02

7 listopada 2019

RODO a technologia blockchain

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.

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".

Wersja 1.01

Opracowanie przygotował i zredagował zespół autorski:

Jan Byrski, Kancelaria Traple Konarski Podrecki & Wspólnicy, Uniwersytet Ekonomiczny w Krakowie
Agnieszka Hołownia-Niedzielska, ProtectAuth
Marta Kownacka, kancelaria LawIT
Janusz Łaski, ING Bank Śląski SA, Rada Banków Depozytariuszy przy ZBP
Piotr Rutkowski, Ministerstwo Cyfryzacji, NASK PIB
Michał Starczewski, kancelaria BWHS
Michał Tuszyński, kancelaria GWW Legal
Marcin Zarakowski, Lisk Foundation

Graficzny opracowanie WK/BM, Ministerstwo Cyfryzacji, Marko Bazarko

SPIS TREŚCI

WSTĘP

RODO zostało przygotowane jako akt prawa neutralny technologicznie, ale stojące za nim założenie bazuje na scentralizowanych bazach danych. W tym układzie dokonuje się dwukierunkowa komunikacja między podmiotem zarządzającym bazą danych a jej użytkownikami. Identyfikacja administratora danych nie sprawia tu większych trudności. Powyższe założenie nie odpowiada architekturze rozproszonych baz danych, takich jak blockchain. Stąd wynikają problemy w określeniu zgodności niektórych rozwiązań opartych na technologii blockchain z RODO.

Mimo że technologia blockchain, a w szczególności niektóre jej cechy (niezmienność zapisu, otwarty charakter rejestrów), pozornie pozostają w konflikcie z założeniami RODO, dalszy rozwój rozwiązań na niej opartych może przyczynić się do pogłębienia ochrony danych osobowych i usprawnienia swobodnego ich przepływu. Dzięki wykorzystaniu technologii blockchain i rejestrów rozproszonych podmioty mogą bowiem na nowo odzyskać kontrolę nad własnymi danymi osobowymi, decydując w bezpieczny dla nich sposób o zakresie, adresatach i czasie udostępnienia. Sieć blockchain jako elektroniczny nośnik trwały gwarantuje niezmienność zapisu, co oznacza, że nie istnieje możliwość wykorzystania danych, a następnie ich modyfikacji czy usunięcia. Dzięki temu technologia blockchain może stanowić znakomity sposób przeciwdziałania nieuprawnionemu wykorzystaniu danych.

Niniejsze opracowanie odnosi się do sytuacji, w których w sieci blockchain umieszczone mają być dane osobowe. Warto nadmienić, że w przypadku umieszczania lub przesyłania danych dotyczących osób prawnych, umożliwiających identyfikację osób prawnych i ich działań nie istnieje potrzeba spełniania wymagań związanych z RODO, gdyż zidentyfikowanie osoby prawnej nie oznacza zidentyfikowania osoby fizycznej. W związku z powyższym, wątpliwości związane z RODO nie będą dotyczyły informacji przechowywanych w sieciach blockchain, których uczestnikami są osoby prawne, w szczególności identyfikowane pieczęcią elektroniczną lub analogicznym rozwiązaniem. Pieczęć elektroniczna może stanowić również częściową odpowiedź na potrzeby innych rozwiązań technologicznych wykorzystujących blockchain, gdzie zagadnienia dotyczące RODO byłyby rozpatrywane tylko w kontekście klientów czy instytucji, które nie mają osobowości prawnej.

O zgodności z RODO można mówić nie tyle w odniesieniu do samego rozwiązania technicznego, ile do sposobu jego wykorzystania. Dlatego ostatecznie zasadność stosowanych metodologii należy zawsze rozpatrywać w stosunku do konkretnych, indywidualnych przypadków.

Warto zaznaczyć, że niniejszy dokument przedstawia dwa aspekty zagadnienia. Część pierwsza dotyczy podstawowych pojęć i ich odniesienia do technologii blockchain oraz sposobów, w jaki technologia może odpowiadać wymaganiom RODO. Część druga zawiera rozważania na temat zasadności ustawowego ograniczenia niektórych praw wynikających z RODO w związku z ogromnym znaczeniem technologii blockchain. Obie etapy wywodu są warte poznania, a zawarte w nich spostrzeżenia pozwalają zrozumieć złożoność odniesienia technologii blockchain do zagadnienia ochrony danych osobowych i drogi, jakimi może zostać wypracowane stanowisko w tym zakresie.

