekspertów, biorących udział w pracach podzespołu eID, RODO, AML,, tym samym nie jest to oficjalne stanowisko Ministra Cyfryzacji.

Wersja 1.01

WPROWADZENIE

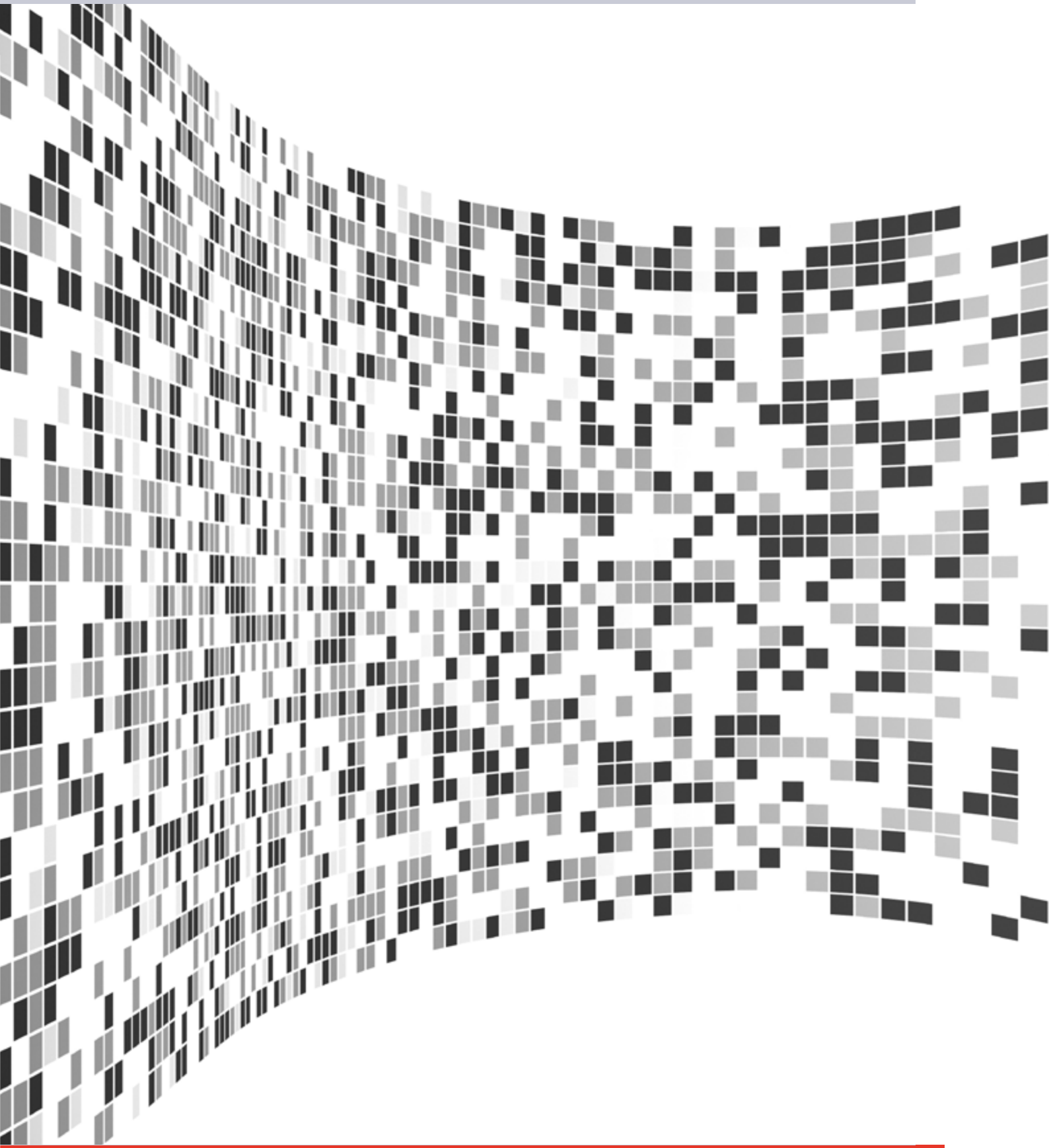
Celem dokumentu jest przedstawienie wstępnej koncepcji rozszerzenia prawnego znaczenia pieczęci elektronicznej w prawie polskim. Aktualne ramy prawne dotyczące pieczęci elektronicznej obejmują jedynie część kwestii pojawiających się wraz z dynamicznym rozwojem cyfrowego obrotu gospodarczego z udziałem podmiotów zbiorowych.

Rozwiązanie, które omawiamy w niniejszym dokumencie, przewiduje przyjęcie określonych prawnych domniemań związanych z posługiwaniem się pieczęcią elektroniczną, na wzór domniemań funkcjonujących w odniesieniu do obrotu gospodarczego odbywającego się w systemie analogowym. Domniemania te mogłyby w istotny sposób przyczynić się do zwiększenia efektywności i zabezpieczenia cyfrowego obrotu gospodarczego.

Rozszerzenie prawnego znaczenia rozpoznawanej już przez system prawa instytucji pieczęci elektronicznej wydaje się tu rozwiązaniem najbardziej skutecznym, bazuje bowiem na instrumencie osadzonym już w systemie prawa i opracowanym pod względem technologicznym. Ma ono także szereg dodatkowych zalet istotnych dla obrotu gospodarczego.
Koncepcja przedstawiona w niniejszym dokumencie ma charakter wstępnej propozycji służącej, po pierwsze, zasygnalizowaniu realnych wyzwań gospodarczych oraz, po drugie, wskazaniu możliwości ich rozwiązania. Ostateczny wybór konkretnych metod działania będzie niewątpliwie wymagał dalszych, pogłębionych dyskusji i analiz.

Nieprzypadkowo koncepcje dyskutowane w tym dokumencie pojawiły się przy okazji prac grupy roboczej ds. rejestrów rozproszonych i blockchain w podzespole, zajmującym się zagadnieniami elektronicznej identyfikacji. Blockchain połączył kilka technologii, wykorzystując najlepszą wiedzę o kryptografii, planowaniu rozproszonych systemów przetwarzania danych oraz dostępność szybkich sieci transmisji danych. Technologia blockchain daje narzędzia, mogące porządkować i automatyzować systemy, w których potrzebne jest zaufanie, co jest wyzwaniem szczególnie niebanalnym w relacjach, których stroną są przedsiębiorcy i instytucje. W pewnym uproszczeniu możemy przyjąć, że technologia blockchain zapewnia tę potrzebę zaufania, co jest bardzo inspirujące. Otwiera pola dla nowych sposób działania.

W praktyce funkcjonowania procesów gospodarczych lub administracyjnych ustalenie prawnej ważności indywidulanych pełnomocnictw, nawet jeżeli są w erze cyfrowej gwarantowane nieźle już zadomowioną techniką podpisu elektronicznego, bywa uciążliwe, zarówno pod kątem prawnym, jak i technicznym. Jest też inną częścią procesu, niż samo ustalenie ważności postanowienia umowy pomiędzy stronami. Wykorzystanie technologii blockchain dla pieczęci elektronicznej, wyrażającej oświadczenie woli podmiotu, pozwala w sposób zautomatyzowany utrwalić i weryfikować wszelkie procedury, które zwykle utwierdza moment przybicia zwykłej pieczęci. Dzięki automatyzacji procesów i pewności zaufania otwierają się nowe możliwości dla relacji gospodarczych.

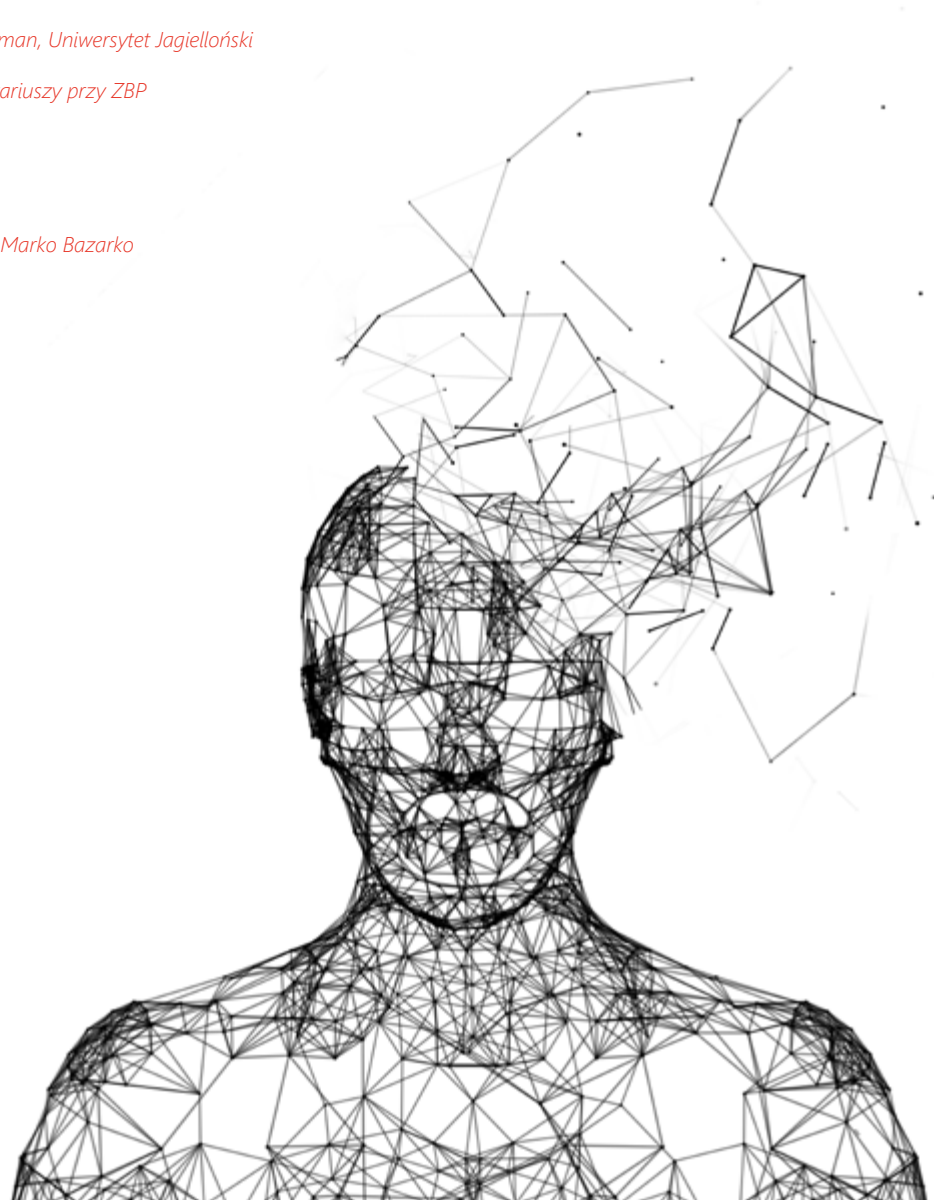


Niniejsze opracowanie jest jednym z efektów prac grupy roboczej ds. rejestrów rozproszonych i blockchain, działającej w ramach strumienia Rejestry Rozproszone utworzonego decyzją nr 7 Przewodniczącego Komitetu Rady Ministrów ds. Cyfryzacji z dnia 10 października 2018 roku, zmieniającą decyzję w sprawie utworzenia Zespołu zadaniowego „od papierowej do cyfrowej Polski". Podczas prac wykorzystano warsztaty przeprowadzone w ramach Koalicji na rzecz Polskich Innowacji.

