

Czwartek, 8 października 2020 r.

P9_TA(2020)0265

Finanse cyfrowe: pojawiające się zagrożenia w zakresie kryptoaktywów – wyzwania regulacyjne i nadzorcze w obszarze usług, instytucji i rynków finansowych

Rezolucja Parlamentu Europejskiego z dnia 8 października 2020 r. zawierające zalecenia dla Komisji w sprawie finansów cyfrowych: pojawiające się zagrożenia w zakresie kryptoaktywów – wyzwania regulacyjne i nadzorcze w obszarze usług, instytucji i rynków finansowych (2020/2034(INL))

(2021/C 395/10)

Parlament Europejski,

- uwzględniając art. 225 Traktatu o funkcjonowaniu Unii Europejskiej,
- uwzględniając art. 7 i 8 Karty praw podstawowych Unii Europejskiej,
- uwzględniając 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) ⁽¹⁾,
- uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającą dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającą dyrektywę 2007/64/WE ⁽²⁾,
- uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniającą rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylającą dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE ⁽³⁾,
- uwzględniając komunikat Komisji z dnia 19 lutego 2020 r. zatytułowany „Europejska strategia w zakresie danych” (COM(2020)0066),
- uwzględniając komunikat Komisji z dnia 8 marca 2018 r. zatytułowany „Plan działania w zakresie technologii finansowej: w kierunku bardziej konkurencyjnego i innowacyjnego europejskiego sektora finansowego” (COM(2018)0109),
- uwzględniając wspólny komunikat Komisji i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 6 kwietnia 2016 r. zatytułowany „Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej” (JOIN(2016)0018),
- uwzględniając Białą księgę Komisji z dnia 19 lutego 2020 r. w sprawie sztucznej inteligencji – Europejskie podejście do doskonałości i zaufania (COM(2020)0065),
- uwzględniając odpowiedź z dnia 10 kwietnia 2017 r. udzieloną przez wiceprzewodniczącego Dombrovskisa w imieniu Komisji na pytanie E-001130/2017,
- uwzględniając sprawozdanie końcowe Dyrekcji Generalnej Komisji Europejskiej ds. Stabilności Finansowej, Usług Finansowych i Unii Rynków Kapitałowych z października 2019 r. zatytułowane „Governance for a DLT/Blockchain enabled European electronic Access Point (EEAP)” („Zarządzanie europejskim elektronicznym punktem dostępu opartym o technologię rozproszonego rejestru / łańcuch bloków”) ⁽⁴⁾,

⁽¹⁾ Dz.U. L 119 z 4.5.2016, s. 1.

⁽²⁾ Dz.U. L 337 z 23.12.2015, s. 35.

⁽³⁾ Dz.U. L 141 z 5.6.2015, s. 73.

⁽⁴⁾ <https://op.europa.eu/en/publication-detail/-/publication/98da7b74-38db-11ea-ba6e-01aa75ed71a1/language-en/format-PDF/source-113099411>

Czwartek, 8 października 2020 r.

- uwzględniając analizę Komisji Europejskiej na temat stosowania rozporządzenia w sprawie opłat interchange ⁽⁵⁾,
- uwzględniając konsultacje publiczne Komisji z dnia 17 lutego 2020 r. w sprawie przeglądu ram regulacyjnych dla firm inwestycyjnych i operatorów rynku,
- uwzględniając sprawozdanie końcowe Forum Wysokiego Szczebla do spraw Unii Rynków Kapitałowych Komisji Europejskiej z dnia 10 czerwca 2020 r. zatytułowane „A New Vision for Europe's Capital Markets” („Nowa wizja europejskich rynków kapitałowych”) ⁽⁶⁾,
- uwzględniając sprawozdanie końcowe grupy ekspertów Komisji ds. przeszkód regulacyjnych dla innowacji finansowych zatytułowane „30 recommendations on regulation, innovation and finance” („30 zaleceń dotyczących regulacji, innowacji i finansów”) z dnia 13 grudnia 2019 r.,
- uwzględniając wspólną poradę Europejskich Urzędów Nadzoru dla Komisji Europejskiej z dnia 10 kwietnia 2019 r. w sprawie potrzeby udoskonalenia przepisów dotyczących wymogów w zakresie zarządzania ryzykiem ICT w sektorze finansowym UE,
- uwzględniając wspólną poradę Europejskich Urzędów Nadzoru dla Komisji Europejskiej z dnia 10 kwietnia 2019 r. w sprawie kosztów i korzyści wynikających z opracowania spójnych ram dotyczących testów cyberodporności dla istotnych uczestników rynku i infrastruktur w całym sektorze finansowym UE,
- uwzględniając wspólne sprawozdanie Europejskich Urzędów Nadzoru z dnia 7 stycznia 2019 r. zatytułowane „FinTech: Regulatory sandboxes and innovation hubs” („Technologia finansowa – piaskownice regulacyjne i centra innowacji”) ⁽⁷⁾,
- uwzględniając wytyczne EUNB w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT z dnia 29 listopada 2019 r.,
- uwzględniając sprawozdanie Europejskiego Urzędu Nadzoru Bankowego z dnia 9 stycznia 2019 r. zawierające porady dla Komisji Europejskiej dotyczące kryptoaktywów,
- uwzględniając poradę Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych dla Komisji z dnia 9 stycznia 2019 r. dotyczącą pierwszych ofert kryptowalutowych i kryptoaktywów,
- uwzględniając dokument konsultacyjny Komisji Europejskiej z grudnia 2019 r. w sprawie unijnych ram dla rynków kryptoaktywów,
- uwzględniając swoją rezolucję ustawodawczą z dnia 27 marca 2019 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskich dostawców usług finansowania społecznościowego dla przedsiębiorstw ⁽⁸⁾,
- uwzględniając swoją rezolucję z dnia 3 października 2018 r. w sprawie technologii rozproszonego rejestru i łańcuchów bloków: budowanie zaufania do przepływów funduszy z pominięciem pośrednictwa bankowego ⁽⁹⁾,
- uwzględniając swoją rezolucję z dnia 17 maja 2017 r. w sprawie FinTech: wpływ technologii na przyszłość sektora finansowego ⁽¹⁰⁾,
- uwzględniając swoją rezolucję z dnia 16 lutego 2017 r. zawierającą zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki ⁽¹¹⁾,
- uwzględniając analizę z kwietnia 2020 r. sporządzoną na zlecenie Komisji Gospodarczej i Monetarnej Parlamentu Europejskiego, zatytułowaną „Crypto-assets: Key developments, regulatory concerns and responses” („Kryptoaktywa: ewolucja, problemy regulacyjne i rozwiązania”),

⁽⁵⁾ <https://ec.europa.eu/competition/publications/reports/kd0120161enn.pdf>

⁽⁶⁾ https://ec.europa.eu/info/files/200610-cmu-high-level-forum-final-report_en

⁽⁷⁾ JC 2018 74.

⁽⁸⁾ Teksty przyjęte, P8_TA(2019)0301.

⁽⁹⁾ Dz.U. C 11 z 13.1.2020, s. 7.

⁽¹⁰⁾ Dz.U. C 307 z 30.8.2018, s. 57.

⁽¹¹⁾ Dz.U. C 252 z 18.7.2018, s. 239.

Czwartek, 8 października 2020 r.

- uwzględniając analizę z lutego 2014 r. sporządzoną na zlecenie Komisji Rynku Wewnętrznego i Ochrony Konsumentów Parlamentu Europejskiego, zatytułowaną „Consumer Protection Aspects of Financial Services” („Usługi finansowe w aspekcie ochrony konsumenta”),
 - uwzględniając sprawozdanie Europejskiego Banku Centralnego z lipca 2019 r. dotyczące skutków cyfryzacji płatności detalicznych dla funkcji Eurosystemu jako katalizatora,
 - uwzględniając przemówienie programowe Benoîta Coeure’a z dnia 31 stycznia 2019 r. zatytułowane „FinTech for the People” („Technologia finansowa dla ludzi”),
 - uwzględniając przemówienie programowe Yves’a Merscha zatytułowane „Lending and payment systems in upheaval: the FinTech challenge” („Wstrząsy w systemach pożyczkowych i płatniczych: wyzwanie w dziedzinie technologii finansowej”), wygłoszone w dniu 26 lutego 2019 r. podczas 3. dorocznej Konferencji na temat technologii finansowych i innowacji cyfrowych,
 - uwzględniając sprawozdanie Rady Stabilności Finansowej z dnia 6 czerwca 2019 r. zatytułowane „Decentralized financial technologies: Report on financial stability, regulatory and governance implications” („Zdecentralizowane technologie finansowe. Sprawozdanie w sprawie skutków dla stabilności finansowej oraz w zakresie regulacji i zarządzania”),
 - uwzględniając sprawozdanie Rady Stabilności Finansowej z dnia 14 lutego 2019 r. zatytułowane „FinTech and market structure in financial services: Market developments and potential financial stability implications” („Technologia finansowa i struktura rynku w sektorze usług finansowych: Rozwój sytuacji rynkowej i potencjalne skutki dla stabilności finansowej”),
 - uwzględniając sprawozdanie Rady Stabilności Finansowej z dnia 16 lipca 2018 r. zatytułowane „Crypto-assets: Report to the G20 on work by the FSB and standard-setting bodies” („Kryptoaktywa: Sprawozdanie dla grupy G-20 w sprawie prac Rady Stabilności Finansowej i organów odpowiedzialnych za ustanawianie standardów”),
 - uwzględniając sprawozdanie Rady Stabilności Finansowej z dnia 27 czerwca 2017 r. zatytułowane „Financial Stability Implications from FinTech – Supervisory and Regulatory Issues that Merit Authorities’ Attention” („Skutki technologii finansowej dla stabilności finansowej – Kwestie regulacji i nadzoru, które zasługują na uwagę organów”),
 - uwzględniając dokument konsultacyjny Rady Stabilności Finansowej z dnia 14 kwietnia 2020 r. zatytułowany „Addressing the regulatory, supervisory and oversight challenges raised by »global stablecoin« arrangements” („Podejmowanie wyzwań regulacyjnych, nadzorczych i kontrolnych związanych z ustaleniami dotyczącymi globalnej stabilnej kryptowaluty”),
 - uwzględniając badanie grupy roboczej G-7 ds. stabilnych kryptowalut z października 2019 r. dotyczące wpływu globalnych stabilnych kryptowalut,
 - uwzględniając dokument Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy z czerwca 2019 r. zatytułowany „Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers” („Wytyczne w sprawie podejścia opartego na analizie ryzyka do wirtualnych aktywów i dostawców usług związanych z wirtualnymi aktywami”),
 - uwzględniając zalecenia Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy zaktualizowane w czerwcu 2019 r., a w szczególności zalecenie 16 w sprawie przekazów pieniężnych,
 - uwzględniając analizę Banku Rozrachunków Międzynarodowych ze stycznia 2020 r. zatytułowaną „Policy responses to FinTech: a cross-country overview” („Działania polityczne w odpowiedzi na technologie finansowe: przegląd sytuacji w poszczególnych krajach”),
 - uwzględniając wystąpienie Fernanda Restoya zatytułowane „Regulating FinTech: what is going on, and where are the challenges?” („Regulacja technologii finansowej – co się dzieje i na czym polegają wyzwania?”) z dnia 16 października 2019 r. w ramach XVI dialogu ASBA-BID-FELABAN w sprawie polityki regionalnej w publicznym i prywatnym sektorze bankowym,
 - uwzględniając art. 47 i 54 Regulaminu,
 - uwzględniając sprawozdanie Komisji Gospodarczej i Monetarnej (A9-0161/2020),
- A. mając na uwadze, że finanse cyfrowe są stale rozwijającym się obszarem sektora finansowego, zasługującym na stałe monitorowanie i uwzględnianie zarówno na poziomie branżowym, jak i regulacyjnym;

