KOMISJA
EUROPEJSKA

Bruksela, dnia 10.1.2017 r.
COM(2017) 9 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

„BUDOWA EUROPEJSKIEJ GOSPODARKI OPARTEJ NA DANYCH”

{SWD(2017) 2 final}

„BUDOWA EUROPEJSKIEJ GOSPODARKI OPARTEJ NA DANYCH"

1. WPROWADZENIE

Dane stały się istotnym elementem wzrostu gospodarczego, tworzenia miejsc pracy i postępu społecznego. Analiza danych ułatwia optymalizację procesów i decyzji, sprzyja innowacyjności i wspomaga przewidywanie zdarzeń. Ten ogólnoświatowy trend niesie ze sobą ogromny potencjał w różnych dziedzinach, począwszy od zdrowia, środowiska naturalnego, bezpieczeństwa żywnościowego, działania w dziedzinie klimatu i efektywnego gospodarowania zasobami, po energię, inteligentne systemy transportowe i inteligentne miasta.

Tak zwana gospodarka oparta na danych[1] charakteryzuje się ekosystemem, w którym różnego rodzaju uczestnicy rynku – producenci, badacze i dostawcy infrastruktury – współpracują ze sobą, zapewniając dostępność i użyteczność danych. Dzięki temu uczestnicy rynku mogą wykorzystywać dane, tworząc rozmaite aplikacje, które w znaczącym stopniu ułatwiają codzienne życie (np. system zarządzania ruchem, optymalizacja zbiorów bądź opieka zdrowotna na odległość).

W 2014 roku wartość unijnej gospodarki opartej na danych oszacowano na 257 mld euro, czyli 1,85 % unijnego PKB[2]. W 2015 roku liczba ta wzrosła do 272 mld euro, czyli 1,87 % unijnego PKB (wzrost o 5,6 % w porównaniu z rokiem poprzednim). Według tej samej prognozy, jeśli w odpowiednim czasie zostaną stworzone ramy prawne dla funkcjonowania gospodarki opartej na danych, jej wartość w 2020 roku wzrośnie do 643 mld euro, czyli 3,17 % całkowitego PKB Unii Europejskiej.

Na mocy ogólnego rozporządzenia o ochronie danych[3], od maja 2018 roku w miejsce 28 krajowych aktów prawnych powstanie jeden ogólnoeuropejski zbiór przepisów. Dzięki nowo utworzonemu mechanizmowi kompleksowej obsługi[4], jeden organ ochrony danych będzie odpowiadał za nadzór nad transgranicznymi operacjami przetwarzania danych prowadzonymi przez przedsiębiorstwo na terytorium UE. Zagwarantowana zostanie konsekwentna interpretacja nowych przepisów. Dotyczy to zwłaszcza spraw o

---

1 Gospodarka oparta na danych mierzy całkowity wpływ rynku danych – tj. rynku, na którym następuje wymiana danych cyfrowych w postaci produktów lub usług pochodzących z danych surowych – na całą gospodarkę. Obejmuje tworzenie, gromadzenie, przechowywanie, przetwarzanie, rozpowszechnianie, analizę, opracowywanie, dostarczanie i wykorzystywanie danych możliwe dzięki technologiom cyfrowym (Badanie europejskiego rynku danych, SMART 2013/0063, IDC, 2016).

2 Badanie europejskiego rynku danych, SMART 2013/0063, IDC, 2016.

3 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 95/56/WE (ogólne rozporządzenie o ochronie danych), Dz. U. L 119 z 4.5.2016, s. 1.

4 Art. 56 ogólnego rozporządzenia o ochronie danych.

charakterze transgranicznym z udziałem kilku krajowych organów ochrony danych, w których wspólne problemy będą rozwiązywane wspólnymi środkami na podstawie jednej decyzji. Ponadto ogólnym rozporządzeniem o ochronie danych ustanowiono równe warunki działania dla przedsiębiorstw unijnych i zagranicznych, w których przedsiębiorstwa spoza UE będą musiały stosować te same zasady co przedsiębiorstwa europejskie w zakresie oferowania dóbr i usług bądź monitorowania zachowań osób na terytorium UE. Większe zaufanie ze strony konsumentów przyniesie korzyści zarówno Unii Europejskiej, jak i zewnętrznym podmiotom gospodarczym.