Opracowanie przygotował i zredagował zespół autorski:

Krzysztof Wojdyło, Wardyński i Wspólnicy
Iwona Karasek-Wojciechowicz, , kancelaria Karasek&Wejman, Uniwersytet Jagielloński
Jacek Czarnecki, KPI
Janusz Łaski, ING Bank Śląski SA, Rada Banków Depozytariuszy przy ZBP
Dorota Mackiewicz , KDPW
Rafał Wawrzyniak, KDPW
Krzysztof Urbański, 7Bulls.com
Piotr Rutkowski, Ministerstwo Cyfryzacji, NASK PIB

Graficzny opracowanie WK/BM, Ministerstwo Cyfryzacji, Marko Bazarko



SPIS TREŚCI

STRESZCZENIE

- Dyskutowane w niniejszym opracowaniu rozwiązanie ma na celu podjęcie dwóch wyzwań wiążących się z postępującym rozwojem cyfrowego obrotu gospodarczego:
  - Braku systemu prawnych domniemań związanych z umocowaniem podmiotów uczestniczących w cyfrowym obrocie;
  - Braku dostatecznych regulacji odnoszących się do zautomatyzowanych czynności prawnych;
- Brak skutecznej odpowiedzi na powyższe wyzwania grozi wzrostem niepewności uczestników cyfrowej wymiany gospodarczej oraz niedostatecznej efektywności cyfrowych procesów gospodarczych;
- Przedstawione rozwiązanie zakłada rozszerzenie prawnego znaczenia pieczęci elektronicznej uregulowanej na gruncie Rozporządzenia eIDAS;
- Aktualnie pieczęć elektroniczna może służyć jedynie jako narzędzie do potwierdzania pochodzenia oraz integralności cyfrowych treści. Przedstawione rozwiązanie zakłada, że system prawa będzie kojarzył z użyciem kwalifikowanej pieczęci elektronicznej domniemanie prawne zakładające, że treść cyfrowego komunikatu sygnowanego taką pieczęcią jest objęta oświadczeniem woli podmiotu wskazanego w certyfikacie pieczęci;
- Rozwiązanie zakłada uniwersalne zastosowanie domniemania. Mogłoby ono działać zarówno w relacjach B2B, B2C oraz w relacjach z organami administracji. Ze względów pragmatycznych oraz ostrożnościowych do rozważenia jest stopniowe wprowadzanie domniemania do systemu prawa. W pierwszym etapie można przetestować działanie domniemania w ograniczonym zakresie, ograniczając jego zastosowanie np. do określonego sektora gospodarki;
- Domniemanie byłoby skuteczne jedynie w ramach prawa polskiego, jest to bowiem domniemanie, które nie wynika z Rozporządzenia eIDAS. Jednocześnie wychodzimy z założenia, że Rozporządzenie eIDAS nie zawiera przepisów, które zabraniałyby nadawania przez systemy prawne poszczególnych państw członkowskich dodatkowych skutków prawnych użycia pieczęci elektronicznej.

JAKI PROBLEM CHCEMY ROZWIĄZAĆ?

W obrocie gospodarczym obserwujemy narastające tendencje do cyfryzacji oraz automatyzacji procesów wymiany gospodarczej. Strony wykorzystują do zawierania oraz do wykonywania czynności prawnych w coraz większym stopniu systemy cyfrowe. Są to również systemy, które coraz częściej cechuje także pewna autonomia działania.

Nasilanie się tych tendencji to naturalna konsekwencja rozwoju Internetu Rzeczy oraz gospodarki opartej na danych, w ramach której wiele modeli biznesowych przewiduje transfery danych za pomocą np. zautomatyzowanych transakcji opartych na modelu Machine to Machine (M2M).

W celu lepszego zilustrowania istoty zjawiska polegającego na postępującej cyfryzacji oraz automatyzacji obrotu gospodarczego na końcu opracowania zamieszczamy opisy przypadków, w których może dochodzić do cyfrowego i zautomatyzowanego obrotu gospodarczego.

Wobec omawianych zjawisk kluczowe staje się wytworzenie odpowiednich narzędzi oraz ram prawnych dla bezpiecznego i efektywnego zawierania oraz wykonywania cyfrowych, zautomatyzowanych czynności prawnych. Istnienie takich narzędzi jest warunkiem aktywnego uczestnictwa polskiej gospodarki w najnowszych procesach rozwojowych .

Istniejące dzisiaj rozwiązania prawne nie pozwalają na pełne osiągnięcie wskazanych powyżej celów. Widoczny staje się rozdźwięk między dostępnymi konstrukcjami prawnymi a praktyką obrotu gospodarczego. Rozdźwięk ten skutkuje brakiem efektywności wielu procesów oraz rosnącą niepewnością uczestników obrotu.

W trakcie warsztatów towarzyszących przygotowywaniu niniejszego opracowania zidentyfikowaliśmy dwie podstawowe kategorie wyzwań, jakie towarzyszą aktualnemu obrotowi cyfrowemu:

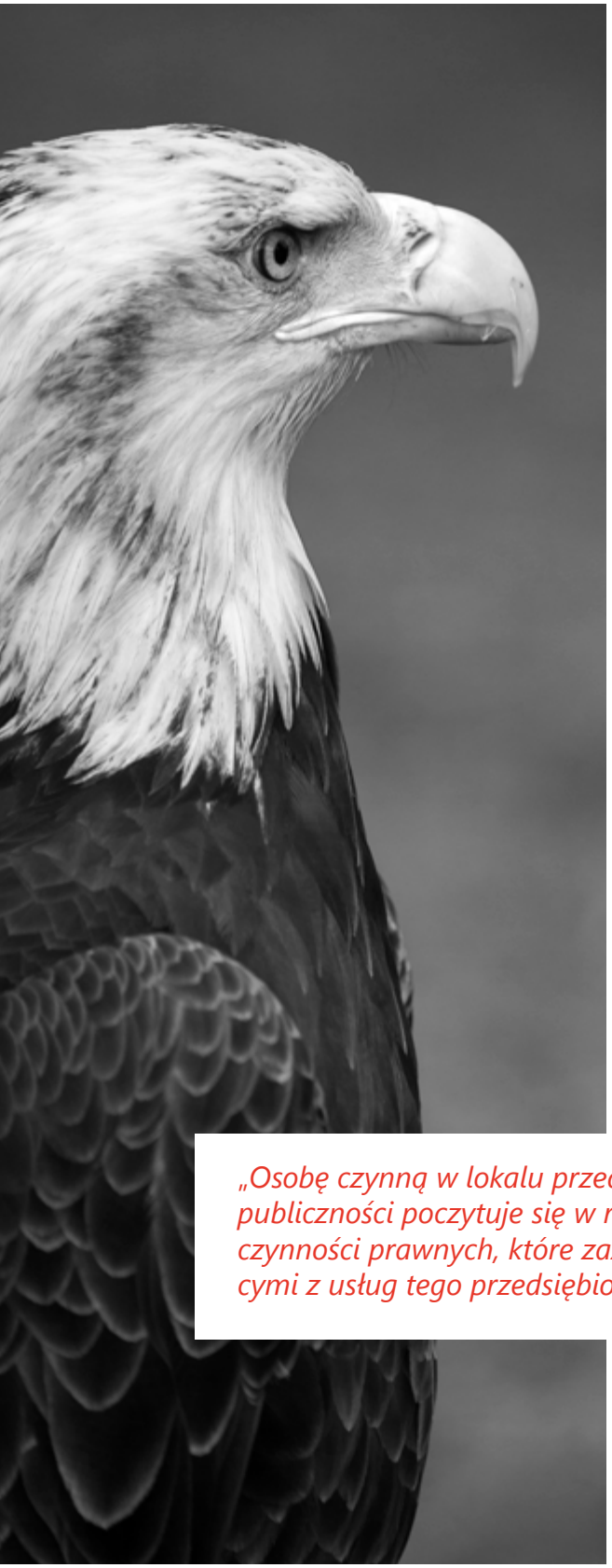
Wyzwanie 1 – Brak systemowych domniemań dotyczących cyfrowych oświadczeń woli

Istniejący obecnie system prawa umożliwia dokonywanie cyfrowych czynności prawnych, w tym składanie cyfrowych oświadczeń woli. Narzędzia służące do ich składania są jednak przypisane określonym osobom fizycznym. Jednocześnie system nie tworzy żadnych domniemań dotyczących cyfrowych oświadczeń woli, analogicznych do domniemań w odniesieniu do obrotu realizowanego w systemie analogowym (np. art. 97 Kodeksu cywilnego, domniemanie dotyczące osoby czynnej w lokalu przedsiębiorstwa). W efekcie, w przypadku składania elektronicznych oświadczeń woli przez przedstawicieli osób prawnych, pomimo cyfrowej formy oświadczeń (zakładającej zwiększenie efektywności procesów) zachodzi nadal konieczność czasochłonnej weryfikacji łańcucha uprawnień osób składających cyfrowe oświadczenie woli w imieniu osoby prawnej. Powoduje to istotne ograniczenia w rozwoju cyfrowego obrotu. Skutkuje również swoistą dyskryminacją tego obrotu. Nie może on bowiem korzystać z domniemań, które istnieją w odniesieniu do obrotu analogowego. Paradoksalnie zatem analogowy obrót gospodarczy może okazać się bardziej efektywny od obrotu cyfrowego.

Wyzwanie 2 – Niepewność prawna związana z automatyzacją obrotu

Cyfrowy obrót gospodarczy odbywa się w coraz większym stopniu bez udziału czynnika ludzkiego. W taki sposób dochodzi do zawierania umów oraz transferu aktywów, często o bardzo istotnych wartościach. Czynności te są również coraz częściej dokonywane z wykorzystaniem narzędzi, które w sposób autonomiczny determinują parametry zawieranych transakcji. Istniejące w obecnym systemie prawa zasady składania oświadczeń woli przestają odpowiadać realiom tak realizowanego obrotu. W konsekwencji, w odniesieniu do coraz większej ilości cyfrowych transakcji powstają wątpliwości co do ich ważności.

KOMENTARZ DO WYZWANIA **1.**



Istotą Wyzwania 1. jest brak systemowych domniemań towarzyszących działaniom podmiotów zbiorowych w przestrzeni cyfrowej. Adresaci elektronicznej komunikacji kierowanej przez podmioty zbiorowe mogą co najwyżej, dzięki wykorzystywaniu podpisów elektronicznych i pieczęci elektronicznej, mieć gwarancję, że pochodzi ona od danego podmiotu. Chcąc jednak mieć pewność, że komunikat jest faktycznie oświadczeniem woli konkretnej osoby odpowiednio umocowanej do działania w imieniu danego podmiotu zbiorowego, należy dokonać tradycyjnego odtworzenia łańcucha umocowań.