Czwartek, 8 października 2020 r.

- B. mając na uwadze, że rynek wewnętrzny Unii charakteryzuje się otwartą konkurencją i dąży do zapewnienia równych warunków działania za pomocą zharmonizowanych ram regulacyjnych, stosowania norm międzynarodowych, konwergencji praktyk nadzorczych oraz współpracy w zakresie nadzoru; mając na uwadze, że w związku z tym te same zasady powinny być podstawą unijnej strategii w zakresie finansów cyfrowych;
- C. mając na uwadze, że regulując działalność spółek z branży technologii finansowych, należy zagwarantować równowagę między sprzyjaniem innowacjom a zapewnieniem wysokiego poziomu ochrony inwestorów i stabilności finansowej;
- D. mając na uwadze, że termin „kryptoaktywa” stosuje się w odniesieniu do wielu różnych aktywów cyfrowych, między innymi walut wirtualnych i tokenów, ale czasami z wyłączeniem niektórych form stabilnych kryptowalut lub niektórych tokenów, takich jak tokeny inwestycyjne;
- E. mając na uwadze, że dwa najczęściej przyjmowane elementy składowe kryptoaktywów to: (i) prywatny charakter uprawnienia do bazowych aktywów, roszczeń lub praw oraz (ii) wykorzystanie kryptografii i technologii rozproszonego rejestru lub podobnych technologii jako podstawy wymiany aktywów oraz określania ich właściwej lub przypisywanej wartości;
- F. mając na uwadze, że obecnie kryptoaktywa nie są ani emitowane, ani gwarantowane przez żaden bank centralny czy organ sektora publicznego w Unii i że mogą one być wykorzystywane na różne sposoby, w tym jako środki wymiany, do celów inwestycyjnych i aby uzyskać dostęp do towaru lub usługi;
- G. mając na uwadze, że stabilne kryptowaluty wykazują cechy podobne do kryptoaktywów i nie przybierają postaci żadnej określonej waluty, lecz są oparte na zestawie narzędzi, których celem jest zminimalizowanie wahań ich ceny wyrażonej w danej walucie; mając na uwadze, że niektóre kryptoaktywa, w tym stabilne kryptowaluty i związane z nimi technologie, mogą zwiększyć wydajność, konkurencję i przejrzystość oraz stworzyć znaczące możliwości dla społeczeństwa i przynieść mu znaczące korzyści, jako że niektóre z nich mogą umożliwić tańsze i szybsze dokonywanie płatności oraz zapewniać nowe źródła finansowania dla małych i średnich przedsiębiorstw (MŚP); mając na uwadze, że ów zestaw narzędzi mających na celu zminimalizowanie wahań ceny nie został przetestowany w sytuacjach, w których przeprowadzana jest znaczna liczba transakcji opartych na stabilnych kryptowalutach;
- H. mając na uwadze, że debata publiczna na temat prywatnie uruchomionych stabilnych kryptowalut może być związana z pewnymi niedostatkami unijnego systemu płatności;
- I. mając na uwadze, że stabilne kryptowaluty mogą stać się powszechnie stosowanym środkiem płatniczym, co powinno spowodować podjęcie odpowiednich działań regulacyjnych i nadzorczych;
- J. mając na uwadze, że cyfrowa waluta banku centralnego (CBDC) opiera się na koncepcji stabilnego składnika aktywów i ma charakter suwerenny, a zatem odmienny od kryptowalut; mając na uwadze, że Bank Ludowy Chin testuje cyfrową walutę banku centralnego, system elektronicznej waluty cyfrowej (DCEP); mając na uwadze, że potencjalne globalne zastosowanie DCEP może mieć wpływ na handel międzynarodowy i ochronę konsumentów;
- K. mając na uwadze, że rozważane są ewentualne inicjatywy na rzecz wdrożenia CBDC, zarówno na szczeblu unijnym, jak i globalnym;
- L. mając na uwadze, że finanse cyfrowe mają silny element transgraniczny, który wykracza poza szczebel unijny, a zatem niezbędna jest międzynarodowa współpraca i wyznaczanie standardów oraz efektywny i skuteczny nadzór Unii w tej dziedzinie;
- M. mając na uwadze, że rozwój narzędzi finansów cyfrowych może się wiązać z silnymi przepływami kapitału, co przyciąga inwestycje transgraniczne; podkreśla, że w związku z tym finanse cyfrowe mogą przyczynić się do konkurencyjności Unii na rynkach światowych;
- N. mając na uwadze, że według danych rynkowych⁽¹²⁾ w czerwcu 2020 r. na całym świecie istniało ponad 5 600 kryptoaktywów o łącznej kapitalizacji rynkowej przekraczającej 260 mld USD⁽¹³⁾, z których 65 % stanowiły same bitcoiny;

⁽¹²⁾ <https://coinmarketcap.com>

⁽¹³⁾ [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU\(2020\)648779_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf)

Czwartek, 8 października 2020 r.

- O. mając na uwadze, że według danych rynkowych łączna kapitalizacja rynkowa stabilnych kryptowalut wzrosła z 1,5 mld EUR w styczniu 2018 r. do 10 mld EUR w czerwcu 2020 r. i że pomimo nadal ograniczonego zasięgu w porównaniu z innymi kryptowalutami mogą one szybko osiągnąć skalę globalną i zyskać masową bazę użytkowników, zwłaszcza jeśli zostaną przyjęte przez giganty technologiczne wykorzystujące ich sieci;
- P. mając na uwadze, że eksperci Europejskiego Banku Centralnego (EBC) zauważyli w publikacji z 2019 r. ⁽¹⁴⁾, że chociaż kryptoaktywa mają charakter wysoce spekulacyjny, nie stanowią one bezpośredniego zagrożenia dla stabilności finansowej; mając na uwadze, że pogląd ten podzielają zarówno Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA) ⁽¹⁵⁾, jak i Europejski Urząd Nadzoru Bankowego (EUNB) ⁽¹⁶⁾; mając na uwadze, że takie same wnioski przedstawił Międzynarodowy Fundusz Walutowy (MFW) w swoim sprawozdaniu w sprawie światowej stabilności finansowej z 2018 r. oraz Rada Stabilności Finansowej w sprawozdaniu z lipca 2018 r., lecz jest ona zdania, że należy kontynuować analizę z uwagi na szybkie tempo rozwoju rynków;
- Q. mając na uwadze, że, jak wskazano w sprawozdaniu EUNB, obecne zaangażowanie instytucji finansowych w działania związane z kryptoaktywami jest stosunkowo ograniczone, ale zainteresowanie nimi prawdopodobnie wzrosło, w szczególności w związku z coraz częstszym wykorzystaniem rozwiązań opartych na technologii rozproszonego rejestru; mając na uwadze, że działania takie obejmują posiadanie lub pozyskiwanie udziałów w kryptoaktywach, subemisję pierwszych ofert kryptowalutowych czy świadczenie usług związanych z kryptoaktywami, takich jak prowadzenie kont waluty wirtualnej czy świadczenie usług wymiany; mając na uwadze, że obecne wymogi ostrożnościowe nie są odpowiednio dostosowane do wysokiej niestabilności i wysokiego ryzyka kryptoaktywów;
- R. mając na uwadze, że ostatnie badania sugerują, iż kryptoaktywa są głównie wykorzystywane jako inwestycje spekulacyjne, a nie jako sposób płatności za towary lub usługi oferowane przez legalnie działające punkty usługowo-handlowe; mając na uwadze, że Europejskie Urzędy Nadzoru podkreślały, iż kryptoaktywa, które nie mogą zostać uznane za instrumenty finansowe w rozumieniu unijnych regulacji finansowych, są obciążone szczególnym ryzykiem, zwłaszcza w odniesieniu do ochrony inwestorów i konsumentów oraz integralności rynku; mając na uwadze wysoki stopień ryzyka związanego z kryptoaktywami, jeśli chodzi o wykorzystywanie ich do celów prania pieniędzy, oszustw, unikania opodatkowania i ataków z zewnątrz;
- S. mając na uwadze, że zastosowanie nowych technologii może znacząco wspomóc przedsiębiorstwa świadczące usługi finansowe w wywiązywaniu się z bieżących zobowiązań w zakresie nadzoru i zgodności z przepisami;
- T. mając na uwadze, że klasyfikacja tych kryptoaktywów, które na mocy prawa unijnego kwalifikują się jako instrumenty finansowe, zależy od właściwych organów krajowych wdrażających prawo unijne w danym państwie, co powoduje rozbieżności w podejściu nadzorczym i regulacyjnym oraz zagraża spójności i równości warunków działania w Unii; mając na uwadze, że dokonanie takiej klasyfikacji i włączenie do unijnych ram legislacyjnych nie jest pozbawione trudności, gdyż kryptoaktywa odznaczają się różnymi cechami, które mogą się zmieniać z upływem czasu;
- U. mając na uwadze, że pierwsze oferty kryptowalutowe mogą stanowić alternatywne źródło finansowania dla innowacyjnych przedsiębiorstw i przedsiębiorstw typu start-up na wczesnych etapach ich rozwoju, ale jednocześnie narażają one inwestorów na wysokie ryzyko strat ze względu na ich wysoce spekulacyjny charakter i podatność na nadużycia finansowe; mając na uwadze, że według rocznego sprawozdania gospodarczego Banku Rozrachunków Międzynarodowych z 2018 r. co najmniej 22,5 % pierwszych ofert kryptowalutowych okazało się być nieuczciwymi piramidami finansowymi;
- V. mając na uwadze, że kryptoaktywa mogą w bezpieczny sposób zmniejszyć koszty transakcji w coraz bardziej cyfrowo nadzorowanym świecie, jeśli zostaną poddane rygorystycznemu systemowi regulacyjnemu, odpowiedniemu do zamierzonego celu i opartemu na analizie ryzyka;
- W. mając na uwadze, że finanse cyfrowe mogą na wiele sposobów przyczynić się do zaradzenia skutkom gospodarczym wybuchu epidemii COVID-19, jeżeli chodzi o konsekwencje dla obywateli, MŚP i innych przedsiębiorstw oraz usług finansowych; mając na uwadze, że epidemia COVID-19 pokazuje – w różnym stopniu w różnych państwach członkowskich – potencjał finansów cyfrowych zarówno dla konsumentów, jak i dla gospodarki;