Dyrektywa o prywatności i łączności elektronicznej dotyczy poufności usług łączności elektronicznej w UE. Zmieniona dyrektywa o prywatności i łączności elektronicznej, której projekt został zgłoszony równolegle z niniejszym komunikatem w formie rozporządzenia[5] ma zapewnić wysoki poziom ochrony w pełnej zgodności z ogólnym rozporządzeniem o ochronie danych. Skuteczne przepisy o ochronie danych osobowych budują zaufanie, które umożliwi rozwój gospodarki cyfrowej na rynku wewnętrznym.

Jak podkreślał przewodniczący Juncker w swoim orędziu o stanie Unii wygłoszonym w dniu 14 września 2016 roku, *„[b]ycie Europejczykiem oznacza prawo do ochrony własnych danych osobowych za pomocą skutecznych europejskich przepisów. Bo Europejczycy nie lubią dronów nad głowami, rejestrujących każdy ich ruch, ani przedsiębiorstw śledzących każde kliknięcie myszką. Dlatego Parlament, Rada i Komisja uzgodniły w maju tego roku wspólne europejskie rozporządzenie w sprawie ochrony danych. To mocne europejskie prawo mające zastosowanie do przedsiębiorstw, niezależnie od tego, gdzie się znajdują i kiedy przetwarzają Wasze dane. Bo w Europie prywatność jest ważna. To kwestia ludzkiej godności*”.

W komunikacie pt. „Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku” z 2012 roku[6] oraz komunikacie pt. „Ku gospodarce opartej na danych” z 2014 roku[7] Komisja uznała potrzebę wprowadzenia nowoczesnych, spójnych zasad na terytorium całej Unii Europejskiej, które umożliwiałyby swobodny przepływ danych pomiędzy państwami członkowskimi, i stwierdziła, że europejska gospodarka cyfrowa zbyt wolno przyjmuje rewolucję w zakresie danych w porównaniu z USA i brakuje jej porównywalnego potencjału przemysłowego. Komisja doszła do wniosku, że brak otoczenia prawnego uwzględniającego handel danymi w UE może przyczynić się do ograniczenia dostępu do większych zbiorów danych, powstania barier wejścia dla nowych podmiotów oraz zahamowania innowacyjności.

Nieuzasadnione **ograniczenia swobodnego przepływu danych** mogą zahamować rozwój unijnej gospodarki opartej na danych. Ograniczenia te odnoszą się do wymogów narzucanych przez organy publiczne w zakresie lokalizacji przechowywanych bądź przetwarzanych danych. Kwestia swobodnego przepływu danych dotyczy wszelkiego rodzaju danych: przedsiębiorcy i podmioty gospodarki opartej na danych mają styczność z danymi przemysłowymi i generowanymi maszynowo (nie tylko osobowymi), a także danymi stworzonymi przy udziale człowieka. W strategii jednolitego rynku cyfrowego Komisja zapowiedziała przedstawienie inicjatywy znoszącej ograniczenia swobodnego

[5] COM (2017) 10.

[6] COM (2012) 9.

[7] COM (2014) 442.

przepływu danych niepodyktowane ochroną danych osobowych na terytorium UE oraz nieuzasadnione ograniczenia w zakresie lokalizacji przechowywanych bądź przetwarzanych danych. Wśród takich ograniczeń znajdują się akty prawne uchwalone przez państwa członkowskie, przepisy administracyjne i praktyki o równoważnym skutku. Ich liczba zazwyczaj wzrasta w miarę rozwoju gospodarki opartej na danych, powodując niepewność co do miejsca, w którym dane mogą być przechowywane lub przetwarzane. Może to uderzyć we wszystkie sektory gospodarki i organizacje sektora zarówno prywatnego, jak i publicznego, które mogłyby mieć trudności z dostępem do bardziej innowacyjnych lub tańszych usług w zakresie danych. Nieuzasadnione restrykcje w zakresie lokalizacji danych ograniczają swobodę świadczenia usług i swobodę przedsiębiorczości ustanowione w Traktacie, a ponadto są niezgodne ze stosownymi przepisami prawa wtórnego. W efekcie istnieje ryzyko rozdrobnienia rynku, obniżenia jakości usług świadczonych użytkownikom i ograniczenia konkurencyjności dostawców usług w zakresie danych, zwłaszcza mniejszych podmiotów.