W przypadku dużych organizacji odtworzenie pełnego łańcucha umocowań może wymagać wielu czasochłonnych czynności. Skutkuje to brakiem efektywności wielu procesów gospodarczych. W praktyce dochodzi również do powstawania szeregu nieznajdujących podstawy w przepisach prawa fikcji polegających np. na sztucznym przypisywaniu elektronicznych oświadczeń działaniu określonego reprezentanta osoby prawnej, podczas gdy strony czynności prawnej doskonale zdają sobie sprawę z tego, że dany reprezentant nie obejmuje swoją świadomością dokonywanych czynności.

Nieco inaczej wygląda dokonywanie czynności prawnych w obrocie analogowym. Systemowi prawa cywilnego od dawna znane jest domniemanie działania w imieniu osoby prawnej osoby czynnej w lokalu przedsiębiorstwa (art. 97 Kodeksu cywilnego):

„Osobę czynną w lokalu przedsiębiorstwa przeznaczonym do obsługiwania publiczności poczytuje się w razie wątpliwości za umocowaną do dokonywania czynności prawnych, które zazwyczaj bywają dokonywane z osobami korzystającymi z usług tego przedsiębiorstwa."

Domniemanie to zostało wprowadzone do systemu prawa w celu zwiększenia efektywności oraz pewności obrotu gospodarczego. Umożliwia kontrahentom przedsiębiorcy bezpieczne dokonywanie czynności prawnych z przedsiębiorcą, bez konieczności

przeprowadzania czasochłonnej weryfikacji umocowania jego reprezentantów. Domniemanie to zwiększa oczywiście ryzyko po stronie przedsiębiorcy, może bowiem skutkować związaniem przedsiębiorcy z działaniami osób, które nie były przez niego odpowiednio umocowane. Z uwagi na racje społeczno-gospodarcze ustawodawca zdecydował się jednak obciążyć przedsiębiorców takim ryzykiem, w imię zwiększenia efektywności i pewności po stronie kontrahentów przedsiębiorcy.

Omawiane domniemanie wymusza na przedsiębiorcach dbałość o odpowiednie zorganizowanie wewnętrznych procesów zarządczych i systemu kontroli. Jednocześnie ustawodawca wprowadził systemowe zabezpieczenia w treści art. 97, które w odpowiedni sposób ograniczają zakres ryzyka po stronie przedsiębiorców (przede wszystkim domniemanie ograniczono do czynności prawnych, które zazwyczaj bywają dokonywane z osobami korzystającymi z usług tego przedsiębiorstwa).

Teoretycznie można się zastanawiać nad tym, czy omawianego wyzwania nie podejmuje już dzisiaj w dostateczny sposób przywołany art. 97 Kodeksu cywilnego. Naszym zdaniem jest on jednak niewystarczający. Przede wszystkim posługuje się on pojęciem „lokalu przedsiębiorstwa". Nie jest ono wprawdzie zdefiniowane, ale zgodnie z dominującym do tej pory poglądem uważano, że odnosi się ono do materialnej przestrzeni dostępnej dla publiczności, w której prowadzona jest działalność przedsiębiorcy.

Nie sposób jednoznacznie rozstrzygnąć, w jakim zakresie pojęcie to może odnosić się do działalności przedsiębiorcy prowadzonej w przestrzeni cyfrowej. W ostatnim czasie pojawiają się koncepcje postulujące przynajmniej częściowe stosowanie domniemania z art. 97 do elektronicznych czynności prawnych. Przykładowo, w wyroku Sądu Apelacyjnego w Szczecinie z dnia 22 marca 2017 r., sygn. I ACa 964/16 pojawia się stwierdzenie:

„Nie ma żadnych podstaw, by wyłączyć możliwość zawierania umów na odległość przy pomocy faksu, jak również, by wyłączyć w takiej sytuacji stosowanie art. 97 k.c. Użyte w art. 97 k.c. pojęcie <<lokal przedsiębiorstwa przeznaczony do obsługiwania publiczności>> musi być rozumiane szeroko, jako każde miejsce w przedsiębiorstwie, w którym znajdują się osoby i urządzenia służące do kontaktów z klientami i zawierania umów także na odległość".

Próby rozumienia pojęcia „lokalu przedsiębiorstwa przeznaczonego do obsługi przedsiębiorstwa" jako odnoszącego się również do przestrzeni cyfrowej traktujemy raczej jako wymuszone przez brak odpowiednich regulacji próby dostosowania istniejących przepisów do realiów systemu cyfrowego, niż jako odpowiadające intencjom i treści art. 97 Kodeksu cywilnego. Budowanie ewentualnego domniemania dla cyfrowych oświadczeń woli w oparciu o art. 97 Kodeksu cywilnego wydaje się nam rozwiązaniem ułomnym i wręcz niebezpiecznym. Przepis ten nie jest dostosowany do tego obrotu. W ekstremalnej sytuacji próby jego stosowania do elektronicznych oświadczeń woli mogą doprowadzić do uznania, że do zaistnienia tego domniemania wystarczy np. wysłanie wiadomości mailowej z adresu zawierającego domenę przedsiębiorcy. Mając świadomość tego, jak łatwe jest posłużenie się cudzym adresem mailowym, przyjęcie takiego rozwiązania w praktyce w istotny i trudny do zaakceptowania sposób zwiększałoby ryzyko po stronie przedsiębiorców.

Z uwagi na zasadnicze trudności w stosowaniu domniemania z art. 97 Kodeksu cywilnego do obrotu cyfrowego doszło do powstania paradoksalnej sytuacji, w której obrót cyfrowy, który miał z założenia przyczynić się do zwiększenia efektywności procesów gospodarczych, okazuje się pod pewnymi względami mniej efektywny od obrotu analogowego. Kontrahenci przedsiębiorcy w pewnych obszarach obrotu analogowego mogą bowiem bezpiecznie dokonywać czynności prawnych z przedsiębiorcą bez konieczności przeprowadzania żmudnej weryfikacji umocowania przedstawiciela przedsiębiorcy do dokonania danej czynności prawnej. W świecie cyfrowym brakuje takiej możliwości.

Mając to na uwadze należy – naszym zdaniem – rozważyć wprowadzenie do systemu prawa nowego domniemania, które wprost odniesie się do działania przedsiębiorców w przestrzeni cyfrowej. Umożliwi ono odpowiednie zdefiniowanie warunków, które muszą się spełnić, aby takie domniemanie było skuteczne. Dzięki temu ograniczone zostanie również ryzyko, które może powstać w związku z pojawiającymi się próbami stosowania art. 97 Kodeksu cywilnego do obrotu cyfrowego.

KOMENTARZ DO WYZWANIA **2.**

Rodzaje zautomatyzowanych czynności prawnych

Dla prawidłowego zrozumienia specyfiki zautomatyzowanego obrotu kluczowe jest zdefiniowanie podstawowych rodzajów zautomatyzowanych czynności prawnych. Cechuje je bowiem duża różnorodność. Wskazany poniżej podział ma charakter abstrakcyjny. W praktyce systemy zautomatyzowane są wielokrotnie hybrydą poniższych kategorii.

1. **Czynności techniczne**
2. **Algorytmiczne oświadczenia woli**
   a. Rozwiązania w całości zdeterminowane;
   b. Rozwiązania częściowo zdeterminowane (tzw. *gap-filling*);
   c. Rozwiązania adaptacyjne.

Ad. 1 Czynności techniczne

Aktualnie praktyka obrotu cyfrowego zakłada często, że strony zawierają umowę w tradycyjny sposób. Umowa określa ramowe zasady współpracy między stronami, przewidując jednocześnie zestaw czynności technicznych, które składają się na faktyczne wykonanie umowy oraz są realizowane w sposób cyfrowy i zautomatyzowany (np. przez komunikację z API jednej ze stron umowy). Takie podejście zakłada, że elektroniczna komunikacja i wymiana danych między stronami są realizacją czynności technicznych, a nie składaniem oświadczeń woli. W odniesieniu do tego rodzaju sytuacji pieczęć elektroniczna w rozumieniu Rozporządzenia eIDAS-a jest wystarczająca i może okazać się bardzo pomocnym narzędziem. Służy ona przede wszystkim prawidłowej identyfikacji stron dokonujących technicznych czynności. Nie musi realizować innych funkcji, w szczególności być „nośnikiem" oświadczenia woli. To ostatnie bowiem, jak się przyjmuje, zostało złożone podczas tradycyjnego zawierania pierwotnej umowy ramowej. Czynności wykonywane automatycznie są jedynie wykonaniem uprzednio zawartej umowy.

Ad. 2a Algorytmiczne oświadczenia woli. Rozwiązania w całości zdeterminowane

Wraz z rozwojem narzędzi cyfrowego obrotu pojawia się coraz więcej modeli gospodarczych, w których zautomatyzowana wymiana danych nie jest wyłącznie czynnością techniczną, a zaczyna odgrywać funkcję oświadczeń woli. Czynności realizowanych przez zautomatyzowane narzędzie nie poprzedza żadne tradycyjnie złożone oświadczenie woli. Stosunek prawny jest zawiązywany przez zautomatyzowane działanie przynajmniej jednej strony stosunku prawnego. To zautomatyzowany system określa („godzi się") na parame-

try kontraktu. W przypadku rozwiązań w całości zdeterminowanych zautomatyzowane narzędzia nie mają żadnej autonomii w determinowaniu treści stosunku prawnego. Jest on w pełni zdeterminowany przez twórców narzędzia (algorytmu). Z góry wiadomo zatem, jaka będzie treść stosunku prawnego zawartego w taki sposób.