⁽¹⁴⁾ https://www.ecb.europa.eu/pub/economic-bulletin/articles/2019/html/ecb.ebart201905_03~c83aeaa44c.en.html#toc4

⁽¹⁵⁾ ESMA Advice – Initial Coin Offerings and Crypto-Assets (Porady ESMA – pierwsze oferty kryptowalutowe i kryptoaktywa) (https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf).

⁽¹⁶⁾ Sprawozdanie EUNB zawierające porady dla Komisji Europejskiej dotyczące kryptoaktywów (<https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf>).

Czwartek, 8 października 2020 r.

- X. mając na uwadze, że duże firmy technologiczne i światowe platformy cyfrowe coraz częściej oferują usługi finansowe; mając na uwadze, że te duże podmioty w sektorze cyfrowym posiadają przewagę konkurencyjną m.in. dlatego, że mogą korzystać z efektu skali, rozległych transgranicznych sieci użytkowników, łatwego dostępu do finansowania i możliwości zbierania danych udostępnianych przez użytkowników za pomocą technologii przetwarzania danych, takich jak analityka na podstawie dużych zbiorów danych, które to korzyści generują na różne sposoby ogromną wartość dodaną; mając na uwadze, że obecność gigantów technologicznych na rynkach technologii finansowych może potencjalnie zaszkodzić uczciwej konkurencji i innowacyjności;
- Y. mając na uwadze, że niedawno odkryte oszustwa związane z przedsiębiorstwami z branży technologii finansowych podkreślają potrzebę holistycznego spojrzenia na zagrożenia dla ochrony konsumentów i inwestorów związane z nieprawidłowościami w procedurach dotyczących sprawozdawczości finansowej, nadużyć finansowych i niewypłacalności;
- Z. mając na uwadze, że w ostatnich latach udział płatności bezgotówkowych znacząco wzrósł; mając na uwadze, że ulepszenie systemu transakcji bezgotówkowych nie powinno ograniczać możliwości korzystania z gotówki jako środka płatniczego;
- AA. mając na uwadze, że sektor finansowy jest największym na świecie użytkownikiem technologii informacyjno-komunikacyjnych (ICT), odpowiadającym za mniej więcej jedną piątą wszystkich wydatków w dziedzinie ICT;
- AB. mając na uwadze, że stosowanie nowych technologii w sektorze finansowym może wiązać się z nowymi zagrożeniami, które należy uregulować oraz monitorować w celu zagwarantowania stabilności finansowej, integralności rynku wewnętrznego i ochrony konsumentów;
- AC. mając na uwadze, że zwiększone wykorzystywanie sztucznej inteligencji w usługach finansowych doprowadzi do konieczności wzmocnienia odporności operacyjnej, odpowiedniego nadzoru i odpowiedniej ochrony danych zgodnie z prawem Unii;
- AD. mając na uwadze, że nowe problemy operacyjne, w szczególności ryzyko związane z technologiami i bezpieczeństwem ICT, mogą stwarzać ryzyko systemowe dla sektora finansowego; takiemu nowemu ryzyku należy przeciwdziałać za pomocą odpowiednich środków, na co zwróciła uwagę Europejska Rada ds. Ryzyka Systemowego ⁽¹⁷⁾;
- AE. mając na uwadze, że w obecnym zbiorze przepisów UE dotyczących usług finansowych przyjmuje się fragmentaryczne podejście do kwestii przepisów odnoszących się do ryzyka operacyjnego;
- AF. mając na uwadze, że ryzyko związane z technologiami i bezpieczeństwem ICT, na które narażony jest sektor finansowy, oraz poziom integracji tego sektora na poziomie Unii uzasadniają podjęcie konkretnych i bardziej zaawansowanych działań, które opierają się na dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii ⁽¹⁸⁾, ale wykraczają poza tę dyrektywę;
- AG. mając na uwadze, że cyberodporność stanowi integralną część prac nad odpornością operacyjną instytucji finansowych prowadzonych przez organy na szczeblu światowym;
- AH. mając na uwadze, że prawidłowo funkcjonujący, zrównoważony i odporny rynek finansowy Unii powinien charakteryzować się wysoką efektywnością alokacji kapitału i ryzyka oraz jak najszerzym włączeniem społecznym obywateli pod względem dostępu do usług finansowych;
- AI. mając na uwadze, że usługi przetwarzania w chmurze mogą zapewnić dostawcom usług finansowych znaczące korzyści odnośnie do odporności operacyjnej i efektywności w porównaniu z tradycyjnymi rozwiązaniami na miejscu, ale wiążą się z dodatkowymi wyzwaniem dotyczącymi bezpieczeństwa danych i procesów, ciągłości działania w przypadku wyłączeń i ogólnie większego zagrożenia cyberprzestępstwami;

⁽¹⁷⁾ <https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200107~29129d5701.en.html>

⁽¹⁸⁾ Dz.U. L 194 z 19.7.2016, s. 1.

Czwartek, 8 października 2020 r.

- AJ. mając na uwadze, że konieczne są równe warunki działania dla firm świadczących usługi finansowe i firm technologicznych, aby zapewnić, by wszystkie firmy konkurowały ze sobą na równych prawach, zgodnie z zasadą „to samo ryzyko, ta sama działalność, te same przepisy”;
- AK. mając na uwadze, że wprowadzenie cyfrowych usług finansowych nie powinno prowadzić ani do arbitrażu regulacyjnego, ani do osłabienia ochrony konsumentów, ograniczenia bezpieczeństwa czy zagrożenia stabilności finansowej;
- AL. mając na uwadze, że wiele dużych instytucji finansowych Unii korzysta z usług przetwarzania w chmurze świadczonych przez dostawców z państw trzecich;
- AM. mając na uwadze, że Europejska Rada Ochrony Danych ma do odegrania ważną rolę polegającą na pomaganiu przedsiębiorstwom w zrozumieniu, jakie są ich zobowiązania dotyczące przestrzegania przepisów RODO;
- AN. mając na uwadze, że twórcy kryptowalut zwykle nie są znani i że kryptowaluty nie stwarzają roszczenia finansowego do aktywów bazowych w przeciwieństwie do stabilnych kryptowalut, tokenów inwestycyjnych i towarowych, których twórcy są zawsze znani;
- AO. mając na uwadze, że chociaż tokeny emitowane przez przedsiębiorców w formie roszczeń do przepływów pieniężnych, należności kapitałowej czy roszczenia do przyszłego towaru lub przyszłej usługi mogą zostać sklasyfikowane na różne sposoby, ich klasyfikacja w prawie Unii powinna zapewniać przewidywalność regulacyjną i jednorodność na rynkach europejskich; mając na uwadze, że odpowiednie technologicznie i funkcjonalne przepisy dotyczące tokenów powinny uwzględniać potencjalne modele hybrydowe i zawierać definicje maksymalizujące ochronę konsumentów i inwestorów, zwiększające pewność prawa i wykorzystujące silny potencjał tych instrumentów do finansowania ryzykownych przedsięwzięć; mając na uwadze, że bazowa funkcja ekonomiczna tokenów jest istotnym wskaźnikiem, jak należy je sklasyfikować;
- AP. mając na uwadze, że Grupa Specjalna ds. Przeciwdziałania Praniu Pieniądzy (FATF) przyjęła szeroką definicję waluty wirtualnej i zaleciła nałożenie zobowiązań w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu na wszystkie osoby fizyczne i prawne podejmujące działania związane z wymianą kryptoaktywów, transferem kryptoaktywów i korzystaniem z usług finansowych związanych z pierwszą ofertą krypto walutową oraz świadczeniem takich usług;
- AQ. mając na uwadze, że pranie pieniędzy stanowi ogromne zagrożenie, któremu należy zapobiegać w obszarze finansów cyfrowych; mając na uwadze, że choć finanse cyfrowe mogą przyczynić się do poprawy włączenia społecznego pod względem finansowym, nadal powinien istnieć kompleksowy system oparty na zasadzie „znaj swojego klienta” i przeciwdziałający praniu pieniędzy, zgodnie z prawem Unii; mając na uwadze, że choć kryptowaluty mogą być wykorzystywane do nielegalnej działalności, uregulowanie ich jako środka płatniczego, a nie środka wymiany, może poprawić monitorowanie i zapobieganie przestępczości finansowej;
- AR. mając na uwadze, że zwiększona łączność, internet rzeczy i interakcja ludzi z maszynami mogą ulepszyć korzystanie z usług finansowych, ale również pociągają za sobą nowe ryzyko dotyczące prywatności i ochrony danych osobowych, jakości interakcji, zarządzania ryzykiem operacyjnym i wyzwania związane z cyberbezpieczeństwem;