Grupa Robocza może przedstawić wskazówki, co do interpretacji obowiązujących przepisów, a także nakreślić wytyczne technologiczne, które zwiększają bezpieczeństwo danych w sieciach. Należy mieć jednak na uwadze, że instytucją kompetentną do pełnienia funkcji nadzorczych nad przetwarzaniem danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych.

KLUCZOWE POJĘCIA

W celu uniknięcia wątpliwości niniejszy rozdział zawiera definicje pojęć używanych w dokumencie.

Pojęcia związane z technologią

- **Blockchain** – to rozproszona, współdzielona między siecią komputerów baza danych, działająca według określonych dla danej sieci zasad. Nazwa oznacza łańcuch bloków, czyli sposób, w jaki organizuje się informacje umieszczając je jedna za drugą wraz ze wskaźnikiem na poprzednią wiadomość. Wskaźnik oraz zawartość bloku są zabezpieczane kryptograficznie[1]. Sieci blockchain składają się z węzłów, (node), które są uczestnikami sieci i przechowują dane.

- **Funkcja haszująca** – funkcja, która na podstawie dowolnego ciągu danych generuje ciąg znaków o określonej długości (zob. hash)[2]. Danymi, dla których wykonuje się funkcję, mogą być dowolne ciągi znaków, zestawienia informacji, pliki czy programy komputerowe. W przypadku funkcji haszującej ważną cechą jest odporność na kolizje, rozumiana jako zminimalizowanie szansy na uzyskanie takiego samego wyniku z dwóch różnych informacji.

- **Hash** (indeks, wskaźnik, skrót nieodwracalny) – efekt działania funkcji haszującej, ciąg znaków przyporządkowany określonym danym, które mają formę elektroniczną. W niniejszym dokumencie mowa o wskaźnikach, które powstają w wyniku funkcji jednokierunkowej, tzn. pozwalającej na uzyskanie wskaźnika z danych, ale nie odwrotnie. Funkcje takie, ze względu na odporność na kolizje (por. funkcja haszująca), pełnią rolę zabezpieczeń kryptograficznych.

- **Miner** (górnik) – osoba lub instytucja wykorzystująca moc obliczeniową komputera czy komputerów do tworzenia kolejnych bloków informacji w sieci blockchain. Proces ten nazywany jest „kopaniem". Za stworzenie kolejnego bloku miner otrzymuje nagrodę w postaci kryptowaluty[3].

- **Peppered hash** – bezpieczniejszy kryptograficznie hash, który powstaje poprzez wprowadzenie do informacji poddanych funkcji haszującej dodatkowego losowego, sekretnego składnika znanego jedynie haszującemu[4]. Dodatkowy składnik jest taki sam dla wszystkich danych w określonej sekcji, np. dla haseł dla jednej aplikacji.

[1] na podst. Polska Izba Informatyki i Telekomunikacji, *Blockchain w Polsce możliwości i zastosowanie*, Warszawa 2018.
[2] na podst. Rajeev Sobti1, G.Geetha, *Cryptographic Hash Functions: A Review,* „International Journal of Computer Science Issues", Vol. 9, Issue 2, Nr 2, March 2012.
[3] na podst. Jakub A. Bartoszewski, *Blockchain Compass 2018*, Fundacja Startup Poland, Warszawa 2018.
[4] na podst. https://en.wikipedia.org/wiki/Pepper_(cryptography) (dostęp:14.10.2019.

- **Proof-of-Stake** (PoS) – sposób dodawania bloków do łańcucha, który można porównać do praw majątkowych z tytułu udziałów w spółce kapitałowej. Nagroda za zatwierdzenie bloku może być rozdysponowana zgodnie z liczbą posiadanych aktywów danego typu. W związku z tym nie ma konieczności podłączania do sieci tak dużej mocy obliczeniowej, jak w przypadku Proof of Work[5].

- **Proof-of-Work** (PoW) – sposób dodawania bloków do łańcucha wykorzystany np. w sieci Bitcoin. W tym typie sieci wszystkie węzły mają możliwość umieszczania kolejnego bloku danych, a prawdopodobieństwo dodania kolejnego bloku przez węzeł zależy od mocy obliczeniowej, z jakiej korzysta węzeł6. Wykonywaniem PoW w sieciach zajmują się minerzy.