Nieuzasadniona lokalizacja danych stanowi także temat rozmów toczonych między Unią Europejską a jej partnerami handlowymi w związku z rosnącym znaczeniem danych i usług w zakresie danych w gospodarce globalnej i potencjalnymi uwagami w tej kwestii ze strony państw trzecich. Unijne zasady dotyczące ochrony danych nie mogą podlegać negocjacjom przy zawieraniu porozumień o wolnym handlu. Jak wyjaśniono w komunikacie o wymianie i ochronie danych osobowych w zglobalizowanym świecie[8], dialog dotyczący ochrony danych i negocjacje handlowe z krajami trzecimi muszą być prowadzone osobno. Oprócz tego, jak wskazano w komunikacie pt. „Handel z korzyścią dla wszystkich”[9], Komisja zamierza wykorzystać umowy handlowe UE do ustanowienia zasad handlu elektronicznego i transgranicznego przepływu danych oraz zwalczania nowych przejawów protekcjonizmu cyfrowego w pełnej zgodności z unijnymi przepisami w zakresie ochrony danych i bez uszczerbku dla nich.

Ponadto, w miarę postępującej, opartej na danych transformacji gospodarki i społeczeństwa, coraz większe ilości danych generowane są przez maszyny lub procesy oparte na nowych technologiach, takich jak internet rzeczy (ang. *Internet of Things*, IoT), tzw. fabryki jutra bądź autonomiczne systemy połączone. Sama łączność zmienia formy dostępu do danych: coraz częściej dane, które do tej pory były zwykle udostępniane za pomocą połączeń fizycznych, mogą być pozyskiwane na odległość. Olbrzymia różnorodność źródeł i rodzajów danych oraz ogromne możliwości ich analizy w różnych domenach, w tym w celu opracowania polityki publicznej, dopiero zaczynają się zarysowywać. Aby móc korzystać z tych możliwości, zarówno publiczne, jak i prywatne podmioty rynku danych muszą mieć dostęp do dużych i różnorodnych zbiorów danych. Dlatego kwestia dostępu i transmisji danych generowanych przez wspomniane maszyny i procesy ma zasadnicze znaczenie dla ukształtowania się gospodarki opartej na danych i wymaga uważnej oceny.

Inne wyłaniające się zagadnienia dotyczą zastosowania zasad odpowiedzialności za wszelkie szkody powstałe w wyniku błędu urządzenia bądź robota, a także możliwości przenoszenia i interoperacyjności danych. W związku z nowymi technologiami, takimi jak internet rzeczy bądź robotyka, występują złożone i zawiłe zależności zarówno w

[8] COM (2017) 7.

[9] COM (2015) 497

ramach produktów (opartych na sprzęcie i oprogramowaniu), jak i połączonych urządzeń. Ponadto mogą pojawić się nowe kwestie związane z autonomicznymi maszynami, których nieoczekiwane i niezamierzone zachowania mogą powodować szkody na osobach i mieniu. Opisane zjawiska mogą powodować brak pewności prawa w zakresie stosowania istniejących ram prawnych dotyczących odpowiedzialności i bezpieczeństwa.

Zgodnie z treścią strategii jednolitego rynku cyfrowego celem Komisji jest stworzenie przejrzystych i odpowiednio dostosowanych zasad i ram prawnych gospodarki opartej na danych poprzez usunięcie pozostałych barier w przepływie danych i wyjaśnienie wątpliwości natury prawnej związanych z nowymi technologiami danych. Kolejne zadania leżące u podstaw niniejszego komunikatu to zwiększenie dostępności i wykorzystania danych, promowanie nowych modeli biznesowych w zakresie danych, a także polepszenie warunków dostępu do danych i rozwój unijnej analityki danych. W tym celu Komisja przedstawia zagadnienia do dyskusji, mając na względzie „budowę europejskiej gospodarki opartej na danych".