Zalecenia:**Uwagi ogólne**

1. z zadowoleniem przyjmuje przyjęcie przez Komisję pakietu dotyczącego finansów cyfrowych obejmującego dwa wnioski ustawodawcze w sprawie kryptoaktywów i odporności operacyjnej; uważa, że wniosek Komisji dotyczący kryptoaktywów oraz wniosek dotyczący odporności operacyjnej i cyberodporności zostały przedstawione w odpowiednim momencie i że są one przydatne i konieczne ze względu na ostatnie wydarzenia na rynku unijnym i rynkach światowych, a także stanowią istotny krok w kierunku zapewnienia jasności prawa i opracowania nowego systemu regulacyjnego; ubolewa jednak, że Komisja nie zajęła się we właściwy sposób problemami związanymi z praniem pieniędzy, finansowaniem terroryzmu i działalnością przestępczą związaną z kryptoaktywami, które to problemy w dużej mierze pozostają nierozwiązane; zwraca się do Komisji o podjęcie pilnych działań w tych obszarach zgodnie z zaleceniami przedstawionymi w załączniku do niniejszego projektu rezolucji;

Czwartek, 8 października 2020 r.

2. uważa, że finansowanie cyfrowe, które odgrywa bardzo istotną rolę w rozwijaniu działalności finansowej, będzie jednym z kluczy do sukcesu unii rynków kapitałowych dzięki zwiększeniu możliwości finansowania dla przedsiębiorstw i obywateli oraz możliwości inwestycyjnych, i zachęca Komisję do zastanowienia się nad tym, w jaki sposób wzmocnić pozycję innowatorów, a tym samym wykorzystać możliwości finansowania cyfrowego do wspierania integracji rynków kapitałowych i udziału inwestorów detalicznych w Unii oraz do zwiększenia jego skali na świecie;
3. podkreśla większą wagę środków monitorowania i przeglądu przepisów dotyczących finansów cyfrowych, w szczególności mając na względzie rosnące znaczenie tego sektora w czasie, gdy świat zmaga się z pandemią COVID-19; podkreśla ponadto potrzebę zajęcia się konkretnymi zagrożeniami, jakie niosą ze sobą finanse cyfrowe na poziomie regulacyjnym i nadzorczym, za pomocą odpowiednich ram prawnych i przepisów dotyczących ochrony konsumentów;
4. podkreśla, że ważne jest, by ze względu na transgraniczny charakter finansów cyfrowych Komisja ściśle współpracowała z międzynarodowymi forami i organami regulacyjnymi w celu opracowania norm międzynarodowych, bez uszczerbku dla prawa Unii do przyjęcia przepisów regulacyjnych i nadzorczych dostosowanych do okoliczności panujących w Unii; przypomina w szczególności o potrzebie zapewnienia interoperacyjności unijnych ram regulacyjnych z zasadami uzgodnionymi na szczeblu międzynarodowym;
5. zwraca uwagę, że rozwój wielu technologii związanych z finansami cyfrowymi wciąż znajduje się w stadium początkowym; podkreśla, że w związku z tym wszelkie nowe środki ustawodawcze muszą podlegać dogłębnej i przyszłościowej ocenie ryzyka i korzyści dla konsumentów i stabilności finansowej; wzywa Komisję do zastosowania proporcjonalnego, opartego na analizie ryzyka, zorientowanego na wyniki, międzysektorowego i całościowego podejścia do prac nad finansami cyfrowymi;
6. wzywa Komisję, by wykorzystała wiedzę i doświadczenie zdobyte w ramach europejskiego forum koordynatorów innowacji i jako pierwsza podjęła działania w celu stworzenia korzystnego i zrównoważonego środowiska dla europejskich centrów i przedsiębiorstw z branży technologii finansowych, a także dla tradycyjnego sektora finansowego korzystającego z finansowania cyfrowego, w celu zwiększenia skali, przyciągnięcia inwestycji zagranicznych i zwiększenia obecności Unii na rynkach światowych;
7. uważa w związku z tym, że finanse cyfrowe powinny być uznane za niezbędne i skuteczne narzędzie dla europejskich MŚP, mogące zapewnić działające w czasie rzeczywistym szybkie rozwiązania dopasowane do ich potrzeb w zakresie finansowania; jest zdania, że finanse cyfrowe mogą wypełnić lukę w finansowaniu MŚP;
8. podkreśla, że wszystkie środki przyjmowane na szczeblu Unii powinny gwarantować, by uczestnicy rynku, od małych do dużych, mieli przestrzeń regulacyjną do innowacji i że wszystkie nowe lub aktualizowane regulacje oraz nadzór w obszarze technologii finansowej powinny opierać się na następujących zasadach:
 - a) te same działania i te same usługi oraz powiązane z nimi podobne ryzyko powinny podlegać tym samym przepisom;
 - b) proporcjonalność i neutralność technologiczna;
 - c) podejście oparte na ryzyku, przejrzystości i rozliczalności;
 - d) przestrzeganie praw podstawowych, zwłaszcza prawa do prywatności i ochrony danych osobowych, zagwarantowanego w art. 7 i 8 Karty praw podstawowych Unii Europejskiej;
 - e) wysokie standardy ochrony konsumentów i inwestorów;
 - f) równe warunki działania;
 - g) podejście przyjazne dla innowacji;
9. zwraca uwagę, że wszystkie nowe lub aktualizowane środki przyjmowane na szczeblu Unii powinny uwzględniać dynamiczne zmiany na rozwijających się rynkach kryptoaktywów i pierwszych ofert kryptowalutowych; podkreśla, że należy zapewnić równe warunki działania na całym rynku wewnętrznym, które pozwolą uniknąć wykorzystywania różnic w systemach prawnych i arbitrażu regulacyjnego; ostrzega, że takie środki nie powinny ograniczać możliwości rozwoju przedsiębiorstw, zwłaszcza MŚP, i powinny oferować zrównoważony ekosystem dla rozwoju finansów cyfrowych na rynku wewnętrznym, przy jednoczesnym zapewnieniu stabilności finansowej, integralności rynku oraz ochrony inwestorów i konsumentów;

Czwartek, 8 października 2020 r.

10. zwraca uwagę, że piaskownice regulacyjne i centra innowacji mają potencjał, aby być dla przedsiębiorstw z branży finansów cyfrowych przydatnym narzędziem do testowania innowacyjnych produktów i usług finansowych oraz modeli biznesowych w kontrolowanym środowisku, a także pozwolić właściwym organom lepiej zrozumieć taką działalność i uzyskać ekspercką wiedzę w zakresie regulacji innowacyjnych technologii, a tym samym ułatwić dialog między przedsiębiorstwami i regulatorami; podkreśla jednak, że mogą one również stanowić poważne zagrożenie dla ochrony konsumentów i inwestorów oraz umożliwiać oszustwa finansowe, stwarzając jednocześnie ryzyko fragmentacji nadzoru i arbitrażu regulacyjnego;

11. podkreśla, że wszelkie „piaskownice”, w tym paneuropejskie, powinny dążyć do równowagi między wspieraniem innowacyjności i stabilności finansowej a ochroną inwestorów i konsumentów, przy jednoczesnym uwzględnieniu wielkości, znaczenia systemowego i działalności transgranicznej zainteresowanych przedsiębiorstw; wzywa Komisję do ustanowienia wspólnych unijnych ram dla paneuropejskiej piaskownicy cyfrowych usług finansowych, ponieważ przyniosłoby to dodatkowe korzyści dla innowacji finansowych i stabilności finansowej oraz ograniczyłoby rozdrobnienie nadzoru;

12. podkreśla znaczenie trójkąta, tworzonego przez zaufanie, weryfikację tożsamości i dane, dla zapewnienia, aby uczestnicy rynku, inwestorzy, konsumenci i organy nadzorcze mogli mieć zaufanie do finansów cyfrowych;

13. uważa, że należałoby dogłębniej zbadać inicjatywy na rzecz wdrożenia cyfrowych walut banku centralnego, zarówno w Unii, jak i na szczeblu ogólnosięciowym; zachęca EBC, aby rozważył przeprowadzenie kompleksowej oceny skutków w celu przedstawienia możliwości rozwoju cyfrowych walut banku centralnego, w tym analizy szans i zagrożeń związanych z ustanowieniem cyfrowego euro; uważa, że ocena ta powinna również uwzględniać rolę zastosowanych technologii; ponadto wzywa unijne organy nadzorcze do promowania dalszych badań w tej dziedzinie oraz wzywa Komisję i EBC do zaangażowania się w dialog na szczeblu międzynarodowym w celu oceny potencjalnych korzyści i skutków szerszego stosowania cyfrowych walut banku centralnego na całym świecie;

14. jest zdania, że przy określaniu parametrów i zasad stosowanych w ocenie skutków i dalszej analizie należy wziąć pod uwagę rolę cyfrowych walut banku centralnego, jeżeli chodzi o rekompensowanie coraz rzadszego korzystania z gotówki, zapewnienie zaufania do systemu finansowego, umożliwienie większego włączenia społecznego pod względem finansowym i dostępu do publicznego środka płatniczego, przy jednoczesnym zagwarantowaniu stabilności finansowej i pieniężnej;