- **Salted hash** - bezpieczniejszy kryptograficznie hash, który powstaje przez wprowadzenie do informacji poddanych funkcji haszującej dodatkowego, indywidualnego losowego składnika[7]. Dodatkowy składnik jest inny dla każdego wykonania funkcji haszującej, np. dla każdego z haseł dla jednej aplikacji.

- **Sieci prywatne** – sieć blockchain, do której dołączenie jest możliwe jedynie po spełnieniu wymogów określonych instytucji, takich jak: zaproszenie, podpisanie umowy, posiadanie określonego statusu prawnego itp. Dopiero po uzyskaniu zgody można zyskać status węzła sieci, pobierać z niej dane czy udostępniać je innym zweryfikowanym podmiotom[8].

- **Sieci publiczne** – sieci blockchain, do których może dołączyć każda osoba lub instytucja zyskując status węzła sieci, pobierając dane i udostępniając je kolejnym jednostkom[9]. Nie jest potrzebna zgoda żadnej jednostki, aby kolejny uczestnik mógł zostać częścią sieci.

- **Sieci permissioned** – sieć blockchain, w której dodawanie nowych informacji i potwierdzanie ich prawdziwości (walidacja) jest dostępne tylko dla jednostek, które uzyskały zgodę na dołączenie do sieci. Zdecydowana większość sieci permissioned jest sieciami prywatnymi, stąd pojęcia te są często utożsamiane.

- **Sieci permissionless** – sieć blockchain, w której dodawanie nowych informacji i potwierdzanie ich prawdziwości (walidacja) jest dostępne dla każdego i nie wymaga uzyskania zgody od żadnego podmiotu czy osoby. Zdecydowana większość sieci permissionless jest sieciami publicznymi, stąd pojęcia te są często utożsamiane.

Pojęcia z zakresu prawa

- **Administrator danych osobowych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

[5] za. Polska Izba Informatyki i Telekomunikacji, Blockchain w Polsce możliwości i zastosowanie, Warszawa 2018.
[6] Tamże.
[7] na podst. https://en.wikipedia.org/wiki/Salt_(cryptography), (dostęp: 14.10.2019).
[8] Leksykon pojęć na temat technologii blockchain i kryptowalut, red. Krzysztof Piech, Ministerstwo Cyfryzacji, Warszawa 2016.
[9] Tamże.

- **Anonimizacja danych** – pojęcie niezdefiniowane wprost w aktach prawnych, oznaczające nieodwracalne przetworzenie danych w taki sposób, by osób, których te dane dotyczą, nie można było zidentyfikować.

- **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

- **Podmiot Przetwarzający (Procesor)** – podmiot przetwarzający dane osobowe w imieniu Administatora i na jego żądanie; nie ustala samodzielnie celów i sposobów przetwarzania danych.

- **Pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; proces pseudonimizacji jest możliwy do odwrócenia (w przeciwieństwie do procesu anonimizacji), a dane osobowe przetworzone w taki sposób umożliwią ponowne ich przypisanie osobie fizycznej.

- **Przetwarzanie danych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

- **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), [Dz.U.UE.L z 2016 roku, pozycja 119/1].

- **Współadministrator danych** - Administrator danych osobowych, który wraz z co najmniej jednym innym Administratorem ustala cele i sposoby przetwarzania danych osobowych;

POJĘCIA ZWIĄZANE Z TECHNOLOGIĄ KLUCZOWE POJĘCIA

POJĘCIA Z ZAKRESU PRAWA

ZASADNICZE ZIDENTYFIKOWANE PROBLEMY I POTRZEBY

Zdecentralizowany charakter sieci blockchain oraz trwałość zapisanych w niej informacji jest źródłem dwóch rodzajów trudności związanych z przetwarzaniem danych osobowych przy wykorzystaniu tej technologii.

Pierwszy rodzaj trudności jest związany z identyfikacją ról zdefiniowanych przez RODO. Kim jest administrator danych osobowych? Czy da się zidentyfikować podmiot przetwarzający dane? Zależnie od odpowiedzi na te pytania różnie będą się rozkładać obowiązki uczestników sieci blockchain oraz ich odpowiedzialność.