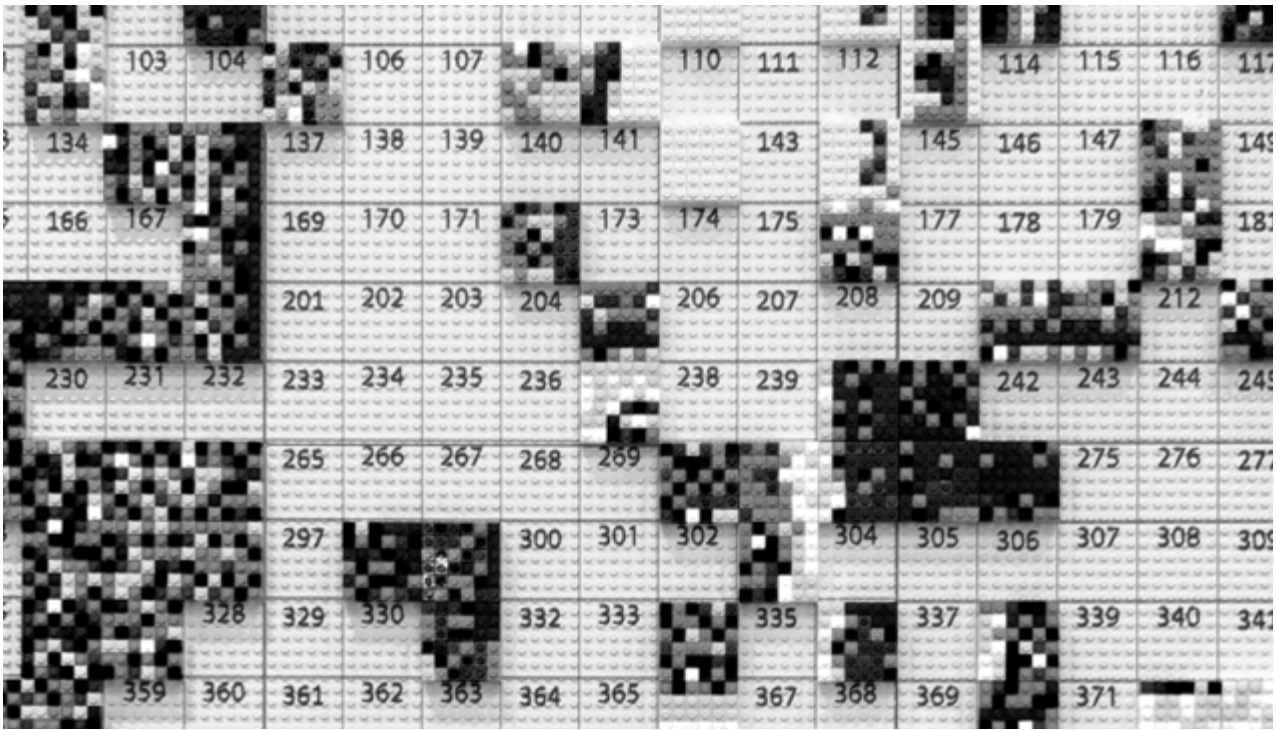
Ad. 2b Algorytmiczne oświadczenia woli. Rozwiązania częściowo zdeterminowane

W rozwiązaniach częściowo zdeterminowanych twórcy narzędzia określają brzegowe parametry stosunku prawnego, ale w pewnych zakresach (np. cena za usługę) pozostawiają przestrzeń decyzyjną dla zautomatyzowanego narzędzia. Ostateczny kształt i treść stosunku prawnego nie jest więc znana, znane są natomiast jego brzegowe parametry (np. wiadomo, że cena nie przekroczy z góry określonych wartości).

Ad. 2c Algorytmiczne oświadczenia woli. Rozwiązania adaptacyjne

W przypadku rozwiązań adaptacyjnych dopuszczalne jest, by wszystkie bądź niektóre elementy stosunku prawnego nie miały określonych parametrów brzegowych i mogły być określane w sposób autonomiczny przez narzędzie (algorytm). Dopuszczamy również możliwość ewolucji narzędzia, które będzie modyfikowało zasady jego działania, doprowadzając do ostatecznego oderwania narzędzia i zasad jego działania od świadomości jego twórców.

Opisane rodzaje zautomatyzowanych czynności prawnych nie wyczerpują całego możliwego spektrum takich czynności. Pokazują jednak ich możliwą gradację z uwzględnieniem stopnia powiązania rezultatów działania wykorzystywanych do ich składania narzędzi ze świadomością podmiotów, w imieniu których działają. W przypadku rozwiązań w całości zdeterminowanych można przyjąć, że podmioty te zyskują świadomość skutków działania narzędzi przez sam fakt skorzystania z takich narzędzi. Świadoma decyzja o wykorzystaniu narzędzia jest w tym przypadku tożsama ze świadomością treści stosunków prawnych, warunkowanych przez takie narzędzie. Ta prosta zależność zostaje zaburzona w przypadku rozwiązań częściowo zdeterminowanych. Wówczas można przyjąć jednak, ze przedmiotem uświadomienia były przynajmniej parametry brzegowe czynności prawnej. Jeśli chodzi o rozwiązania adaptacyjne, w ekstremalnych sytuacjach może dojść do całkowitego zerwania związku świadomości z wytworami narzędzia. Przedmiotem świadomości mógłby być w takim przypadku co najwyżej sam fakt skorzystania z narzędzia.



ZASADY SKŁADANIA OŚWIADCZEŃ WOLI JAKO GŁÓWNE WYZWANIE PRAWNE

Kluczowym zagadnieniem prawnym w odniesieniu do omawianych wyzwań są zasady składania oświadczeń woli. Fundamenty tych zasad były tworzone w rzeczywistości analogowej, która zakładała pełną kontrolę czynnika ludzkiego nad treścią dokonywanej czynności prawnej. Wraz z rozwojem cywilizacji oraz postępującą komplikacją obrotu gospodarczego stało się jasne, że już nawet w systemie analogowym takie założenie jest w dużym stopniu fikcyjne.

Widać to bardzo wyraźnie w aspekcie czynności prawnych zawieranych przez osoby prawne. W teorii osoby prawne, zgodnie z regulacjami prawa cywilnego, działają przez swoje organy. W praktyce jednak, szczególnie w odniesieniu do dużych korporacji, organy osoby prawnej nie obejmują swoją świadomością znacznej części czynności prawnych realizowanych przez te podmioty. Jest to naturalna konsekwencja skali prowadzonej działalności. Osoby prawne działają więc przez wielu swoich przedstawicieli, stanowiących swoiste przedłużenie organów danej osoby prawnej.

Obowiązujący system prawa rozpoznaje te realia, tworząc odpowiednie ramy prawne dla działania reprezentantów osób prawnych. Ramy te przewidują m.in. określone zasady działania pełnomocników oraz domniemania, np. dotyczące osób czynnych w lokalu przedsiębiorstwa.

Wraz z rozwojem obrotu cyfrowego pojawiły się jednak nowe zjawiska, do których obowiązujące ramy prawne odnoszą się w bardzo ograniczonym zakresie. Poza potwierdzeniem tego, że oświadczenia woli mogą być składane w postaci cyfrowej, system prawa nie podejmuje kluczowych wyzwań tego obrotu. W kontekście zasad składania oświadczeń woli wyzwania te polegają m.in. na:

- Rozluźnieniu, a w ekstremalnych przypadkach również zerwaniu związku między świadomością uprawnionego reprezentanta podmiotu a rezultatami działania narzędzia wykorzystywanego do komunikacji w imieniu tego podmiotu;
- Braku systemowych domniemań dotyczących przypisywania rezultatów działań zautomatyzowanych narzędzi do podmiotów prawa.

Bez rozwiązania wskazanych wyzwań ryzykujemy rozwojem swoistej prawnej próżni, w której wyniki działań zautomatyzowanych systemów nie będą mogły być w jednoznaczny sposób przypisane do określonych podmiotów stosunków prawnych. Czynności prawne realizowane w taki sposób będą naznaczone potencjalnymi wadami.

Fakt, że obrót cyfrowy z udziałem osób prawnych odbywa się już dzisiaj, nawet bez istnienia systemowych rozwiązań, nie oznacza bynajmniej, że jest on prawnie bezpieczny. Towarzyszy mu wiele fikcji i założeń (np. to, że zautomatyzowanym oświadczeniom generowanym przez systemy IT rzeczywiście towarzyszy „wola" uprawnionych reprezentantów), które są stosunkowo łatwe do obalenia w przypadku ewentualnego sporu. Widać to wyraźnie na przykładzie sporów dotyczących błędnego działania systemów IT generujących automatyczne komunikaty. Okazuje się, że ustalenie, czy w przypadku działania takich systemów dochodziło do składania wiążących oświadczeń woli, nie jest łatwe i oczywiste. Dalszy rozwój obrotu cyfrowego nie może bazować na fikcyjnych założeniach dotyczących udziału czynnika ludzkiego w zautomatyzowanym obrocie gospodarczym. Niezbędne są solidne podstawy prawne rozstrzygające zasady składania oświadczeń w ramach takiego obrotu.

AKTUALNE UREGULOWANIE PIECZĘCI ELEKTRONICZNEJ

Definicje

Pieczęć elektroniczną definiują aktualnie Artykuł 3 pkt 25-27 rozporządzenia PE i Rady (UE) nr 910/2014 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 (**„Rozporządzenie eIDAS”**).

Rozporządzenie eIDAS wprowadza 3 rodzaje pieczęci elektronicznej: pieczęć elektroniczną, zaawansowaną pieczęć elektroniczną oraz kwalifikowaną pieczęć elektroniczną.

„Pieczęć elektroniczna” oznacza dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych. Pieczęć elektroniczna nie musi spełniać wymogu umożliwienia ustalenia na jej podstawie tożsamości podmiotu składającego pieczęć.

„Zaawansowana pieczęć elektroniczna” oznacza pieczęć elektroniczną, która, zgodnie z Artykułem 36 Rozporządzenia eIDAS, spełnia następujące wymogi:

a) jest unikatowo przyporządkowana podmiotowi składającemu pieczęć;

b) umożliwia ustalenie tożsamości podmiotu składającego pieczęć;

c) jest składana przy użyciu danych służących do składania pieczęci elektronicznej, których podmiot składający pieczęć może, mając je z dużą dozą pewności pod swoją kontrolą, użyć do złożenia pieczęci elektronicznej; oraz

d) jest powiązana z danymi, do których się odnosi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

I wreszcie „kwalifikowana pieczęć elektroniczna” oznacza zaawansowaną pieczęć elektroniczną, która została złożona za pomocą kwalifikowanego urządzenia do składania pieczęci elektronicznej i która opiera się na kwalifikowanym certyfikacie pieczęci elektronicznej.

Skutki prawne pieczęci elektronicznej

Skutki prawne wykorzystania pieczęci elektronicznej określa Artykuł 35 Rozporządzenia eIDAS.

Zgodnie z Rozporządzeniem eIDAS, zwykłej pieczęci 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. Oznacza to, że sąd nie może odmówić dopuszczalności, jako dowodu w postepowaniu, dokumentu opatrzonego pieczęcią elektroniczną. Zwykła pieczęć nie korzysta jednak z domniemania integralności danych i autentyczności pochodzenia danych powiązanych z tą pieczęcią. Z tego domniemania korzysta dopiero kwalifikowana pieczęć elektroniczna.

Domniemanie to jest co prawda możliwe do obalenia, ale dowód przeciwny musi podnieść osoba, która chce uzyskać z tego korzyść. Także kwalifikowana pieczęć elektroniczna oparta na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawana za kwalifikowaną pieczęć elektroniczną we wszystkich pozostałych państwach członkowskich.

Ustawodawca unijny nie określił dalej idących skutków prawnych wykorzystania pieczęci elektronicznej, jak i sposobów jej wykorzystywania (poza uwierzytelnianiem witryn internetowych). Nie przesądził zatem, czy użycie pieczęci elektronicznej spełnia wymogi elektronicznej formy dokonywania czynności prawnych przez podmiot składający pieczęć. Nie przyznał jej zatem, odmiennie niż w przypadku podpisu elektronicznego, znaczenia równoważnego ze złożeniem podpisu własnoręcznego.

Przepisy prawa krajowego również nie wiążą z pieczęcią elektroniczną skutków równoważnych z formą elektroniczną. Artykuł 781 Kodeksu cywilnego jednoznacznie wskazuje, ze do zachowania elektronicznej formy czynności prawnej wymagane jest złożenie oświadczenia w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym. Na poziomie ogólnych norm kodeksowych nie ma przepisów, które przyznawałyby pieczęci elektronicznej znaczenie inne niż forma dokumentowa, którą jest złożenie oświadczenia woli w postaci dokumentu będącego dowolnym nośnikiem informacji, w sposób umożliwiający ustalenie osoby składającej oświadczenie.