15. podkreśla potrzebę większej zbieżności przepisów i praktyk nadzorczych w celu opracowania wspólnych ram unijnych; podkreśla kluczową rolę Europejskich Urzędów Nadzoru w ułatwianiu realizacji tego celu; apeluje o zorganizowany dialog między Europejskimi Urzędami Nadzoru a właściwymi organami krajowymi, który powinien koncentrować się na obecnych wyzwaniach nadzorczych i konwergencji praktyk w celu zapewnienia sprawnego nadzoru na wszystkich szczeblach, zwłaszcza w odniesieniu do finansów cyfrowych, przeciwdziałania praniu pieniędzy, ochrony prywatności i ochrony danych oraz wyzwań i możliwości w zakresie cyberbezpieczeństwa; uważa, że ten zorganizowany dialog powinien koncentrować się, w dziedzinie finansów cyfrowych, na ograniczeniu arbitrażu i konkurencji nadzorczej oraz na innych istniejących przeszkodach dla operacji transgranicznych;

16. proponuje wyznaczenia jednolitego europejskiego organu nadzoru, który ściśle współpracowałby z innymi Europejskimi Urzędami Nadzoru i właściwymi organami krajowymi, w oparciu o wspólny zbiór przepisów i uprawnienia w zakresie interwencji produktowej w celu sprawowania nadzoru w odniesieniu do następujących obszarów działalności związanej z kryptoaktywami: podmiotów zajmujących się świadczeniem usług wymiany walut pomiędzy walutami wirtualnymi a walutami fiducjarnymi, a także dostawców kont waluty wirtualnej i wszystkich innych dostawców usług w zakresie aktywów wirtualnych objętych standardami FATF; jednocześnie zauważa, że należy zapewnić rozliczalność tego europejskiego organu nadzoru oraz zapewnić kontrolę sądową działań europejskiego organu nadzoru; odnotowuje w związku z tym wniosek Komisji z 24 września 2020 r. dotyczący rozporządzenia w sprawie rynków kryptoaktywów; podkreśla, że jednolity organ nadzoru, we współpracy z innymi właściwymi organami nadzoru na szczeblu Unii, powinien sprawować nadzór nad działalnością związaną z kryptoaktywami o istotnym wymiarze transgranicznym w Unii, oraz powinien opracować odpowiednie struktury wewnętrzne, aby zapewnić na szczeblu Unii sprawny i skuteczny nadzór nad kryptoaktywami;

17. zgadza się ze stanowiskiem EBC co do znaczenia pieniądza fizycznego jako legalnego środka płatniczego; podkreśla, że postępy w dziedzinie walut wirtualnych i płatności cyfrowych nie mogą prowadzić do ograniczeń dotyczących detalicznych płatności gotówkowych ani do likwidacji gotówki;

Czwartek, 8 października 2020 r.

18. podkreśla swoje obawy co do oddziaływania wydobywania kryptowalut na środowisko; podkreśla potrzebę rozwiązań mających na celu ograniczenie śladu ekologicznego popularnych kryptoaktywów; wzywa Komisję, by wzięła ten fakt pod uwagę w nadchodzących inicjatywach regulacyjnych, pamiętając o zaangażowaniu UE w osiągnięcie celów zrównoważonego rozwoju i niezbędne przejście na neutralność klimatyczną społeczeństwa najpóźniej do 2050 r.;

Określenie ram dla kryptoaktywów

19. uważa, że opracowanie kompleksowej ogólnoeuropejskiej taksonomii nowych produktów takich jak kryptoaktywa jest niezbędnym krokiem w kierunku promowania wspólnego rozumienia, ułatwiania współpracy między jurysdykcjami i zapewniania większej pewności prawnej uczestnikom rynku prowadzącym działalność transgraniczną; zaleca uwzględnienie istniejących krajowych ram regulacyjnych i nadzorczych; odnotowuje znaczenie współpracy międzynarodowej i inicjatyw globalnych w odniesieniu do unijnych ram dla kryptoaktywów, mając na uwadze w szczególności ich wolny od granic charakter;

20. uważa, że bardziej odpowiednie może być opracowanie otwartego wzorca taksonomii na szczeblu unijnym, przy uwzględnieniu, że jest to rozwijający się segment rynku, a taka taksonomia powinna służyć za podstawę odpowiednich działań ustawodawczych lub regulacyjnych; uważa jednak, że nie ma uniwersalnego rozwiązania, jeśli chodzi o kwalifikację prawną kryptoaktywów, dlatego też ważne jest, by ramy pozwalały organom nadzorczym na monitorowanie i dostosowywanie;

21. podkreśla, że przedsiębiorstwa typu start-up często tworzą innowacyjne usługi finansowe z korzyścią dla obywateli i przedsiębiorstw Unii i że wszelkie ramy prawne powinny być opracowywane z myślą o umożliwieniu dalszych innowacji i wyboru konsumentom w zakresie usług finansowych;

22. zauważa, że przy braku wspólnego unijnego podejścia regulacyjnego do kryptoaktywów państwa członkowskie już zaczęły podejmować jednostronne działania ustawodawcze i nadzorcze i że ze względu na niepokój o ochronę konsumentów państwa członkowskie podlegają coraz większej presji, by działać; zwraca uwagę, że rozbieżne interpretacje i nieskoordynowane podejście państw członkowskich mogą doprowadzić do fragmentacji rynku, zwiększyć brak pewności prawa, utrudniać równe warunki działania i stworzyć możliwości arbitrażu regulacyjnego;

23. uważa zatem, że wszelka dalsza kategoryzacja powinna być zrównoważona i elastyczna w celu dostosowywania się do zmieniających się modeli biznesowych i rodzajów ryzyka oraz zapewnienia przestrzeni dla innowacji i konkurencyjności w sektorze, przy jednoczesnym zadbanie o rozpoznawanie i ograniczanie ryzyka na wczesnym etapie;

24. podkreśla ponadto, że konieczne jest wyjaśnienie wytycznych dotyczących obowiązujących procesów regulacyjnych i ostrożnościowych w celu zapewnienia pewności regulacyjnej i nakreślenia odpowiedniego nadzoru i ostrożnościowego traktowania kryptoaktywów; zgadza się z opinią komitetu bazylejskiego i EUNB, że banki nabywające kryptoaktywa powinny stosować konserwatywno-ostrożnościowe podejście do kryptoaktywów, zwłaszcza tych wysokiego ryzyka;

25. uważa, że regulowane instytucje finansowe, w szczególności instytucje kredytowe, instytucje płatnicze i fundusze emerytalne, podlegają określonym maksymalnym limitom ekspozycji w świetle potencjalnych zagrożeń dla ochrony konsumentów i inwestorów oraz dla stabilności finansowej związanej z wysokim poziomem działalności kryptoaktywów; zgadza się również z opinią, że niezwykle ważne są: rzeczywiście należyta staranność, solidna administracja i solidne zarządzanie ryzykiem, pełne ujawnianie wszelkiej ekspozycji na ryzyko i trwały dialog z organami nadzorczymi; jest zdania, że nadchodzący przegląd ramowych zasad wymogów kapitałowych powinien uwzględnić poprawki w tym względzie;

26. uważa, że wszyscy pośrednicy i uczestnicy biorący udział w działalności związanej z kryptoaktywami powinni podlegać normom obowiązujących finansowych ram regulacyjnych, w zależności od przypadku; podkreśla ponadto potrzebę ustanowienia przepisów i mechanizmów zapewniających, aby normy regulacyjne dotyczące działań związanych z kryptoaktywami, w szczególności w odniesieniu do ochrony konsumentów i przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, były również egzekwowane, gdy taka działalność jest prowadzona lub takie usługi są świadczone poza Unią; podkreśla ponadto potrzebę wprowadzenia szczegółowych przepisów dotyczących przejrzystości i integralności rynku, które byłyby co najmniej równoważne przepisom dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniającej dyrektywę 2002/92/WE i dyrektywę 2011/61/UE⁽¹⁹⁾ (MiFID II) w odniesieniu do wszystkich emitentów lub sponsorów kryptoaktywów, ustanawiających rygorystyczne zasady dotyczące informacji dla potencjalnych klientów, które to informacje powinny być jasne i nie powinny wprowadzać w błąd, a także wymogi oceny odpowiedności;

⁽¹⁹⁾ Dz.U. L 173 z 12.6.2014, s. 349.

Czwartek, 8 października 2020 r.