W związku z tym w niniejszym komunikacie poruszane są następujące zagadnienia: swobodny przepływ danych, dostęp i transfer w zakresie danych generowanych maszynowo, odpowiedzialność i bezpieczeństwo w związku z nowymi technologiami oraz możliwość przenoszenia danych nieosobowych, interoperacyjność i normy. W komunikacie znalazły się także propozycje eksperymentów w zakresie wspólnych rozwiązań regulacyjnych w warunkach rzeczywistych.

Komisja inicjuje obejmujący szerokie grono interesariuszy dialog, dotyczący kwestii poruszanych w niniejszym komunikacie. Pierwszy krok w procesie dialogu stanowią konsultacje społeczne podejmowane równolegle do pakietu dotyczącego gospodarki opartej na danych[10].

2. SWOBODNY PRZEPŁYW DANYCH

Aby gospodarka oparta na danych mogła sprawnie funkcjonować i dynamicznie się rozwijać, należy umożliwić przepływ danych na rynku wewnętrznym i zapewnić jego ochronę. W gwałtownie zmieniającym się środowisku technologicznym bezpieczny i pewny przepływ danych ma zasadnicze znaczenie dla ochrony czterech podstawowych swobód jednolitego rynku UE (przepływu towarów, osób, usług i kapitału) zagwarantowanych postanowieniami Traktatów. Następuje gwałtowny rozwój usług w zakresie danych w Unii Europejskiej i na całym świecie. Sprawnie funkcjonujący i pozbawiony barier jednolity rynek w tym sektorze stworzyłby znaczne szanse na szybszy rozwój i nowe miejsca pracy.

We wspomnianym rozwoju i innowacyjności gospodarki opartej na danych, a także wprowadzeniu transgranicznych usług publicznych, przeszkodzić mogą bariery w swobodnym przepływie danych w UE, takie jak nieuzasadnione wymogi dotyczące lokalizacji danych narzucone przez organy publiczne. Restrykcje w zakresie lokalizacji danych w praktyce powodują przywrócenie „kontroli granicznych" w cyfrowej postaci[11].

[10] https://ec.europa.eu/digital-single-market/news-redirect/52039

[11] OECD, „Emerging Policy Issues: Localisation Barriers to Trade" (Nowe kwestie polityczne: bariery dla handlu związane z lokalizacją), 2015 i prace bieżące.

Przyjmują one różne formy, od stawianego przez organy nadzoru wymogu lokalnego przechowywania danych przez dostawców usług finansowych, poprzez wprowadzanie zasad tajemnicy służbowej pociągających za sobą wymóg lokalnego przechowywania i przetwarzania danych, rygorystyczne przepisy zobowiązujące do lokalnego przechowywania informacji archiwalnych generowanych przez sektor publiczny, niezależnie od stopnia ich wrażliwości.

Ochrona prywatności znajduje swoje uzasadnienie, organy publiczne nie mogą jednak tłumaczyć nią nieuzasadnionych prób ograniczania swobodnego przepływu danych. Jak zaznaczono powyżej, ogólne rozporządzenie o ochronie danych przewiduje jednolity zbiór zasad zapewniających wysoki poziom ochrony danych osobowych w całej UE. Zwiększa zaufanie konsumentów do usług online i zapewnia jednakowe stosowanie zasad we wszystkich państwach członkowskich dzięki wzmocnieniu krajowych organów ochrony danych. Rozporządzenie przyczynia się do wzrostu zaufania niezbędnego do przetwarzania danych i stanowi fundament swobodnego przepływu danych w UE. Rozporządzenie znosi ograniczenia w swobodnym przepływie danych osobowych na terytorium Unii tłumaczone potrzebą ochrony danych osobowych[12]. Natomiast ograniczenia podyktowane innymi powodami niż ochrona danych osobowych, np. na podstawie przepisów podatkowych lub o rachunkowości, nie stanowią przedmiotu ogólnego rozporządzenia o ochronie danych. Ponadto dane nieosobowe, tj. dane niedotyczące osoby fizycznej, której tożsamość została ustalona lub którą można ustalić[13], nie zostały objęte zakresem rozporządzenia i mogą dotyczyć na przykład danych nieosobowych wygenerowanych maszynowo.