Drugi rodzaj trudności wynika z obowiązku zapewnienia praw osób, których dane są przetwarzane. W szczególności jest to prawo do informacji, kto, w jaki sposób i jak długo przetwarza dane. Jest to także prawo do żądania poprawienia danych lub zaprzestania ich przetwarzania. Trwałość informacji zapisanych w łańcuchu bloków utrudnia, lub wręcz uniemożliwia, wypełnienie wszystkich tych praw.

WSKAZANIE POTRZEB NA PRZYKŁADZIE PRZYPADKU BIZNESOWEGO

Jasne określenie relacji między obowiązkami wynikającymi z RODO a technologią blockchain ma kluczowe znaczenie dla kolejnych zastosowań technologii. Niepewność w zakresie możliwości przechowywania czy przesyłania danych poprzez sieci prywatne czy publiczne pozostawia rynek w sytuacji decyzji dotyczącej nie tylko prac nad rozwojem nowych produktów, ale też podejmowania pewnego ryzyka, bądź wycofywania się z potrzebnych i poszukiwanych na rynku rozwiązań ze względu na wątpliwości związane z aspektami prawnymi. Zagadnienie danych osobowych jest obecne w tak wielu projektach, produktach czy usługach, że wiele firm pracujących z nowymi technologiami już się z nim zetknęło lub zetknie się z nim w najbliższym czasie. Poniżej omówiono przykładowe rozwiązanie biznesowe, dla którego zagadnienia związane z siecią blockchain i danymi osobowymi mają fundamentalne znaczenie.

Potwierdzenie i historia działań klienta w sieci publicznej

Blockchain publiczny charakteryzuje się tym, że jest niezależny i dostępny dla każdego na równych zasadach: zarówno dla indywidualnego klienta, jak dla ogromnej korporacji. Ta cecha sprawia, że informacje zapisane w sieci są tak samo dostępne dla obu stron i potwierdzone przez niezależną technologię. Jeśli klient wykonał jakąś znaczącą akcję w systemie sprzedawcy, to w interesie obu stron, często wymaganym przez przepisy prawa konsumenckiego, jest zapisanie tego działania na trwałym nośniku z dostępem dla obu stron. Przykładem takich działań będzie zawarcie umowy ubezpieczenia, czy zlecenie wykonania indywidualnego zamówienia. W takim przypadku w sieci powinny zostać zapisane podstawowe parametry akcji, w tym: kto ją wykonał i kto zatwierdził, a instytucja przyjmująca zlecenie zapisuje jego dane w sieci, zaś klient, za pomocą strony internetowej czy aplikacji zatwierdza dane, tym samym potwierdzając swoje zobowiązanie, w przypadku indywidualnego zamówienia lub godzinę zawarcia polisy w przypadku ubezpieczenia. W razie wątpliwości lub konfliktu obie strony mają możliwość uzyskania jednoznacznego potwierdzenia treści i stron biorących udział w procesie bez możliwości modyfikacji danych. Równocześnie w sieci jest tworzona historia zleceń danego klienta, dostępna dla niego również po zakończeniu współpracy z instytucją. Takie rozwiązanie ma pełną funkcjonalność biznesową jedynie wtedy, gdy w sieci znajdują się dane osobowe klienta, pracownika sprzedawcy (jeśli taki występuje w procesie) oraz osób zaangażowanych, np. ubezpieczanych.

ADMINISTRATOR DANYCH OSOBOWYCH W PROJEKTACH OPARTYCH NA TECHNOLOGII BLOCKCHAIN

W przypadku sieci typu *permissioned* będą nim niejednokrotnie operatorzy sieci, nierzadko funkcjonujący jako współadministratorzy (art. 26 RODO).

Przy zachowaniu odpowiedniej decentralizacji tego typu sieci za administratorów nie powinny zostać uznane podmioty uczestniczące w mechanizmie konsensusu, tzw. węzły sieci (np. wspomniani wyżej minerzy w przypadku *Proof-of-work* czy walidatorzy w przypadku *Proof-of-stake*). Nie decydują one o celach przetwarzania danych; wykonują jedynie czynności techniczne wyabstrahowane od treści danych zawartych w przetwarzanych transakcjach.

Nie oznacza to, że w kontekście blockchainów *permissionless* nigdy nie będziemy mieli do czynienia z administratorami danych. Mogą stać się nimi podmioty używające zdecentralizowanej infrastruktury do prowadzonej przez siebie działalności. Wtedy może powstać jednak problem sprostania ciążącym na administratorze obowiązkom wobec podmiotów danych, a czasem możliwe będzie stosowanie art. 11 RODO.