27. uważa, że niektóre kryptoaktywa, wykorzystywane głównie w nielegalnych kanałach, nie powinny być legitymizowane poprzez objęcie ich istniejącym systemem regulacyjnym; podkreśla, że wszelka niepożądana legitymizacja stanowiłaby zagrożenie dla ochrony konsumentów i podważałaby integralność rynku; w związku z tym wzywa Komisję do ustanowienia surowych przepisów dotyczących ostrzeżeń dla potencjalnych klientów oraz do zagwarantowania, że właściwym organom zostaną przyznane niezbędne uprawnienia interwencyjne w celu ograniczenia lub zakazania operacji i działań w odniesieniu do tych kryptoaktywów, które są w przeważającej mierze wykorzystywane do celów niezgodnych z prawem;
28. podkreśla, że po udostępnieniu taksonomii ryzyko związane z udziałami w kryptoaktywach i ekspozycją na kryptoaktywa powinno zostać całkowicie uwzględnione w procesie przeglądu i oceny nadzorczej; zwraca w tym kontekście uwagę, że potrzebne są odpowiednie i znormalizowane wymogi ujawniania informacji dotyczących wszelkiej znaczącej ekspozycji lub wszelkich istotnych usług w związku z kryptoaktywami;
29. zwraca uwagę, że konieczne będzie zlikwidowanie luk prawnych w obowiązującym prawie Unii poprzez ukierunkowane zmiany, a także utworzenie specjalnych systemów regulacyjnych w odniesieniu do nowych i rozwijających się działań związanych z kryptoaktywami, takich jak pierwsze oferty kryptowalutowe lub pierwsze oferty kryptogieldowe; zauważa, że niektóre rodzaje kryptoaktywów mogą wpisać się w istniejące ramy regulacyjne, np. jako „zbywalne papiery wartościowe” zgodnie z definicją zawartą w MiFID II; uważa, że te kryptoaktywa, które mogłyby wejść w zakres MiFID II, powinny być traktowane w taki sam sposób jak inne zbywalne papiery wartościowe objęte tym systemem i jako takie nie wymagałyby dostosowanych ram prawnych, lecz raczej ukierunkowanych zmian w odpowiednich przepisach MiFID II;
30. podkreśla konieczność uregulowania na szczeblu unijnym w sposób zharmonizowany niektórych kryptoaktywów, które nie byłyby objęte zakresem MiFID II;
31. zauważa, że stabilne kryptowaluty stanowią unikalną kategorię kryptoaktywów; zwraca uwagę, że do tej pory korzystanie ze stabilnych kryptowalut nie rozpowszechniło się jeszcze w Unii; podkreśla jednak, że ich powszechne użycie może stanowić poważne zagrożenie dla stabilności finansowej i transmisji polityki pieniężnej, a także dla kontroli demokratycznej; w związku z tym z zadowoleniem przyjmuje przyjęcie przez Komisję ram prawnych, które mają zapewnić m.in. stabilny kurs wymiany między stabilnymi kryptowalutami a walutami fiducjarnymi oraz możliwość dokonywania w dowolnym momencie ponownej konwersji odnośnych stabilnych kryptowalut na waluty fiducjarne według wartości nominalnej; podkreśla jednak, że wszyscy emitenci stabilnych kryptowalut muszą być prawnie zobowiązani do przyznania posiadaczowi bezpośredniego roszczenia oraz do wymiany stabilnych kryptowalut według wartości nominalnej na walutę fiducjarną w dowolnym momencie, a także do wprowadzenia w tym celu odpowiednich mechanizmów służących zabezpieczeniu i segregacji rezerw stabilizacyjnych;
32. podkreśla, że pierwsze oferty kryptowalutowe i pierwsze oferty kryptogieldowe mają potencjał, by zwiększyć dostęp do finansowania dla MŚP, innowacyjnych przedsiębiorstw typu start-up i scale-up, mogą przyspieszyć transfer technologii i mogą stanowić istotną część unii rynków kapitałowych; zauważa jednak, że różne organy nadzoru wydały ostrzeżenia dotyczące pierwszych ofert kryptowalutowych ze względu na brak przejrzystości i wymogów w zakresie ujawniania informacji, które mogą powodować ryzyko dla inwestorów i konsumentów;
33. w związku z tym wzywa Komisję, by oceniła korzyści zaproponowania ram ustawodawczych dla pierwszych ofert kryptowalutowych i pierwszych ofert kryptogieldowych w celu zwiększenia przejrzystości, pewności prawa, ochrony inwestorów i konsumentów i ograniczenia ryzyka płynącego z jednostronnych informacji, nieuczciwych praktyk i nielegalnej działalności; nalega, by nadzór nad tymi ramami i ich monitorowanie były koordynowane na szczeblu Unii;
34. podkreśla, że wspólne unijne ramy dotyczące kryptoaktywów powinny pomóc w zagwarantowaniu wysokiego poziomu ochrony konsumentów i inwestorów, integralności rynku i stabilności finansowej, egzekwowaniu stosowania przepisów dotyczących przeciwdziałania praniu pieniędzy, takich jak obowiązki wynikające z zasady „znaj swojego klienta” w odniesieniu do agentów zaangażowanych w transakcje związane z kryptoaktywami, z wyłączeniem jedynie sporadycznych transakcji poniżej minimalnego progu, oraz poprawić nadzór nad technologią bazową, tak aby zapewnić organom prowadzącym dochodzenia w sprawie przestępstw możliwość zidentyfikowania końcowych beneficjentów transakcji płatniczych w sposób wiarygodny i przy ograniczonym wysiłku;
35. wyraża zaniepokojenie ustaleniami z przeprowadzonych niedawno badań⁽²⁰⁾, zgodnie z którymi połowa transakcji dokonywanych przy pomocy kryptoaktywów jest związana z nielegalną działalnością, taką jak kupno i sprzedaż nielegalnych towarów lub usług, pranie pieniędzy i płatności w następstwie ataków za pomocą oprogramowania wymuszającego okup; podkreśla, że według niedawnych ustaleń wartość bitcoinów wykorzystywanych do nielegalnej działalności wynosi 76 mld USD rocznie;

⁽²⁰⁾ Dostępne w wersji elektronicznej na stronie <https://ssrn.com/abstract=3102645>

Czwartek, 8 października 2020 r.

36. ponownie zwraca uwagę na potrzebę skutecznego ograniczenia ryzyka prania pieniędzy i finansowania terroryzmu, które to ryzyko jest związane z działalnością transgraniczną i nowymi technologiami, w szczególności ryzyka stwarzanego przez kryptoaktywa;

37. podkreśla, że istniejące luki w ramowych przepisach w sprawie przeciwdziałania praniu pieniędzy dla kryptoaktywów, np. dotyczące stosowania zasady „znaj swojego klienta”, prowadzą do nierównych warunków działania dla różnych rodzajów działalności finansowej; uważa, że przepisy w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu dla dostawców usług związanych z kryptoaktywami powinny być egzekwowane również w przypadku zagranicznych dostawców oferujących usługi w Unii; podkreśla, że w celu lepszego odzwierciedlenia natury i funkcji kryptoaktywów na potrzeby przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu potrzebna jest kompleksowa definicja „wirtualnych aktywów”; zwraca uwagę, że należy także uaktualnić definicję finansowania terroryzmu, aby zapewnić, by odpowiednio uwzględniała ona kryptoaktywa;

38. odnotowuje aktualizację istniejącego zalecenia 16 FATF dotyczącą zasady przechowywania i udostępniania informacji o transakcjach przez dostawców usług aktywów wirtualnych (VASP) i wzywa Komisję do zbadania jej konsekwencji dla dostawców usług wymiany kryptoaktywów i dostawców kont waluty wirtualnej w ramach dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniającej rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylającej dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE⁽²¹⁾,

39. wzywa ponadto Komisję, by poszerzyła zakres podmiotów zobowiązanych na mocy przepisów ramowych w sprawie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, zgodnie z zaleceniami FATF i ESMA, w celu zapewnienia, by wszelkie działania obejmujące kryptoaktywa, w odniesieniu do dostawców usług wymiany w systemie maszynowa wirtualna – maszyna wirtualna, innych kategorii dostawców portfeli i pierwszych ofert kryptowalutowych, podlegały tym samym zobowiązaniom w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu;

40. wyraża przekonanie, że rozpowszechnienie finansów cyfrowych nie powinno nikogo wykluczyć i że dostępności rozwiązań z dziedziny finansów cyfrowych dla konsumentów i inwestorów detalicznych powinny towarzyszyć większe starania, by zapewnić przejrzystość, świadomość społeczną i dostęp do informacji; wzywa Komisję i państwa członkowskie do inwestowania w programy rozwijające umiejętności cyfrowe i finansowe;

41. zauważa, że wprowadzeniu wszelkiej cyfrowej waluty opracowanej przez bank centralny towarzyszą znaczące wyzwania i zagrożenia (np. zagrożenie dla stabilności finansowej, ochrona depozytów, konsekwencje dla transmisji polityki pieniężnej, konsekwencje dla pośrednictwa kredytowego, zastąpienie innych środków płatności, wyparcie prywatnych uczestników rynku itp.), które mogą łatwo przeważać odczuwalne korzyści płynące z cyfrowych walut banku centralnego;

42. zauważa, że niektóre zaobserwowane braki europejskiego systemu płatności można by naprawić, stopniowo ulepszając istniejący system, np. bardziej rozpowszechniając opłacalne płatności natychmiastowe;

Wspólne podejście do cyberodporności sektora finansowego

43. zwraca uwagę, że postępująca cyfryzacja usług finansowych oraz outsourcing do zewnętrznych dostawców rozwiązań informatycznych lub obsługi technicznej takich jak dostawcy usług w chmurze mogą pomóc w szczególności przedsiębiorstwom typu start-up wprowadzać innowacje i uzyskać dostęp do technologii nieosiągalnych dla nich w inny sposób; ostrzega jednak, że coraz wyraźniejsza staje się ekspozycja instytucji i rynków finansowych na zakłócenia spowodowane awariami wewnętrznymi, atakami zewnętrznymi lub trudna sytuacja finansowa i że w związku z tym należy dokładnie ocenić ryzyko operacyjne w tym zmieniającym się otoczeniu; jest zdania, że w związku z tym nadrzędnymi celami wszelkich proponowanych odnośnych przepisów powinny być bezpieczeństwo, odporność i efektywność;

44. zauważa, że choć niezwykle trudno jest ustalić całkowity koszt cyberincydentów, według szacunków sektora w 2018 r. wyniósł on między 45 mld USD a 654 mld USD w skali światowej;

⁽²¹⁾ Dz.U. L 141 z 5.6.2015, s. 73.

Czwartek, 8 października 2020 r.