Ograniczenia w zakresie lokalizacji danych mogą wynikać z przepisów prawa lub wytycznych lub praktyk administracyjnych, które nakładają wymóg przechowywania lub przetwarzania danych[14] w formacie elektronicznym[15] w ściśle wyznaczonym obszarze geograficznym lub obszarze jurysdykcji. Niekiedy państwa członkowskie wprowadzają ograniczenia w przeświadczeniu, że organy nadzoru będą mogły dzięki temu łatwiej kontrolować dane przechowywane lokalnie. Lokalizację stosuje się także jako zastępczą gwarancję prywatności, audytu i egzekwowania prawa i bezpieczeństwa danych. W praktyce jednak wspomniane środki rzadko pozwalają osiągnąć zamierzony cel.

Bezpieczeństwo informacji zależy od szeregu czynników oprócz fizycznej lokalizacji danych, m.in. zachowania poufności i spójności danych, gdy te są dostępne poza miejscem ich przechowywania. Pod tym względem rzeczywiste bezpieczeństwo przechowywanych i przetwarzanych danych zapewniają nie ograniczenia w zakresie

---

[12] Art. 1 ust. 3. Np. dynamiczny adres IP zarejestrowany przez dostawcę usług medialnych online przy okazji przeglądania przez daną osobę strony internetowej, którą dostawca ten udostępnia publicznie, stanowi wobec tego dostawcy dane osobowe, w sytuacji gdy dysponuje on środkami prawnymi umożliwiającymi mu ustalenie tożsamości osoby, której dane dotyczą, dzięki dodatkowym informacjom, jakimi dostawca usług internetowych dysponuje w odniesieniu do tej osoby. Zob. wyrok Trybunału w sprawie C-582/14, Breyer, ECLI:EU:C:2016:779, akapit 49.

[13] Zgodnie z art. 4 ust. 1 ogólnego rozporządzenia o ochronie danych.

[14] Zarówno danych prywatnych, jak i publicznych.

[15] W tym kopii zbiorów danych.

lokalizacji danych, a najlepsze praktyki w dziedzinie zarządzania nowoczesnymi technologiami informacyjno-komunikacyjnymi na znacznie większą skalę niż pojedyncze systemy. Przykładowo w celu ochrony danych przed występującymi lokalnie klęskami żywiołowymi bądź atakami cybernetycznymi, magazyny danych znajdujące się w różnych państwach członkowskich mogą zabezpieczać się nawzajem, tworząc kopie zapasowe, a także stosować środki techniczne i organizacyjne przewidziane w dyrektywie w sprawie bezpieczeństwa sieci i systemów informatycznych[16]. Ponadto większą dostępność danych na potrzeby kontroli i nadzoru, których zasadność nie jest w żadnym razie podważana, w większym stopniu niż ograniczenia w zakresie lokalizacji danych gwarantowałaby lepsza współpraca między organami krajowymi oraz organami krajowymi a sektorem prywatnym,. W obszarze charakteryzującym się bliską współpracą między organami nadzoru, takim jak usługi finansowe, wymogi w zakresie lokalizacji danych mogłyby przynieść skutek wręcz odwrotny do zamierzonego[17].

Pomimo to wymogi w zakresie lokalizacji danych mogą być uzasadnione i proporcjonalne w określonych warunkach lub w odniesieniu do określonych danych, zwłaszcza przed wejściem w życie stosownych porozumień o współpracy transgranicznej, zapewniających m.in. bezpieczne przechowywanie i przetwarzanie danych związanych z kluczową infrastrukturą energetyczną, dostęp organów ścigania do dowodów cyfrowych (np. lokalnych kopii zbiorów danych) bądź lokalne przechowywanie danych znajdujących się w określonych rejestrach publicznych.