Zasada minimalizacji zapisu danych osobowych na blockchain

Zapisywanie danych osobowych w rejestrach opartych na blockchain wiąże się z istotnym ryzykiem dla osób fizycznych, których te dane dotyczą oraz z niemożliwością pełnego realizowania praw i obowiązków wynikających z RODO. Z tego względu, należy powstrzymywać lub ograniczyć do minimum zapisywanie danych osobowych na rejestrach opartych na blockchain.

ZAPISYWANIE DANYCH OSOBOWYCH OFF-CHAIN

Jeśli to możliwe, dane osobowe powinny być przetwarzane poza łańcuchem bloków (*off-chain*). W łańcuchu bloków mogą znajdować się odnośniki (np. *hash-pointers*) pozwalające zweryfikować poprawność danych. Takie rozwiązania są rodzajem pseudonimizacji danych. Dzięki przetwarzaniu wszystkich danych osobowych *off-chain* unika się trudności z korzystaniem z rozproszonych baz danych zgodnie z RODO. Wszystkie rozwiązania skutecznie uniemożliwiające dostęp z poziomu blockchaina do informacji o danych osobowych osobom nieznającym stosownego hasła będą wystarczające z punktu widzenia RODO.

Dane osobowe przetwarzane off-chain znajdują się w scentralizowanej bazie danych, w przypadku której łatwe jest zidentyfikowanie administratora danych osobowych, na którym ciążą wszelkie obowiązki, na czele z obowiązkiem informacyjnym i obowiązkiem zapewnienia praw osób, których dane przetwarza. Należy mieć jednak na uwadze, że zmiana danych osobowych (np. ich aktualizacja lub uzupełnienie) może spowodować niezgodność między odnośnikiem przechowywanym w łańcuchu bloków a danymi przetwarzanymi *off-chain*.Przy spełnieniu wymagań dotyczących pseudonimizacji za zgodne z RODO należy uznać rozwiązania przechowujące dane osobowe poza łańcuchem bloków (*off-chain*), a pozostawiające w rejestrze opartym na blockchain wyłącznie odnośniki do tych danych, np. w postaci *hash-pointers.* Tego rodzaju rozwiązania mogą być atrakcyjne głównie dla sieci prywatnych lub sieci typu *permissioned*, a nie dla sieci publicznych (*public, permissionless*), albowiem wiążą się z ograniczeniem decentralizacji rejestru opartego na blockchain i wprowadzeniem swego rodzaju zaufanej trzeciej strony, trzymającej pieczę nad danymi osobowymi zapisanymi poza rejestrem (*off-chain*). W takim wypadku administratorem danych jest podmiot przechowujący dane off-chain i prowadzony przez niego rejestr musi być zgodny z wymaganiami RODO. Poszczególne węzły sieci (node) nie pełnią roli współadministratorów ani procesorów.

W zapewnieniu, by sposób zapisania odnośnika do danych przechowywanych off-chain uniemożliwiał identyfikację osoby, pomocne jest wykorzystanie technologii, która chroni dane osoby nawet w przypadku posiadania tych danych. Dotyczy to sytuacji, w której wskaźniki w sieci blockchain zostałyby zapisane przez firmę X w formie standardowej funkcji haszującej wykonywanej np. na imionach i nazwiskach. Przy odpowiednio licznej bazie imion i nazwisk istnieje techniczna możliwość ustalenia, jakim osobom odpowiadają wskaźniki danych zapisane w sieci. Najnowsze środki techniczne i technologiczne blokują takie działania. Do środków tych należy np. stosowanie nieodwracalnej, odpowiednio złożonej funkcji skrótu zawierającej dodatkowe informacje, niezwiązane z danymi poddawanymi działaniu funkcji (*salt and pepper hashes*).