Reasumując, uznać należy, że w obecnym stanie prawnym pieczęć elektroniczna nie jest instrumentem, który może służyć do składania oświadczeń woli. W szczególności, nie ma możliwości uznania oświadczeń złożonych z wykorzystaniem pieczęci elektronicznej za formę elektroniczną. Podmiot posługujący się pieczęcią, mimo że zaawansowana pieczęć elektroniczna umożliwia ustalenie tożsamości tego podmiotu, nie może posłużyć się tą pieczęcią do złożenia oświadczenia woli, bez jednoczesnej identyfikacji osoby/osób posługujących się pieczęcią. Osiągnięcie skutku złożenia oświadczenia woli byłoby możliwe wyłącznie po wprowadzeniu odpowiednich zmian w przepisach prawa, które dawałyby możliwość składania oświadczeń woli przez osobę prawną z wykorzystaniem pieczęci elektronicznej, a więc bez ujawniania tożsamości osób reprezentujących tę osobę.

Obowiązujące podstawy prawne wykorzystania pieczęci elektronicznej

Wykorzystanie pieczęci elektronicznej do składania oświadczeń woli przewiduje od 2000 r. prawo czeskie. Pieczęć służy tam zarówno jako gwarancja autentyczności i integralności dokumentu podpisanego z jej użyciem, jak i do potwierdzenia oświadczeń woli osób prawnych i jest wykorzystywana przez organy skarbowe. W Irlandii pieczęć jest wykorzystywana przez notariuszy. W Hiszpanii wprowadzono pieczęć elektroniczną w 2015 r. jako narzędzie do wystawiania e-faktur.

Najszersze zastosowanie pieczęci elektronicznej przewidywał projekt ustawy belgijskiej dostosowujący prawo do wymogów Rozporządzenia eIDAS. Zgodnie z tym projektem kwalifikowana pieczęć elektroniczna może być wykorzystywana w stosunkach prawnych zawieranych między osobami fizycznymi i prawnymi z miejscem zamieszkania lub siedzibą w Belgii i ma skutek taki sam jak podpis własnoręczny osoby fizycznej reprezentującej osobę prawną. W ogólnodostępnych źródłach informacji brak jest jednak potwierdzenia, czy przepisy projektowa-

ne w Belgii weszły ostatecznie w życie. W Polsce pieczęć elektroniczną od 2005 r. stosują urzędy administracji publicznej. Podstawą do jej stosowania jest rozporządzenie o warunkach technicznych doręczania dokumentów podmiotom publicznym z wykorzystaniem elektronicznej skrzynki podawczej (ESP), wydane na podstawie art. 16 ust. 3 ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Zawarta w rozporządzeniu definicja urzędowego poświadczenia odbioru jako "danych dołączonych do dokumentu elektronicznego" (par. 2 ust. 4) to funkcjonalnie pieczęć elektroniczna, tyle że ograniczona do stosowania w ESP.

Zgodnie z rozporządzeniem, urzędowym poświadczeniem odbioru są dane elektroniczne dołączone do dokumentu elektronicznego doręczonego podmiotowi publicznemu lub połączone z tym dokumentem w taki sposób, że jakakolwiek późniejsza zmiana dokonana w tym dokumencie jest rozpoznawalna. Dane te określają:

- pełną nazwę podmiotu publicznego, któremu doręczono dokument elektroniczny,
- datę i czas doręczenia dokumentu elektronicznego rozumiane jako data i czas wprowadzenia albo przeniesienia dokumentu do systemu teleinformatycznego podmiotu publicznego,
- datę i czas wytworzenia urzędowego poświadczenia odbioru.

W praktyce pieczęć elektroniczną wprowadziły np. władze Wołomina. Obowiązująca od początku 2017 r. uchwała nr XXVIII-155/2016 Rady Miejskiej w sprawie wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi, składanej przez właścicieli nieruchomości (Dz.Urz. Woj. Mazowieckiego z 2016 r. poz. 9371) w par. 3 ust. 3 przewiduje, że dokumenty te, jeżeli są przesyłane w formie elektronicznej, mogą być opatrzone kwalifikowaną pieczęcią elektroniczną.

Ograniczenie stosowania pieczęci elektronicznej w prawie polskim

Powszechne stosowanie pieczęci elektronicznej w stosunkach prawnych między osobami prawnymi oraz między osobami prawnymi i fizycznymi, ze względu na ograniczone skutki prawne, jakie przypisuje pieczęci ustawa, jest ograniczone.

W obecnym stanie prawnym praktyczne zastosowanie pieczęci elektronicznej ogranicza się wyłącznie do sytuacji, w których odbiorca oczekuje integralności dokumentu i pewności, że dany dokument pochodzi od danej osoby prawnej, ale bez konieczności identyfikacji osoby fizycznej, która go udostępniła. Wszędzie tam, gdzie istnieje potrzeba potwierdzenia, kto podpisał dokument – pieczęć elektroniczna nie znajdzie zastosowania. Pieczęć elektroniczna nie znajdzie więc zastosowania przede wszystkim w stosunkach prawnych związanych z dokonywaniem czynności prawnych, w szczególności zaś przy zawieraniu umów. Ważność umowy zawartej z wykorzystaniem pieczęci i tak zależałaby od potwierdzenia jej zawarcia przez osoby uprawnione do reprezentowania osoby prawnej.

Pieczęć elektroniczna nie znajdzie także zastosowania w relacji organ – obywatel, gdzie przepisy szczególne określają wymogi podpisywania przez upoważnione osoby działające w imieniu organu decyzji, postanowień, zaświadczeń i innych dokumentów urzędowych.

ZARYS KONCEPCJI ROZSZERZENIA ZNACZENIA PRAWNEGO PIECZĘCI ELEKTRONICZNEJ

Idea

Wszędzie, gdzie mowa o automatyzacji, wymagane jest możliwie daleko idące uproszczenie procesów, w szczególności eliminacja czynności manualnych wykonywanych przez człowieka. Chodzi nie tylko o sam proces wymiany danych, ale także o procesy przygotowawcze, oparte na wszelkiego rodzaju weryfikacjach potwierdzających możliwość ustanowienia komunikacji automatycznej między określonymi i zidentyfikowanymi podmiotami przy utrzymaniu akceptowalnego poziomu ryzyka. Zaawansowany podpis elektroniczny, zrównany z podpisem odręcznym dla osób fizycznych, jest tożsamy technologicznie z zaawansowaną pieczęcią cyfrową. Samo wykorzystanie certyfikatów elektronicznych do złożenia podpisu pod określonym dokumentem jest rozwiązaniem dużo bardziej bezpiecznym od podpisu złożonego w sposób tradycyjny, bo poza potwierdzeniem tożsamości osoby składającej podpis daje gwarancję integralności podpisanego dokumentu. W praktyce oznacza to, że ten, kto otrzymuje dokument, ma pewność, że podpisała go konkretna osoba i został on przekazany w niezmienionej i niezmanipulowanej wersji. Jeśli dokument wytworzony będzie w formie ustrukturyzowanej i zostanie podpisany z wykorzystaniem zaawansowanego podpisu elektronicznego istnieje możliwość automatyzacji jego przetwarzania włącznie z potwierdzeniem poprawności podpisu osoby go składającej. To pozwala z kolei na zastosowanie podpisu także w zautomatyzowanej komunikacji w relacjach między systemami informatycznymi.

Aby możliwe było podniesienie poziomu automatyzacji procesów w relacjach między osobami prawnymi lub, w których uczestniczą osoby prawne, niezbędne jest posiadanie podobnego narzędzia, zarówno co do cech w obszarze bezpieczeństwa, jak i skutków prawnych. Proponujemy, aby takim narzędziem uczynić pieczęć elektroniczną przy założeniu, że dokument podpisany z jej użyciem będzie można uznawać za potwierdzony zgodnie z reprezentacją danego podmiotu. Brak nadania pieczęci odpowiednich skutków prawnych w praktyce uniemożliwia przeprowadzanie potwierdzenia autentyczności i posiadania właściwych upoważnień przez składającego dokument w komunikacji automatycznej. Biorąc pod uwagę wolumen przetwarzanych dokumentów, uniemożliwia to automatyzację i budowę wiarygodnej komunikacji z wykorzystaniem systemów informatycznych.

Obecnie do uzyskania pieczęci elektronicznej wymaga się złożenia następujących dokumentów:

- odpisu z KRS nie starszego niż 6 miesięcy od daty jego wydania lub w przypadku osób prowadzących indywidualną działalność gospodarczą wydruku z CEiDG,
- potwierdzenia nadania numeru NIP,
- zaświadczenia o numerze identyfikacyjnym REGON,
- pełnomocnictwa (jeżeli osoba występująca o certyfikat nie jest organem danego podmiotu – tzn. nie jest osobą upoważnioną do samodzielnego

reprezentowania danej instytucji). Jest to praktycznie pełen zestaw niezbędnych dokumentów, które w przypadku oświadczenia woli muszą być weryfikowane ręcznie, indywidulanie przez każdego z kontrahentów. Myśląc o możliwej w przyszłości uznawalności stosownej pieczęci w relacjach międzynarodowych, warto już teraz wziąć pod uwagę wykorzystanie w ramach danych referencyjnych pieczęci także kodu LEI, który jest globalnym identyfikatorem podmiotów prawnych.

Należy także podkreślić, że podpisy elektroniczne składane z wykorzystaniem stosownych certyfikatów elektronicznych znacznie trudniej sfałszować niż podpisy składane odręcznie, a weryfikacja autentyczności jest możliwa bez umiejętności grafologicznych wymaganych przy porównaniu podpisu np. z kartą wzorów podpisów. Tym samym skorzystanie z tej technologii, przy wykorzystaniu odpowiedniego poziomu funkcji skrótu (np. SHA-256) i zachowaniu elementarnych zasad bezpieczeństwa w zakresie ochrony dostępu do pieczęci elektronicznej, praktycznie uniemożliwia podrobienie lub sfałszowanie treści przekazywanych dokumentów.

Umożliwienie wykorzystywania pieczęci elektronicznej do zawierania czynności prawnej w formie elektronicznej, zoptymalizowałoby w znacznym stopniu procesy komunikacji, przede wszystkim jednak ograniczyłoby konieczność weryfikacji oraz zarządzania pełnomocnictwami osób reprezentujących kontrahenta. W obecnych realiach funkcjonowania rynku są to procesy kosztowne i często nieadekwatne do ryzyk. Niemniej, przy braku odpowiednich mechanizmów prawnych minimalizujących te ryzyka, a więc pozwalających działać w środowisku pełnego zaufania prawnego, pieczęć elektroniczna nie znajdzie zastosowania tak długo, jak długo nie nastąpią odpowiednie zmiany.