Niestety zarówno w Europie, jak i na całym świecie przeważa tendencja ku większej lokalizacji danych, często oparta na błędnym przeświadczeniu, że usługi lokalne są z zasady bezpieczniejsze niż usługi transgraniczne. Co więcej, znaczący wpływ na rynek usług w zakresie danych ma brak przejrzystych zasad i mocno zakorzenione przekonanie o potrzebie lokalizacji danych. Powyższe czynniki mogą ograniczyć dostęp przedsiębiorstw i organizacji sektora publicznego do tańszych lub bardziej innowacyjnych usług w zakresie danych lub zmusić przedsiębiorstwa działające w wymiarze transgranicznym do zwiększenia możliwości w zakresie przechowywania i przetwarzania danych. Może to także utrudnić przedsiębiorstwom opartym na danych, w szczególności przedsiębiorstwom typu start-up oraz MŚP, wejście na nowe rynki (np. ze względu na konieczność zainwestowania w ośrodki przetwarzania danych w 28 państwach członkowskich) lub centralizację możliwości w zakresie danych i analityki w celu opracowania nowych produktów i usług.

Obecnie Europa zaspokaja 84 % końcowego popytu na usługi związane z ICT (konsulting, hosting, prace rozwojowe) na terytorium UE. Ułatwienie realizacji tych usług także na poziomie transgranicznym w ramach UE dzięki usunięciu ograniczeń w

[16] Dyrektywa 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, Dz. U. L 194 z 19.7.2016, s. 1.

[17] Zgodnie z przepisami unijnymi dotyczącymi usług finansowych i Europejskiego Systemu Nadzoru Finansowego organy nadzoru muszą mieć zapewniony dostęp do danych dotyczących instytucji finansowych i transakcji na całym terytorium Unii Europejskiej. Wymóg przechowywania danych na terytorium określonego kraju lub wymogi warunkujące dostęp organów nadzoru do procedur administracyjnych mogą ograniczyć dostęp organów nadzoru do danych, które są niezbędne do wykonywania przez nie swoich uprawnień.

zakresie lokalizacji danych mogłoby przynieść wzrost PKB nawet do 8 mld euro rocznie w postaci oszczędności kosztów i przyrostu wydajności[18].

Lokalizacja danych utrudnia również szersze zastosowanie przechowywania i przetwarzania danych w chmurze, co z kolei może przynieść daleko idące skutki społeczne. Efektywniejsze wykorzystanie zasobów informatycznych pomogłoby ograniczyć zużycie energii i emisję dwutlenku węgla o co najmniej 30 % netto. Małe przedsiębiorstwo przenoszące dane do chmury mogłoby zmniejszyć zużycie energii i emisję dwutlenku węgla o ponad 90 % dzięki obsłudze swoich aplikacji biznesowych w chmurze zamiast przy użyciu własnej infrastruktury. Oczekuje się, że do końca 2020 roku nastąpi wzrost globalnego rynku energooszczędnych ośrodków przetwarzania danych do niemal 90 mld euro. Rozdrobnienie rynku usług w zakresie danych spowolniłoby rozwój bardziej energooszczędnych usług w UE i ograniczyłoby skłonność do inwestowania.

Aby rozwiązać problemy i usunąć ograniczenia opisane powyżej oraz w pełni zrealizować potencjał europejskiej gospodarki opartej na danych, każde działanie państwa członkowskiego mające wpływ na przechowywanie lub przetwarzanie danych powinno być zgodne z **„zasadą swobodnego przepływu danych w Unii Europejskiej”**, będącą koniecznym następstwem zobowiązań państw członkowskich w ramach postanowień Traktatu i stosownych przepisów prawa wtórnego dotyczących swobodnego przepływu usług i swobody przedsiębiorczości. Każde dotychczasowe lub nowe ograniczenia w zakresie lokalizacji danych musiałyby znaleźć należyte uzasadnienie w Traktacie i stosownych przepisach prawa wtórnego, które wskazywałyby, że ich wprowadzenie jest niezbędne i proporcjonalne wobec nadrzędnego celu związanego z interesem ogólnym, np. bezpieczeństwa publicznego[19].

Zasada swobodnego przepływu danych osobowych[20] zagwarantowana przepisami prawa pierwotnego i wtórnego powinna także mieć zastosowanie w przypadkach gdy ogólne rozporządzenie o ochronie danych pozwala państwom członkowskim na uregulowanie poszczególnych kwestii. Państwa członkowskie powinny być zachęcane do tego, aby nie wykorzystywały klauzul otwartych w ogólnym rozporządzeniu o ochronie danych do dalszego ograniczania swobody przepływu danych.