45. podkreśla, że sektor finansowy jest od dawna głównym celem dla cyberprzestępców poszukujących zysków finansowych;

46. wyraża zaniepokojenie analizą ERRS, w której wykazano, że jest to jak najbardziej wyobrażalne, by cyberincydent mógł przekształcić się w systemowy cyberkryzys zagrażający stabilności finansowej ⁽²²⁾;

47. zwraca uwagę, że niektóre sektorowe elementy unijnego prawa dotyczącego usług finansowych już zawierają szczegółowe wymagania dotyczące zarządzania bezpieczeństwem informacji, natomiast nie jest tak w przypadku innych obszarów unijnego prawa dotyczącego usług finansowych; przypomina, że organy nadzorcze wydały ostrzeżenie dla konsumentów w sprawie pierwszych emisji kryptowalutowych, jako że brak odpowiednich wymogów przejrzystości i ujawniania informacji może być źródłem potencjalnych i poważnych zagrożeń dla inwestorów;

48. wzywa Komisję do zaproponowania zmian legislacyjnych w obszarze wymogów dla unijnego sektora finansowego związanych z ICT i cyberbezpieczeństwem, uwzględniających normy międzynarodowe, aby wyeliminować wszelkie niespójności, braki i luki, które stwierdzono we właściwych przepisach; w tym kontekście wzywa Komisję, aby rozważyła potrzebę wprowadzenia kontroli nadzorczej dostawców ICT, biorąc pod uwagę ryzyko koncentracji i efektu domina, które może wynikać z dużej zależności sektora usług finansowych od niewielkiej liczby dostawców ICT i usług przetwarzania w chmurze;

49. uważa, że zmiany te powinny być skupione na czterech kluczowych obszarach:

- a) modernizacji zarządzania ICT i zarządzania ryzykiem oraz zgodnością z normami międzynarodowymi;
- b) dostosowaniu zasad sprawozdawczości w odniesieniu do incydentów związanych z ICT;
- c) wspólnych ramach dotyczących testów penetracyjnych i testów odporności operacyjnej we wszystkich sektorach finansowych;
- d) nadzorze nad krytycznymi zewnętrznymi dostawcami ICT oraz normach minimalnych dla tych dostawców;

50. podkreśla potrzebę dalszej wymiany informacji, w szczególności o incydentach, oraz lepszej koordynacji między właściwymi organami regulacyjnymi i nadzorczymi, mając na uwadze, iż budowanie odporności i gotowości radzenia sobie z cyberincydentami i incydentami operacyjnymi na dużą skalę wymaga skutecznej współpracy, nie tylko transgranicznej, ale również międzysektorowej; jest zdania, że winno to nastąpić poprzez przyznanie organom nadzorczym pewnych uprawnień, aby mogły one bardziej skutecznie nadzorować działalność prowadzoną przez osoby trzecie, tj. wzmocnione uprawnienia do inspekcji, audytu i nakładania sankcji;

51. wzywa Komisję do wzmocnienia współpracy na forach międzynarodowych, aby ułatwić opracowanie norm międzynarodowych w zakresie przetwarzania w chmurze i outsourcingu; wzywa ponadto do przeprowadzenia analizy dotyczącej potrzeby wprowadzenia specjalnych środków unijnych, aby dostosować nadzór nad przetwarzaniem w chmurze i outsourcingiem do poziomu nadzoru nad tradycyjnymi systemami; zwraca uwagę, że również w tych obszarach konieczne jest opracowanie norm międzynarodowych; jest zdania, że choć odpowiedzialność za przestrzeganie prawa leży po stronie podmiotów finansowych, nadzór nad krytycznymi dostawcami zewnętrznymi powinien mieć na celu monitorowanie ryzyka koncentracji i zagrożenia dla stabilności finansowej oraz zapewnienie współpracy pomiędzy właściwymi organami; jest zdania, że winno to nastąpić poprzez przyznanie organom nadzorczym pewnych uprawnień, aby mogły one bardziej skutecznie nadzorować działalność prowadzoną przez osoby trzecie, tj. wzmocnione uprawnienia do inspekcji, audytu i nakładania sankcji;

52. podkreśla, że odporność systemu finansowego wymaga silnych ram technologicznych do nadzoru nad zastosowaniem zaawansowanej technologii w obszarze usług finansowych; zwraca uwagę na potrzebę konkretnej strategii, zwiększającej wykorzystanie technologii regulacyjnej (RegTech) i nadzorczej (SupTech);

53. wzywa Komisję i organy nadzorcze do prowadzenia działań nieustawodawczych mających na celu wzmocnienie gotowości operacyjnej sektora finansowego na cyberincydenty i incydenty operacyjne na dużą skalę, takich jak wspólne ćwiczenia, protokoły operacyjne („podręczniki taktyczne”), narzędzia bezpiecznej współpracy i inwestycje we wzmocnienie krytycznej infrastruktury i europejskie zdolności w zakresie redundancji; podkreśla, że aby przeprowadzać takie ćwiczenia i działania nadzorcze, organy nadzorcze muszą dysponować wewnętrzną wiedzą ekspercką i odpowiednimi zasobami;

⁽²²⁾ ERRS opublikowała w lutym 2020 r. sprawozdanie w sprawie systemowych cyberataków (<https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html>).

Czwartek, 8 października 2020 r.

54. wzywa Komisję do oceny i uregulowania ryzyka możliwości transakcji na czarnym rynku, prania pieniędzy, finansowania terroryzmu, oszustw, unikania opodatkowania i innych rodzajów działalności przestępczej;

Dane

55. przypomina, że gromadzenie i analizowanie danych odgrywa kluczową rolę w odniesieniu do finansów cyfrowych, dlatego podkreśla potrzebę spójnego i neutralnego pod względem technologicznym stosowania istniejących przepisów dotyczących danych; podkreśla, że sztuczna inteligencja jest jedną z kluczowych technologii mogących wzmocnić globalną konkurencyjność Unii;

56. zwraca uwagę, że Unia wyznacza światowe normy w dziedzinie ochrony danych osobowych; podkreśla, że przekazywanie i wykorzystywanie danych osobowych i nieosobowych w sektorze usług finansowych powinno odbywać się zgodnie ze wszystkimi właściwymi przepisami Unii i umowami międzynarodowymi, a jednocześnie umożliwiać zgodny z prawem i bezpieczny przepływ danych niezbędny do zwiększenia skali innowacyjnych inicjatyw finansowych;

57. podkreśla, że w celu zwiększenia skali innowacyjnych finansów potrzebny jest swobodny przepływ danych w Unii; zwraca uwagę, że transgraniczne przepływy danych, w tym do i z państw trzecich, muszą być monitorowane i regulowane przez prawo Unii w zakresie prywatności i ochrony danych;

58. zwraca się w związku z tym do Komisji o zapewnienie podmiotom sektora finansów cyfrowych możliwość dostępu na równych warunkach do istotnych, wiarygodnych i użytecznych danych zgodnie z RODO poprzez tworzenie większej wartości dla klienta, rozwijanie potencjału finansów cyfrowych i zapewnienie innowacyjnym przedsiębiorstwom z branży technologii finansowej możliwości rozwoju w Unii i poza nią; podkreśla znaczenie przestrzegania zasad konkurencji na rynku wewnętrznym oraz zadbania, aby nie ucierpiały interesy konsumentów i innowacje; wzywa Komisję, by monitorowała oferowanie usług finansowych przez gigantów technologicznych, a także to, jak przewaga konkurencyjna właściwa dla tych podmiotów może zakłócić konkurencję na rynku, szkodząc interesom konsumentów i innowacjom;

59. podkreśla, że Komisja powinna znaleźć kompromis między zapewnieniem bezpieczeństwa danych i ochrony konsumentów a utrzymaniem wysokiego poziomu zadowolenia konsumentów i wydajności usług;

60. zwraca się do Komisji, aby w oparciu o istniejącą normę unijną na mocy rozporządzenia Parlamentu Europejskiego 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 uchylającego dyrektywę 1999/93/WE⁽²³⁾ rozważyła infrastrukturę dla cyfrowego *onboardingu* i korzystania z cyfrowych tożsamości finansowych, która miałaby na celu zharmonizowanie istniejących wymogów regulacyjnych w całej Unii w niezbędnym zakresie oraz ułatwienie ich stosowania w celu zapewnienia mniej rozdrobnionych operacji na rynku wewnętrznym oraz zgodności z odpowiednimi przepisami dotyczącymi przeciwdziałania praniu pieniędzy; podkreśla znaczenie i potencjalne korzyści płynące z korzystania z cyfrowych tożsamości finansowych we wszystkich sektorach i państwach członkowskich, przy jednoczesnym zapewnieniu ich zgodności z normami ochrony danych i prywatności oraz zagwarantowaniu odpowiednich i proporcjonalnych środków pozwalających uniknąć incydentów związanych z danymi lub tożsamością;

61. zwraca uwagę, że w przypadku procesów wynikających z zasady „znaj swojego klienta” wymogi prawne dla *onboardingu* klientów indywidualnych przez instytucje finansowe różnią się w poszczególnych państwach członkowskich i dlatego *onboarding* transgraniczny z istniejącymi zbiorami danych często nie jest możliwy, co również odnosi się do *onboardingu* klientów korporacyjnych i związanego z nim procesu wynikającego z zasady „znaj swojego klienta” i „znaj swojego partnera biznesowego”; wzywa Komisję do zajęcia się tą kwestią i wspierania harmonizacji danych wymaganych przez państwa członkowskie w związku z zasadą „znaj swojego klienta”;

62. potwierdza, że interoperacyjność między cyfrowymi podmiotami na poziomie krajowym i unijnym jest kluczem do osiągnięcia pożądanego uznania na rynku;

⁽²³⁾ (Dz.U. L 257 z 28.8.2014, s. 73.)

Czwartek, 8 października 2020 r.