Prawna istota proponowanego rozwiązania

Proponujemy rozważenie stworzenia nowego prawnego domniemania dotyczącego działań podejmowanych w przestrzeni cyfrowej przez podmioty zbiorowe. Rozwiązanie to przewiduje skojarzenie domniemania prawnego z faktem wykorzystania pieczęci elektronicznej. W efekcie domniemania przedsiębiorca, z którym powiązana jest dana pieczęć elektroniczna, byłby związany treścią oświadczeń (w tym oświadczeniami woli) opatrzonych pieczęcią elektroniczną. Dzięki temu kontrahent przedsiębiorcy otrzymywałby gwarancję pochodzenia danego oświadczenia od określonego przedsiębiorcy oraz, czego nie daje mu aktualny system prawny, domniemanie tego, że takie oświadczenie jest złożone przez odpowiednio umocowanego reprezentanta. Zwalniałoby go to z konieczności przeprowadzania czasochłonnych i nieefektywnych weryfikacji łańcucha umocowań po stronie przedsiębiorcy.

Proponujemy oprzeć omawiane rozwiązanie na pieczęci elektronicznej w rozumieniu Rozporządzenia eIDAS, ponieważ jest to instrument dopracowany od strony technologicznej oraz usankcjonowany prawnie przez europejskie i polskie regulacje. Aktualne ramy prawne przewidują dla pieczęci elektronicznej określone znaczenie prawne, które nie pozwala jednak na jej wykorzystanie w omawianych w niniejszym opracowaniu celach. W związku z tym proponowane rozwiązanie zakłada interwencję ustawodawcy w celu rozszerzenia skutków prawnych użycia pieczęci elektronicznej. Cel ten można osiągnąć za pomocą skonstruowania odpowiedniego domniemania prawnego, podobnego do domniemania istniejącego w odniesieniu do analogo-

wego obrotu gospodarczego. Certyfikat powiązany z pieczęcią elektroniczną stawia drugą stronę czynności w sytuacji analogicznej do tej, w której znajduje się kontrahent osoby prawnej w lokalu przedsiębiorstwa. Kontrahent znajdujący się w odpowiednio urządzonym lokalu przedsiębiorcy może z dużym prawdopodobieństwem założyć, że osoby przebywające w tym lokalu są umocowane do działania w imieniu przedsiębiorcy. Analogicznie, strona odbierająca oświadczenie opatrzone pieczęcią elektroniczną z dużym prawdopodobieństwem może założyć, że oświadczenie złożył umocowany przedstawiciel podmiotu wskazanego w certyfikacie pieczęci. Użycie pieczęci wymaga bowiem dostępu do odpowiednich danych uwierzytelniających, które w momencie tworzenia pieczęci zostały przekazane umocowanemu reprezentantowi osoby prawnej, na rzecz której wydano pieczęć elektroniczną.

Czynności cyfrowe są zazwyczaj dokonywane na odległość i nie wymagają kontaktu kontrahenta przedsiębiorcy z konkretną osobą fizyczną reprezentującą tego przedsiębiorcę. W praktyce czynności realizowane elektronicznie bardzo często w ogóle nie zakładają nawet identyfikacji reprezentanta przedsiębiorcy. Proponowane rozwiązanie powinno uwzględniać tę specyfikę obrotu cyfrowego. Z tego względu warunkiem skuteczności domniemania nie powinna być identyfikacja konkretnego reprezentanta po stronie przedsiębiorcy. Warunkiem zaistnienia domniemania powinien być sam fakt wykorzystania pieczęci elektronicznej do złożenia określonego oświadczenia. Domniemanie tworzy bowiem założenie, że odpowiednio umocowani reprezentanci przedsiębiorcy, którzy otrzymali pierwotnie dostęp do danych uwierzytelniających niezbędnych do skorzystania z pieczęci, w taki sposób zorganizowali swoją działalność, iż dane uwierzytelniające są wykorzystywane wyłącznie w sposób przez nich uświadomiony i kontrolowany.

Rozwiązanie powinno umożliwić zaadresowanie obydwu Wyzwań analizowanych w niniejszym dokumencie. W odniesieniu do Wyzwania 1 dyskutowane domniemanie będzie skutkowało zwolnieniem kontrahentów przedsiębiorcy z czasochłonnego i nieefektywnego procesu weryfikacji łańcucha umocowań po stronie przedsiębiorcy. Tym samym, ma szansę przyczynić się do zwiększenia efektywności cyfrowego obrotu gospodarczego.

W odniesieniu do Wyzwania 2 domniemanie stwarza szansę na uporządkowanie statusu prawnego czynności realizowanych z faktycznym wyłączeniem lub ograniczeniem zaangażowania czynnika ludzkiego. Czynności te są realizowane już dzisiaj, pomimo że wielokrotnie funkcjonują w prawnej próżni. Proponowane rozwiązanie pozwoliłoby ograniczyć negatywne konsekwencje związane z brakiem jasnych zasad dotyczących zautomatyzowanych oświadczeń przez przesądzenie, że oświadczenia cechujące się określonymi właściwościami (tj. złożone z wykorzystaniem pieczęci elektronicznej) korzystałyby z domniemania i były wiążące dla podmiotu, do którego przypisana jest pieczęć elektroniczna. Rozwiązanie takie z jednej strony zwiększałoby bezpieczeństwo prawne kontrahentów przedsiębiorców wykorzystujących do składania oświadczeń zautomatyzowane systemy, z drugiej strony wymuszałoby na przedsiębiorcach zwiększenie kontroli nad zautomatyzowanymi systemami wykorzystywanymi w ich działalności.

Rozwiązanie zakłada uniwersalne zastosowanie domniemania. Mogłoby one działać zarówno w relacjach B2B, B2C oraz w relacjach z organami administracji. Ze względów pragmatycznych oraz ostrożnościowych do rozważenia jest stopniowe wprowadzanie domniemania do systemu prawa. W pierwszym etapie

można przetestować działanie domniemania w węższym zakresie, ograniczając jego zastosowanie np. do określonego sektora gospodarki.

Rozszerzenie skutków prawnych użycia pieczęci elektronicznej wydaje się dopuszczalne z perspektywy prawa europejskiego, w szczególności dotyczy to Rozporządzenia eIDAS. Ten ostatni akt prawny tworzy w Artykule 35 określone domniemania związane z pieczęcią elektroniczną. Nie zabrania jednocześnie nadawania pieczęci elektronicznej dodatkowego znaczenia prawnego przez poszczególne systemy prawne państw członkowskich.

Propozycja legislacyjna

Poniżej przedstawiamy roboczą wersję propozycji zmian legislacyjnych w celu wprowadzenia do systemu prawa omawianego domniemania prawnego.

DOMNIEMANIE PRAWNE ZWIAZANE Z KORZYSTANIEM Z PIECZĘCI ELEKTRONICZNEJ

„Oświadczenia złożone z wykorzystaniem kwalifikowanej pieczęci elektronicznej w odniesieniu do czynności prawnych wskazanych w kwalifikowanym certyfikacie pieczęci elektronicznej poczytuje się w razie wątpliwości za złożone przez podmiot wskazany w ważnym kwalifikowanym certyfikacie pieczęci elektronicznej, chyba, że posłużenie się kwalifikowaną pieczęcią elektroniczną odbyło się poza kontrolą i bez winy tego podmiotu"

FORMA ELEKTRONICZNA

„Do zachowania elektronicznej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym lub kwalifikowaną pieczęcią elektroniczną"

Odnosząc się do przedstawionej propozycji legislacyjnej chcielibyśmy zwrócić uwagę na następujące zagadnienia:

- Przedstawiona propozycja ma charakter wstępny i roboczy. Jej podstawowym celem jest zainspirowanie dyskusji na temat rozwiązania rozważanego w niniejszym opracowaniu;
- Proponujemy ograniczyć domniemanie jedynie do sytuacji, w których oświadczeniu towarzyszy kwalifikowana pieczęć elektroniczna. Jest to rozwiązanie najbezpieczniejsze,

zwiększające w istotny sposób prawdopodobieństwo pozostawania pieczęci elektronicznej pod faktyczną kontrolą przedsiębiorcy;

- Zakładamy, że z uwagi na swoje uniwersalne znaczenie przepisy dotyczące omawianego domniemania prawnego powinny zostać wprowadzone do Kodeksu cywilnego. Dopuszczamy jednocześnie scenariusz zakładający rozłożenie w czasie wprowadzania domniemania do systemu prawa. Początkowo domniemanie może zostać wprowadzone jedynie do wybranych regulacji sektorowych, np. tam gdzie obowiązujące przepisy przewidują komunikację elektroniczną między podmiotami funkcjonującymi w zamkniętych systemach wynikających z przepisów prawa lub umów, a więc w przypadkach, do których nie znajduje zastosowania ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. Rozwiązania sektorowe dotyczące komunikacji elektronicznej znajdują się w szczególności w przepisach art. 7 Prawa bankowego, art. 43 ustawy o działalności ubezpieczeniowej i reasekuracyjnej, art. 35 ustawy o funduszach inwestycyjnych, art. 13 ustawy o obrocie instrumentami finansowymi, art. 6 ustawy o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych.

W przypadku pozytywnych doświadczeń z pilotażowego funkcjonowania domniemania mogłoby ono zostać rozszerzone na inne segmenty rynku;

- Przyjmujemy, że – podobnie jak w przypadku domniemania mającego zastosowanie do osób czynnych w lokalu przedsiębiorstwa – tak również w tym przypadku niezbędne jest wprowadzenie systemowych ograniczeń w zastosowaniu domniemania. Celem wprowadzenia ograniczeń jest redukcja negatywnych skutków sytuacji, w których pieczęć elektroniczna została przejęta przez osoby niepowołane. Wystąpienie takiej sytuacji jest w istotny sposób ograniczone przez wbudowane w schemat działania pieczęci elektronicznej zabezpieczenia, jednak nie może być całkowicie wykluczone. Propozycja wyklucza działanie domniemania w przypadku, gdy posłużenie się kwalifikowaną pieczęcią elektroniczną jest wynikiem działania będącego poza kontrolą przedsiębiorcy i bez jego winy. Dodatkowo, przedstawiona propozycja zakłada możliwość ograniczania zastosowania domniemania przez określenie w certyfikacie kwalifikowanej pieczęci elektronicznej parametrów czynności, które mogą być realizowane za jej pomocą. Domniemanie działałoby wyłącznie w odniesieniu do czynności spełniających wskazane parametry;

- Naturalną konsekwencją domniemania powinno być również uznanie, że oświadczenia woli opatrzone kwalifikowaną pieczęcią elektroniczną pozwalają zachować elektroniczną formę czynności prawnych. Z tego względu zamieszczamy również propozycję stosownej zmiany przepisów Kodeksu cywilnego o elektronicznej formie czynności prawnych.

PRZEPISY AML JAKO PRZESZKODA W PRAKTYCZNYM WYKORZYSTANIU POSTULOWANEGO ROZWIĄZANIA

Sygnalizujemy, że pełnemu wykorzystaniu proponowanego domniemania prawnego w celu podjęcia wyzwań omawianych w niniejszym opracowaniu mogą przeszkodzić przepisy ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu prania pieniędzy i finansowaniu terroryzmu („**Ustawa AML**"). Ich stosowanie wymaga bowiem identyfikowania konkretnych osób działających w imieniu podmiotów zbiorowych. Problem ten dotyczy wprawdzie wyłącznie tych podmiotów, które podlegają Ustawie AML, niemniej zważywszy, że Ustawa AML obejmuje aktualnie swoim zakresem wiele istotnych sektorów gospodarki, znaczenie sygnalizowanego problemu jest w praktyce bardzo duże.