TECHNIKI PSEUDONIMIZACJI I ANONIMIZACJI A BLOCKCHAIN

RODO nie wskazuje konkretnych technik (zgodnie z zasadą neutralności technologicznej). Administratorzy danych będą rozliczani z efektów: czy przetwarzane przez nich dane zostały zanonimizowane lub spseudonimizowane, czy nie. Poniżej przedstawiono przykładowe techniki, które mogą doprowadzić do skutecznego zanonimizowania lub spseudonimizowania danych. Nie można wykluczyć, że rozwiązania wykorzystujące odpowiednie zabezpieczenie kryptograficzne danych osobowych zapisanych w rejestrach bazujących na technologii blockchain zapewnią wystarczający, zgodny z RODO, poziom bezpieczeństwa dla podmiotów, których te dane dotyczą. Wymagany przez RODO standard ochrony danych osobowych może zostać również zapewniony przy spełnieniu odpowiednich warunków. Chodzi tu o wykorzystanie technologii uniemożliwiających lub wysoce utrudniających identyfikację osób, dzięki zapewnieniu niemożności odszyfrowania danych zapisywanych na blockchain. Każde rozwiązanie zwiększające bezpieczeństwo danych wymaga indywidualnej analizy w kontekście adekwatności zastosowania, zbadania możliwości identyfikacji przez wydzielenie wpisów o konkretnej osobie, czy przez konkretny zapis (np. pojedynczy zapis o określonej cesze, takich np., jak charakterystyczna, wysoka kwota). W ramach rozważania dostępnych rozwiązań warto uwzględnić poniższe możliwości technologiczne:

- szyfrowanie kluczami jednorazowymi,
- funkcje haszujące odporne na ataki z wykorzystaniem komputerów kwantowych,
- salted hashes,
- peppered hashes,
- stealth addresses – jednorazowe adresy generowane na potrzeby umieszczenia danych lub przesłania transakcji,
- ring signatures – schemat służący do podpisania i szyfrowania wiadomości, który jest używany przez grupę osób i umożliwia zweryfikowanie prawdziwości podpisu, ale równocześnie nie umożliwia zidentyfikowania osoby, która go użyła,
- ring confidential transactions – sposób przesyłania transakcji w sieci blockchain, w którym przesyłana wartość nie jest możliwa do poznania przez osoby inne niż uczestnicy transakcji.

Wybrane rozwiązanie należy również przeanalizować, pod kątem:

- rozwoju technologii, który zwiększy szanse podwyższenia poziomu bezpieczeństwa rozwiązania, np. komputery kwantowe,
- czasu, przez jaki zapisywane dane będą stanowiły wartość dla kogoś, kto uzyska do nich dostęp (np. dane dotyczące zakupu nieruchomości, a dane dotyczące zakupów w drogerii),
- liczby i zawartości informacji, jakie będą dodawane do sieci, dotyczących jednej osoby oraz możliwości powiązania tych informacji,
- uzyskania, i w razie potrzeby odzyskania, dostępu do informacji przez osoby uprawnione, np. w przypadku zgubienia urządzenia z kluczem szyfrującym czy usunięcia danych potrzebnych do odczytania informacji.

MOŻLIWOŚĆ USTAWOWEGO OGRANICZENIA NIEKTÓRYCH PRAW PODMIOTÓW DANYCH WYNIKAJĄCYCH Z RODO W PRZYPADKU PRZETWARZANIA DANYCH OSOBOWYCH PRZY UŻYCIU TECHNOLOGII BLOCKCHAIN

W świetle art. 23 RODO jest możliwe ograniczenie (zarówno na podstawie prawa Unii, jak i na podstawie prawa państwa członkowskiego, w tym prawa polskiego) zakresu obowiązków i praw przewidzianych w art. 12-22 i w art. 34, a także w art. 5 RODO, o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22. **Ograniczenie takie jest możliwe jedynie, o ile nie narusza ono istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym celom określonym w art. 23 ust. 1 lit. a-j RODO.**

Jak słusznie wskazuje się w literaturze: *Artykuł 23 stanowi zatem najpoważniejsze odstępstwo w procesie tworzenia jednolitego standardu ochrony danych osobowych. Prawodawca unijny na jego podstawie zezwala państwom członkowskim na przyjęcie przepisów ograniczających przewidziane w rozporządzeniu prawa i obowiązki administratorów i podmiotów przetwarzających, jeśli – zdaniem danego państwa – takie ograniczenie jest niezbędne w celu realizacji określonych przesłanek, w szczególności interesu publicznego tego państwa lub całej UE*[10].