63. zwraca uwagę, że dane dotyczące klientów lub „duże zbiory danych”, kluczowe dla tworzenia dodatkowej wartości dla klienta i utrzymania konkurencyjności, są coraz częściej wykorzystywane przez instytucje finansowe; przypomina wnioski i zalecenia zawarte w rezolucji Parlamentu Europejskiego z dnia 14 marca 2017 r. w sprawie wpływu technologii dużych zbiorów danych na prawa podstawowe; przypomina ramy prawne dla przetwarzania danych osobowych wyznaczone w RODO i wzywa wszystkie zainteresowane strony do wzmoczonych wysiłków, aby zagwarantować egzekwowanie określonych w nich praw; podkreśla w szczególności zasadę dotyczącą prawa osób fizycznych do bycia właścicielem swoich danych i sprawowania kontroli nad nimi oraz prawa do przenoszenia danych;

64. uważa, że suwerenna tożsamość oparta na technologii rozproszonego rejestru może być kluczowym elementem przy opracowaniu wielu nowych usług i platform dla jednolitego rynku cyfrowego niezależnie od agregatorów danych i z pominięciem pośredników, przy jednoczesnym zapewnieniu wysokiego poziomu bezpieczeństwa i norm ochrony danych dla poszczególnych obywateli Unii;

65. uważa, że brak dostępnych i wiarygodnych danych i informacji na temat działalności w dziedzinie finansów cyfrowych może być niekorzystny dla wzrostu, ochrony konsumentów, integralności rynku i stabilności finansowej, a także dla przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, uchylaniu się od opodatkowania i unikaniu opodatkowania; opowiada się za większą przejrzystością i szerszą sprawozdawczością w zakresie działalności w dziedzinie finansów cyfrowych w celu zmniejszenia asymetrii i ryzyka, w szczególności ze strony zasiedziałych operatorów dużych zbiorów danych, którzy mogą czerpać nieproporcjonalnie wysokie zyski ze zwiększonego dostępu do danych; podkreśla znaczenie równych szans w odniesieniu do transgranicznego dostępu do danych, jaki gwarantuje RODO w zakresie danych osobowych;

66. podkreśla, że w tym kontekście normy odgrywają kluczową rolę w dalszym promowaniu zarządzania danymi, ich udostępniania i dzielenia się nimi, w tym interoperacyjności i możliwości przenoszenia danych; stwierdza, że wymaga to również niezawodnej i bezpiecznej pod względem prawnym infrastruktury, a także solidnych ram prawnych dotyczących łączenia danych i dzielenia się nimi, które to ramy pozwolą przedsiębiorstwom nabrać zaufania do współpracy w zakresie danych między przedsiębiorstwami, a nawet między sektorami;

67. wzywa do zapewnienia skutecznego nadzoru nad analityką dużych zbiorów danych w sposób uwzględniający brak przejrzystości modeli, a jednocześnie zapewniający wystarczający dostęp do odpowiednich danych wysokiej jakości; podkreśla potrzebę większej rozliczalności, wytłumaczalności i przejrzystości w odniesieniu do algorytmów, przetwarzania danych i analityki, co stanowiłoby niezbędne narzędzia zapewniające odpowiednie informowanie osób fizycznych o przetwarzaniu ich danych osobowych;

68. podkreśla znaczenie otwartej bankowości dla poprawy jakości usług płatniczych przez włączenie nowych uczestników rynku zapewniających konsumentowi większą efektywność operacyjną i cenową; zwraca uwagę, że przejście od otwartej bankowości do otwartych finansów, tj. włączenie usług finansowych innych niż płatności, jest priorytetem strategicznym, który może poprawić efektywność, ograniczyć ryzyko koncentracji i poprawić włączenie społeczne pod względem finansowym;

69. uznaje, że wymagany wniosek nie pociąga za sobą skutków finansowych;

o

o o

70. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji oraz zaleceń zawartych w załączniku Komisji i Radzie oraz parlamentom i rządóm państw członkowskich.

Czwartek, 8 października 2020 r.

ZAŁĄCZNIK DO REZOLUCJI:**ZALECENIA DOTYCZĄCE TREŚCI PROPONOWANEGO WNIOSKU****A. ZASADY I CELE WNIOSKU**

1. Przygotowanie podstaw dla zorientowanego na przyszłość podejścia do przepisów dotyczących finansów cyfrowych w Unii.
2. Zapewnienie, aby finansowanie cyfrowe nadal mogło stanowić innowacyjny czynnik napędzający wzrost i tworzenie miejsc pracy na całym jednolitym rynku.
3. Promowanie wspólnego rozumienia kluczowych kwestii dotyczących finansów cyfrowych i promowanie harmonizacji odpowiednich przepisów, co doprowadzi do wzmożenia działalności transgranicznej.
4. Zwiększenie udostępniania danych zgodnie z zasadami Unii, aby stymulować innowacje. Celem powinno być ułatwienie dostępu do danych publicznych w całej Unii. Byłoby to korzystne nie tylko dla przedsiębiorstw z branży finansów cyfrowych, lecz także dla wielu innych obszarów polityki Unii i zwiększyłoby przejrzystość rynku.
5. Rozważenie trzech obszarów wstępnych działań Unii, mianowicie opracowania ram dla kryptoaktywów, opracowania ram dotyczących cyberodporności i odporności operacyjnej oraz dążenia do harmonizacji koncepcji cyfrowego *onboardingu* na jednolitym rynku.

B. DZIAŁANIA, JAKIE NALEŻY ZAPROPONOWAĆ

1. Przedstawienie wniosku ustawodawczego w sprawie kryptoaktywów, który zapewnia jednocześnie pewność prawa w odniesieniu do traktowania kryptoaktywów oraz wysoki standard ochrony konsumentów i inwestorów, integralność rynku i stabilność finansową. Takie ramy powinny uwzględniać otwartą i kompleksową taksonomię ogólnounijną i mieć na celu stanowienie prawa zgodnie z zasadą, że te same przepisy mają zastosowanie do tej samej działalności i tego samego ryzyka, oraz z zasadą proporcjonalności, minimalizując tym samym arbitraż regulacyjny i zapewniając równe szanse.

Taki wniosek ustawodawczy powinien:

- a) zawierać wytyczne dotyczące obowiązujących procesów regulacyjnych, nadzorczych i ostrożnościowych oraz postępowania z kryptoaktywami; przyjmując szczegółowe przepisy w sprawie przejrzystości i integralności rynku odpowiadających co najmniej przepisom MiFID II w odniesieniu do emitentów lub sponsorów kryptoaktywów;
 - b) usunąć luki regulacyjne w obowiązującym prawodawstwie Unii w odniesieniu do kryptoaktywów, na przykład klasyfikując niektóre kryptoaktywa jako „zbywalne papiery wartościowe” zgodnie z MiFID II, aby zapewnić ich traktowanie na równi z innymi zbywalnymi papierami wartościowymi;
 - c) stworzyć dostosowany do potrzeb system regulacyjny dla nowych i zmieniających się rodzajów działalności związanej z kryptoaktywami, takich jak pierwsze oferty kryptowalutowe lub pierwsze oferty kryptogieldowe, oraz dla wszelkich kryptoaktywów, które nie są objęte istniejącymi ramami regulacyjnymi, zapewniając ich zharmonizowane uregulowanie na szczeblu Unii;
 - d) zająć się wpływem wydobywania kryptowalut na środowisko oraz potrzebą rozwiązań mających na celu ograniczenie śladu ekologicznego popularnych kryptoaktywów;
2. Dążenie do większej zbieżności przepisów i praktyk nadzorczych w celu opracowania wspólnych ram unijnych; apeluje o zorganizowany dialog między Europejskimi Urzędami Nadzoru a właściwymi organami krajowymi, który powinien koncentrować się na obecnych wyzwaniach nadzorczych i konwergencji praktyk w celu zapewnienia sprawnego nadzoru na wszystkich szczeblach w dziedzinie finansów cyfrowych;

Czwartek, 8 października 2020 r.

3. opracowanie ram prawnych dla stabilnych kryptowalut, gwarantujących, że spełniają one co najmniej normy określone w dyrektywie Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniającej dyrektywy 2005/60/WE i 2006/48/WE oraz uchylającej dyrektywę 2000/46/WE⁽¹⁾, włącznie ze stałym kursem wymiany, po wartości nominalnej, z walutami fiducyjnymi;
4. przedłożenie – w oparciu o ocenę – wniosku w sprawie wspólnych ram unijnych dotyczących ogólnoeuropejskiego „poletka doświadczalnego” dla cyfrowych usług finansowych;
5. wzmocnienie stosowania ram dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu w odniesieniu do kryptoaktywów i wyeliminowanie istniejących luk prawnych, w szczególności poprzez środki opisane w ust. 33–38;
6. dopilnowanie, aby rozprzestrzenianie się finansów cyfrowych nie pozostawiło nikogo w tyle. wzywa Komisję i państwa członkowskie do podjęcia działań na rzecz poprawy umiejętności cyfrowych i finansowych;
7. przedstawienie wniosku ustawodawczego w sprawie cyberodporności, który zapewnia spójne normy bezpieczeństwa ICT i cyberbezpieczeństwa w całym sektorze finansowym Unii, z uwzględnieniem norm międzynarodowych. Takie ramy powinny być zorientowane na przyszłość i skupione na modernizacji obecnych przepisów mających zastosowanie do cyberodporności, a jednocześnie likwidować również wszelkie luki i braki regulacyjne, które mogą stwarzać ryzyko dla przedsiębiorstw, inwestorów i konsumentów.
8. wyznaczenie jednolitego europejskiego organu nadzorczego do nadzoru i rejestracji wszelkiej działalności o wymiarze transgranicznym związanej z kryptoaktywami w Unii, we współpracy z innymi organami nadzoru na szczeblu Unii, w oparciu o wspólny zbiór przepisów;
9. wzywa Komisję, aby rozważyła możliwość przeprowadzenia kontroli nadzorczej dostawców ICT w dziedzinie usług finansowych, którzy świadczą usługi w Unii, jak określono w ust. 47;
10. wzywa Komisję do zaproponowania zmian ustawodawczych w dziedzinie wymogów dotyczących ICT i cyberbezpieczeństwa dla sektora finansowego Unii. Zmiany te powinny koncentrować się na czterech kluczowych obszarach określonych w ust. 48;
11. prace nad opracowaniem unijnych norm w dziedzinie chmur obliczeniowych i outsourcingu, przy jednoczesnej współpracy z partnerami międzynarodowymi w celu opracowania norm międzynarodowych, jak określono w ust. 50;

Dane

12. Zaproponowanie ram dotyczących cyfrowego *onboardingu*. Te zasady powinny być zgodne z odpowiednimi przepisami unijnymi, takimi jak przepisy o przeciwdziałaniu praniu pieniędzy, normy ochrony danych i ochrony prywatności, oraz dążyć do stworzenia wspólnej koncepcji cyfrowych tożsamości finansowych na całym jednolitym rynku, przy wspieraniu harmonizacji *onboardingu* transgranicznego;
13. Prace na rzecz zwiększenia rozliczalności, wytłumaczalności i przejrzystości w odniesieniu do algorytmów, przetwarzania danych i analizy, jak określono w ust. 66.

⁽¹⁾ Dz.U. L 267 z 10.10.2009, s. 7.