Zgodnie z art. 34 ust. 2 Ustawy AML obowiązane instytucje identyfikują osobę upoważnioną do działania w imieniu klienta oraz weryfikują tożsamość i umocowanie do działania w imieniu klienta. Weryfikacja takiej osoby polega m.in. na potwierdzeniu danych identyfikacyjnych na podstawie dokumentu stwierdzającego tożsamość osoby fizycznej. Przytoczony wymóg ma na celu odzwierciedlenie w polskim porządku prawnym rekomendacji wskazanej w nocie interpretacyjnej do Rekomendacji 10 FATF[1] oraz implementację art. 13 ust. 1 Dyrektywy 2015/849, która stanowi w tym względzie pierwowzór legislacyjny dla polskiej Ustawy AML.

[1] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, str. 58

Należy jednak zwrócić uwagę na istotną różnicę, która zachodzi między Ustawą AML a przywołaną Dyrektywą 2015/849 oraz rekomendacją FATF. Zgodnie z art. 13 Dyrektywy „*przy wykonywaniu środków określonych w akapicie pierwszym lit. a) i b) podmioty zobowiązane weryfikują również, czy każda* ***osoba, która twierdzi, że działa w imieniu klienta, jest do tego upoważniona, oraz identyfikują i weryfikują tożsamość takiej osoby***". Brzmienie Dyrektywy w tym zakresie wiernie oddaje rekomendację FATF. W przywołanym przepisie obowiązek identyfikacji i weryfikacji odnosi się wyłącznie do osób, które twierdzą, że działają w imieniu klienta. Tymczasem, brzmienie art. 34 ust. 2 Ustawy AML sugeruje, że identyfikacja osoby upoważnionej do działania w imieniu klienta musi odbywać się zawsze.

Wskazana różnica staje się szczególnie widoczna w odniesieniu do transakcji realizowanych z wykorzystaniem zautomatyzowanych systemów transakcyjnych. W takim przypadku często nie będziemy mieli do czynienia z „osobą, która twierdzi, że działa w imieniu klienta". W świetle treści Dyrektywy 2015/849 moglibyśmy założyć, że w przypadku takich transakcji nie zachodzi obowiązek identyfikacji reprezentanta podmiotu zbiorowego. Tymczasem, wydaje się, że Ustawa AML nie stwarza przestrzeni do różnicowania rodzajów transakcji i również w odniesieniu do transakcji zautomatyzowanych wymaga identyfikacji osoby reprezentującej klienta.

Ogólną zasadę wyrażoną w art. 34 ust. 2 precyzuje art. 36 Ustawy AML, który wymienia rodzaje danych identyfikacyjnych osoby reprezentującej lub osoby upoważnionej do działania w imieniu klienta, które muszą zostać zebrane przez instytucje obowiązane w ramach procesu identyfikacji klienta. Zgodnie z art. 41 brak możliwości przeprowadzenia identyfikacji zgodnie z Ustawą AML powinien skutkować brakiem nawiązania stosunków gospodarczych z danym klientem lub ich rozwiązaniem.

Uzupełnieniem przywołanych przepisów jest art. 72 ust. 6 pkt 3), który wymaga z kolei, aby w ramach informacji przekazywanych do GIIF przez instytucje obowiązane pojawiły się również wskazane dane osoby reprezentującej osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej dokonującej raportowanej transakcji.
Przepisy Ustawy AML wskazują zatem, że instytucje obowiązane muszą pozyskiwać i weryfikować dane osób reprezentujących klientów bez względu na to, czy transakcje podlegające analizie AML są realizowane z wykorzystaniem systemów zautomatyzowanych czy nie. Postulowane w niniejszym dokumencie rozwiązanie, jakkolwiek może usprawnić cyfrowy obrót gospodarczy z perspektywy prawa cywilnego, nie wpłynie więc na modyfikację obowiązków wynikających z Ustawy AML. Tym samym, korzyści płynące z ewentualnego domniemania byłyby bardzo ograniczone.

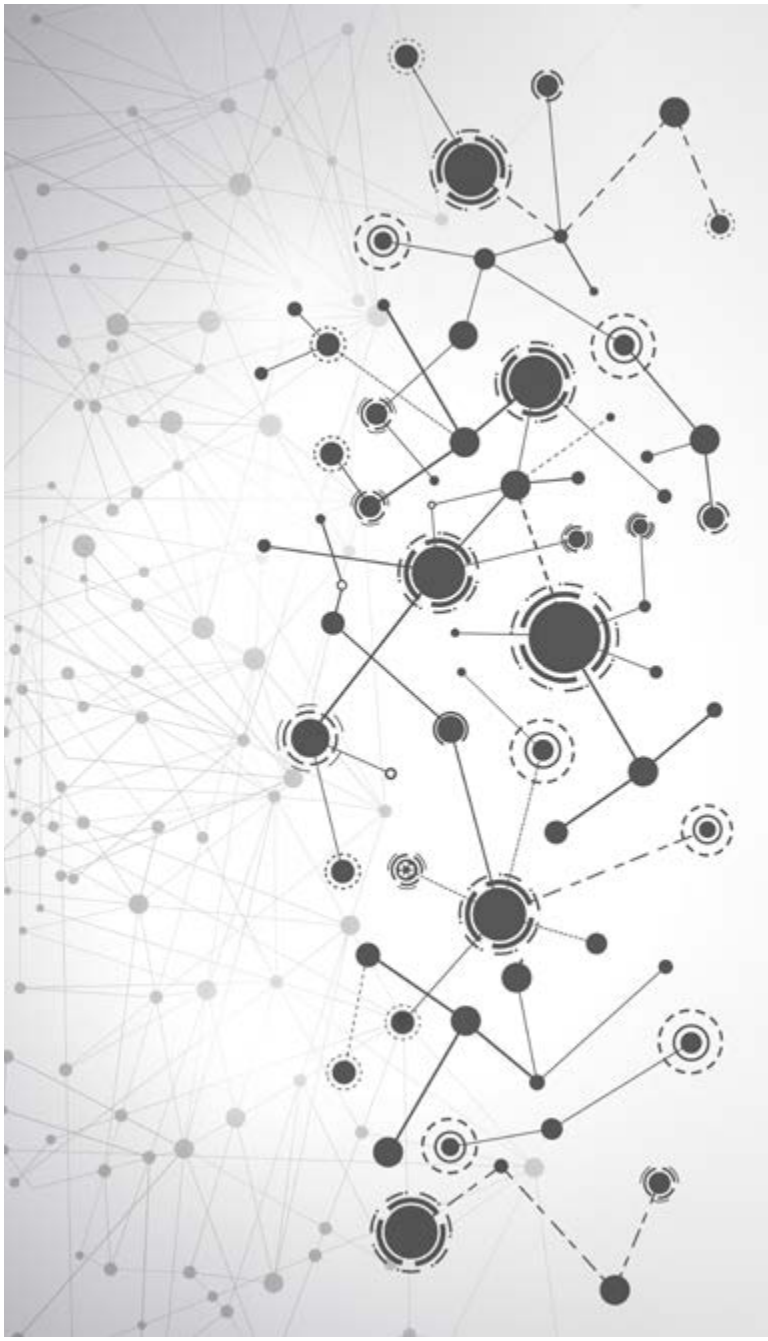
Zmiana takiego stanu rzeczy wymagałaby modyfikacji Ustawy AML lub przynajmniej wydania określonej interpretacji odnoszącej się do stosowania jej przepisów w odniesieniu do zautomatyzowanych systemów transakcyjnych. Chodzi o doprowadzenie do sytuacji, w której Ustawa AML podchodziłaby do identyfikacji osoby reprezentującej klienta w taki sam sposób jak Dyrektywa 2015/849 oraz rekomendacje FATF.

Ustawa AML, zgodnie z zasadą wyrażoną w Dyrektywie 2015/849 oraz w rekomendacjach FATF, powinna obligować do identyfikacji osób reprezentujących klienta tylko w sytuacjach, w których mamy do czynienia z osobą/osobami, które twierdzą, że działają w imieniu klienta. Z taką sytuacją będziemy mieli niewątpliwie do czynienia w większości

przypadków transakcji realizowanych w sposób analogowy. Formy składania oświadczeń woli w odniesieniu do takich transakcji zakładają udział osoby, która to oświadczenie składa. Sposób działania systemów zautomatyzowanych jest odmienny, co zostało wielokrotnie podkreślone w niniejszym dokumencie. Systemy te działają w sposób zautomatyzowany, niekiedy autonomiczny, bez udziału czynnika ludzkiego. Nie występują więc *„osoby, które twierdzą, że działają w imieniu klienta”.*

W przypadku transakcji wykonywanych przez systemy zautomatyzowane obowiązki AML powinny być skoncentrowane na prawidłowej identyfikacji podmiotu zbiorowego, który realizuje transakcje z wykorzystaniem takich systemów (rozwiązanie omawiane w niniejszym dokumencie może być w tym kontekście bardzo pomocne). W świetle specyfiki działania tych systemów obowiązek identyfikacji osoby reprezentującej jest w praktyce przymuszaniem do tworzenia pewnej fikcji. Instytucje obowiązane muszą bowiem wskazywać określone osoby reprezentujące pomimo tego, że mogą one w praktyce nie brać jakiegokolwiek świadomego udziału w transakcjach realizowanych przez zautomatyzowane systemy. Obowiązek regulacyjny, który sprowadza się do tworzenia fikcji należy uznać za nadmierny formalizm zmniejszający elastyczność prowadzenia działalności gospodarczej oraz nieprzyczyniający się do tworzenia jakiejkolwiek wartości dodanej.

W kontekście przepisów AML na uwagę zasługuje również art. 43 ust. 2 pkt 7) Ustawy AML. Zgodnie z tym przepisem nawiązywanie stosunków gospodarczych z klientem bez jego fizycznej obecności świadczy – co do zasady – o wyższym ryzyku prania pieniędzy. Ten sam przepis wprowadza jednocześnie wyjątek, zgodnie z którym domniemanie to nie zachodzi, jeżeli klient jest identyfikowany z użyciem wymienionych w tym przepisie środków, w szczególności kwalifikowanego podpisu elektronicznego. Wśród wymienionych środków nie ma jednak kwalifikowanej pieczęci elektronicznej. Wydaje się, że w przypadku wprowadzenia omawianego w niniejszym dokumencie domniemania do systemu prawa cywilnego należałoby do listy narzędzi, które umożliwiają zmniejszenie ryzyka prania pieniędzy dodać również kwalifikowaną pieczęć elektroniczną. Pozwala ona bowiem na bardzo wiarygodną identyfikację podmiotu zbiorowego.



POTENCJAŁ DLA ROZWOJU TECHNOLOGII

W naszej ocenie proponowane rozwiązanie stwarza bardzo dużą przestrzeń dla rozwoju technologii, które mogą istotnie zwiększyć bezpieczeństwo funkcjonowania domniemania w praktyce obrotu gospodarczego. Poniżej przedstawiamy kilka potencjalnych rozwiązań, które były przedmiotem dyskusji w trakcie warsztatów poprzedzających przygotowanie niniejszego opracowania.