Należy mieć na uwadze, że akt prawny wprowadzający ograniczenie musi zawierać szczegółowe przepisy, o których mowa w art. 23 ust. 2 lit. a-h RODO. Tym samym przepisy krajowe muszą zawierać elementy w celu zagwarantowania pewnego poziomu ochrony danych osobowych (np. w zakresie celów lub kategorii przetwarzania, kategorii danych osobowych, zakresu wprowadzanych ograniczeń, ustanowienia tajemnicy zawodowej etc.). Zgodnie z art. 23 ust. 1 lit. e RODO istnieje możliwość wprowadzenia ograniczenia służącego **innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu** Unii lub

[10] *Ogólne rozporządzenie o ochronie danych osobowych.* Komentarz, red. M. Sakowska-Baryła, Warszawa 2018,

państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu.

Motyw 73 (preambuły) RODO jako przykład interesu publicznego wskazuje m. in. **na ważny interes gospodarczy** lub finansowy Unii lub państwa członkowskiego. Należy przy tym zauważyć, że w art. 23 RODO nie zastrzeżono, aby z ograniczenia praw podmiotów danych związanego z interesem publicznym mogły korzystać tylko organy publiczne. Zatem – i takie zostały wprowadzone już regulacje w ustawie sektorowej (ustawa weszła w życie 4 maja 2019 r.) – regulacje krajowe w tym zakresie mogą odnosić się także do podmiotów sektora prywatnego. Niemniej ograniczenia te powinny być zgodne z wymogami Karty praw podstawowych oraz Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności.

Z uwagi na bardzo szerokie możliwości w zakresie zastosowania technologii blockchain zarówno w sektorze prywatnym (w tym m. in. w sektorze finansowym) jak i publicznym oraz liczne zalety (w tym odporność na awarie systemów informatycznych, odporność na cyberataki, transparentność, niskie koszty, dużą wydajność i skalowalność etc.) można zasadnie przyjąć, że **wykorzystanie tej technologii leży w ogólnym interesie publicznym, jakim jest ważny interes gospodarczy lub finansowy państwa członkowskiego.** Wydaje się, że ważny interes gospodarczy może być w tym zakresie związany także z umożliwieniem (w szczególności przez stworzenie odpowiednich ram prawnych) legalnego rozwoju innowacyjnych i bezpiecznych usług cyfrowych.

Niewątpliwie z uwagi na właściwości technologii blockchain (w tym z uwagi na jej zdecentralizowany i rozproszony charakter) nie jest możliwe skuteczne realizowanie w pełnym zakresie wszystkich praw przysługujących na podstawie przepisów RODO (np. prawa do poprawiania danych, zgłaszania sprzeciwu wobec przetwarzania danych, czy usuwania danych [prawo do bycia zapomnianym]). Problemy z tym związane zostały zasygnalizowane także na oficjalnej stronie organu nadzorczego[11].

Przy ograniczeniu podstawowych praw i wolności należałoby zwrócić w szczególności uwagę na proporcjonalność oraz niezbędność takich działań, tj. zapewnić, aby **ograniczenie dotyczyło jedynie tych praw, które muszą być ograniczone dla możliwości skutecznego wykorzystania technologii blockchain.** Ograniczenia wprowadzone w celu realizacji określonych w 23 ust. 1 lit. e RODO nie mogłyby także naruszać istoty podstawowych praw i wolności.

Przykładowo, wprowadzenie ograniczeń może być niezbędne w kontekście realizacji prawa do bycia zapomnianym (art. 17 RODO). Z uwagi na charakter blockchain **nie sposób byłoby przyjąć, moim zdaniem, że takie prawo można by skutecznie zrealizować w odniesieniu do danych osobowych, które znalazły się w blockchain.** W tym zakresie należałoby jednak zapewnić odpowiednie środki techniczne i organizacyjne mające na celu odpowiednie zabezpieczenie przetwarzanych danych, np. takie, które pozwoliłyby ograniczyć dostęp do danych.

Podobne ograniczenia musiałyby także dotyczyć np. prawa do sprostowania danych (art. 16 RODO), czy prawa do sprzeciwu wobec przetwarzania danych z uwagi na szczególną sytuację (art. 21 ust.1 RODO), o ile podstawę przetwarzania danych stanowiłby prawnie uzasadniony interes administratora danych.

[11] https://techinfo.uodo.gov.pl/technologia-blockchain-a-dane-osobowe/ (dostęp: 24.10.2019)