Ograniczenia zawarte w certyfikacie

Certyfikaty kwalifikowanej pieczęci elektronicznej mogą zawierać dodatkowe nieobowiązkowe atrybuty, takie np. jak parametry czynności prawnych realizowanych za pomocą pieczęci oraz adresaci czynności prawnych dokonywanych z wykorzystaniem pieczęci. Dzięki wprowadzaniu dodatkowych parametrów do certyfikatu podmiot używający certyfikatu ma szansę zyskać większą kontrolę nad jego użyciem (np. wprowadzając maksymalną wartość czynności prawnej, która może być zrealizowana przy użyciu pieczęci). Odpowiednia standaryzacja dodatkowych atrybutów umożliwiłaby zwiększenie automatyzacji ich przetwarzania.

System monitorujący użycie pieczęci

Z uwagi na wynikające z domniemania przypisywanie oświadczeń złożonych z wykorzystaniem pieczęci do konkretnych osób prawnych kluczowa staje się możliwość natychmiastowej reakcji w przypadku wykrycia posługiwania się pieczęcią przez osoby niepowołane. Temu może służyć odpowiedni system tworzenia logów wykorzystywania pieczęci, który umożliwiłby bieżące monitorowanie jej wykorzystywania. W przypadku wykrycia niewłaściwego użycia pieczęci mogłaby ona być natychmiastowo unieważniana.

Zakładamy, że system zapisywania logów użycia pieczęci mógłby być budowany na bazie różnych rozwiązań technologicznych.

Inteligentne systemy dokonywania czynności z wykorzystaniem pieczęci

Standaryzacja i automatyzacja przetwarzania dodatkowych atrybutów zawartych w certyfikatach pieczęci umożliwiłaby budowanie systemów pozwalających na zawieranie cyfrowych umów przy automatycznej weryfikacji, czy parametry przypisane pieczęci elektronicznej umożliwiają zawarcie określonej czynności prawnej. Działanie systemu byłoby możliwe dzięki stworzeniu standardu parametryzacji czynności prawnych oraz uprawnień związanych z pieczęcią. Przewaga takiego rozwiązania nad tradycyjnymi ograniczeniami umocowania polegałaby na tym, że byłoby ono „samoegzekwujace", tj. z technicznego punktu widzenia nie byłoby możliwości wykorzystania pieczęci do dokonania czynności, które nie są zgodne z ustalonymi dla niej parametrami.

Potencjał wykorzystania technologii Blockchain

Szczególnie interesującym trendem w rozwoju technologii jest obecnie zastosowanie technologii Blockchain dla celów rozproszonej tożsamości (*distributed identity, self-sovereign identity* itp.). Również w opisywanych rozwiązaniach pieczęci elektronicznej można dostrzec potencjał zastosowania tej technologii.

Sieć Blockchain można interpretować w tym kontekście jako ujednolicony, powszechnie dostępny, niezmienialny rejestr. Jednak poza przechowywaniem danych rejestr ten umożliwia zaprogramowanie specjalnej logiki związanej z dostępem (odczytem, zapisem) do przechowywanych w nim danych – za pomocą mechanizmu tzw. smart kontraktów.
Można sobie wyobrazić wobec tego taki rejestr, który przechowywałby informacje o wystawionych przez daną organizację pieczęciach elektronicznych, jak również pozwalał na ujednolicony zestaw operacji możliwych do podpisania za pomocą tej pieczęci - dla przykładu, jeśli przy użyciu pieczęci będzie chciało się dokonać transakcji handlowej, to mechanizm smart kontraktu sprawdzi, czy kwota oraz przedmiot zamówienia są w akceptowalnych granicach i albo zaakceptuje taką transakcję, albo poczeka na dodatkową autoryzację.

Zestawy takich możliwych operacji mogłyby być ustandaryzowane i dostępne powszechnie dla przedsiębiorstw bez konieczności ponoszenia przez nie kosztów na utrzymanie własnej infrastruktury związanej z przetwarzaniem tych informacji.

Jednocześnie operacje wykonywane w takim rejestrze byłyby transparentne dla ich użytkowników (np. poszczególnych stron transakcji, ale też organów nadzorczych). Zdecydowanie ułatwiłoby to gromadzenie materiałów dowodowych w przypadku sporów, jak również reagowanie na sytuacje potencjalnie niebezpieczne jak np. niespodziewane, nietypowe wykorzystanie pieczęci do przeprowadzenia operacji masowych.

Zastosowanie technologii Blockchain w takim rozwiązaniu umożliwiłoby zarządzanie przez przedsiębiorstwo wydanymi pieczęciami elektronicznymi i kontrolę nad nimi– pozwalałoby np. na odwołanie wcześniej wystawionej pieczęci (np. w wyniku stwierdzenia wykradzenia cyfrowej kopii takiej pieczęci) czy ograniczenia uprawnień stosowania pieczęci (np. zmniejszenie limitu transakcji możliwych do zawarcia bez dodatkowego potwierdzenia) bez ingerencji w samą pieczęć – aktualizowane byłyby wyłącznie parametry smart kontraktu zapisanego w sieci Blockchain, odpowiadającego za weryfikację operacji wykonywanych przy użyciu pieczęci.

Analiza możliwości zastosowania technologii Blockchain dla pieczęci elektronicznej jest szczególnie interesująca z punktu widzenia planowanego rozwoju publicznych usług cyfrowych, takich jak np. projekt Wspólnej Infrastruktury Informatycznej Państwa (WIIP) czy European Blockchain Services Infrastructure (EBSI), które mogłyby stanowić trzon takiego rozwiązania.


VIRES IN NUMERIS-2013
LITECOINS

PRZYKŁADY ZASTOSOWAŃ

BUSINESS CASE 1
PLATFORMA HANDLOWA

Platforma internetowa działająca w segmencie B2B umożliwia zawieranie czynności prawnych on-line między przedsiębiorcą prowadzącym platformę a jego klientami będącymi przedsiębiorcami.

Platforma umożliwia zawieranie czynności, których przedmiotem są instrumenty finansowe. Każda z dokonywanych na platformie czynności może być potraktowana z perspektywy prawa jako odrębna czynność prawna zakładająca składanie elektronicznych oświadczeń woli.

Czynności realizowane są z dużą częstotliwością, często z ograniczonym udziałem czynnika ludzkiego.

Strony czynności prawnych zawieranych w taki sposób, chcąc mieć pewność, że czynności prawne są ważne i zostały złożone przez właściwe osoby, muszą dzisiaj odtwarzać łańcuch umocowań po stronie kontrahenta w celu upewnienia się, że osoba przypisana do danego elektronicznego oświadczenia woli jest faktycznie umocowana do jego składania. W przypadku zautomatyzowanych oświadczeń realizowanych przez system IT nawet ustalenie prawidłowego łańcucha umocowań może okazać się niewystarczające do zapewnienia bezpieczeństwa prawnego. Zautomatyzowane oświadczenie będzie bowiem zawsze budziło wątpliwości w zakresie tego, czy dany komunikat wytworzony przez zautomatyzowany system faktycznie był objęty świadomością osoby umocowanej do reprezentowania przedsiębiorcy.

Współcześnie wiele internetowych platform handlowych funkcjonuje w omawianym modelu. Pokazuje to tym samym skalę niepewności prawnej, jaką dotknięty jest współczesny obrót cyfrowy.

CO WNOSI ROZSZERZENIE ZNACZENIA PRAWNEGO PIECZĘCI ELEKTRONICZNEJ?

W omawianym przypadku użycie kwalifikowanej pieczęci cyfrowej dawałoby nie tylko gwarancję pochodzenia oświadczenia od danego podmiotu, ale towarzyszyłoby jej również domniemanie skutkujące przypisaniem oświadczenia do tej osoby. Zwalniałoby to kontrahenta z konieczności weryfikacji łańcucha umocowań lub też ewentualnego ryzyka związanego z brakiem przeprowadzenia takiej weryfikacji.

Dokument jest wynikiem prac przeprowadzonych w ramach grupy ds. rejestrów rozproszonych działających w ramach Ministerstwa Cyfryzacji oraz warsztatów przeprowadzonych w ramach Koalicji na rzecz Polskich Innowacji.

BUSINESS CASE 2
SELF-SOVEREIGN DATA

Istotnym trendem, wokół którego zaczyna powstawać coraz więcej ciekawych rozwiązań technologicznych (np. Holochain, Ocean Protocol) jest koncepcja zarządzania danymi przez podmioty danych. Zakłada ona, że to podmioty danych są właścicielami dotyczących ich danych i decydują, komu i na jakich zasadach je udostępniają. Procesy udostępniania/transferów danych odbywają się w sposób zautomatyzowany.

Podmiot danych ustala różne parametry udostępniania danych w odniesieniu do różnych kategorii danych. Parametry są zapisywane w postaci smart kontraktów, których ustandaryzowane warunki są przedstawione podmiotom zainteresowanym dostępem do danych.

Dostęp do danych oraz ewentualne transfery danych odbywają się na zasadzie peer-to-peer w sposób zautomatyzowany. Dane są umieszczone na infrastrukturze IT kontrolowanej przez podmiot danych. Zapytania o dane odbywają się przez API. Dostęp do danych i ewentualne transfery przebiegają na podstawie ustandaryzowanych smart kontraktów.

Na potrzeby obrotu danymi dochodzi do dokonywania czynności prawnych, w tym również do składania oświadczeń woli. Odbywa się to jednak w sposób zautomatyzowany. System podmiotu zainteresowanego wysyła automatycznie kwerendę, która trafia do systemu podmiotu danych. Przedstawiane są oczekiwane parametry transakcji. Automatycznie następuje zawarcie umowy o określonej treści. W procesie w sposób bezpośredni nie uczestniczy jakikolwiek czynnik ludzki.

Przykładem zastosowania powyższej koncepcji jest np. obrót danymi medycznymi. Instytuty badawcze oraz firmy farmaceutyczne poszukują danych medycznych o określonych parametrach na potrzeby rozwoju nowych leków lub terapii. System zamawiającego definiuje parametry pożądanych danych i następnie wysyła kwerendę. Po odnalezieniu żądanych danych dochodzi do ustalenia parametrów transakcji (cena za dane, czas korzystania etc.), a następnie do jej automatycznego zawarcia i realizacji. Wszystko odbywa się bez zaangażowania czynnika ludzkiego.

CO WNOSI ROZSZERZENIE ZNACZENIA PRAWNEGO PIECZĘCI ELEKTRONICZNEJ?

Podmiot danych mógłby skorzystać z rozwiązania wymuszającego stosowanie kwalifikowanej pieczęci elektronicznej przez kontrahentów uzyskujących dostęp do danych. Dzięki temu podmiot danych miałby pewność, że kontrahenci są związani zobowiązaniami wynikającymi z umowy dotyczącej nabywania danych. Zwiększa to bezpieczeństwo obrotu, a jednocześnie daje korzyści wynikające z automatyzacji dysponowania danymi przez podmiot danych.