---

18 „Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States” (Uwolnienie wewnętrznych przepływów danych w UE: ocena ekonomiczna działań związanych z lokalizacją danych w państwach członkowskich UE), ECIPE, 2016, obliczenia na podstawie zwiększonej presji konkurencyjnej powstałej na „przemysłowym” jednolitym rynku cyfrowym charakteryzującym się całkowitą przejrzystością cen.

19 Przy czym wyjątki określone w Traktacie należy interpretować w sposób zawężający. Wśród stosownych przepisów prawa wtórnego znajduje się ogólne rozporządzenie o ochronie danych, dyrektywa 2000/31/WE (dyrektywa o handlu elektronicznym), dyrektywa 2006/123/WE (dyrektywa usługowa) oraz, w odniesieniu do projektu przepisów technicznych i projektu zasad usług społeczeństwa informacyjnego, dyrektywa 2015/1535 (dyrektywa w sprawie przejrzystości).

20 Swoboda przepływu danych osobowych zawiera się w postanowieniach art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, a zasady swobodnego przepływu danych osobowych określają obecne i przyszłe przepisy prawa unijnego w zakresie ochrony danych. Art. 1 ust. 3 ogólnego rozporządzenia o ochronie danych stanowi: „Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych”.

W konkluzjach z dnia 15 grudnia 2016 r. Rada Europejska wezwała do usunięcia pozostałych przeszkód w obrębie jednolitego rynku, w tym utrudnień swobodnego przepływu danych.[21]

W celu urzeczywistnienia zasady swobodnego przepływu danych Komisja podejmie następujące dwa kroki:

- Po opublikowaniu niniejszego komunikatu, Komisja podejmie zorganizowany dialog z państwami członkowskimi i innymi zainteresowanymi stronami na temat zasadności i proporcjonalności restrykcji w zakresie lokalizacji danych, przyjmując za punkt wyjścia ograniczenia zidentyfikowane dotychczas przez Komisję.

- W następstwie dialogu i dalszego dokumentowania zakresu i charakteru ograniczeń lokalizacji danych oraz ich wpływu, w szczególności na MŚP i przedsiębiorstwa typu start-up, m.in. w drodze równoległych konsultacji społecznych, Komisja w razie potrzeby zainicjuje postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego, wzywając do usunięcia nieuzasadnionych lub nieproporcjonalnych restrykcji w zakresie lokalizacji danych, a w razie konieczności może również podjąć dalsze inicjatywy w odniesieniu do swobodnego przepływu danych. W tym odniesieniu do tych kwestii wszelkie działania następcze zostaną podjęte zgodnie z zasadami lepszego stanowienia prawa.

3. DOSTĘP DO DANYCH I ICH PRZEKAZYWANIE

Coraz większa ilość danych jest tworzona przez maszyny lub procesy oparte na nowych technologiach, takich jak Internet rzeczy. Tego rodzaju dane są coraz częściej wykorzystywane jako kluczowy komponent nowych, innowacyjnych usług do udoskonalenia produktów lub procesów produkcyjnych i wspierania procesu decyzyjnego.

Różnorodność danych generowanych przez maszyny lub procesy stwarza dla uczestników rynku danych ogromne możliwości innowacji i analizowania tych danych. Na przykład dane rejestrowane przez czujniki używane w nowoczesnych gospodarstwach rolnych mogłyby zostać wykorzystane do stworzenia aplikacji optymalizującej zbiory, a dane z czujników w sygnalizatorach świetlnych mogłyby posłużyć do stworzenia aplikacji do zarządzania ruchem ulicznym lub optymalizacji tras przejazdu.

Aby w maksymalnym stopniu wykorzystywać tego rodzaju dane, uczestnicy rynku muszą mieć dostęp do dużych i różnorodnych zbiorów danych. Staje się to jednak trudniejsze, jeśli dane pozostają u ich generatora i w rezultacie są analizowane w tzw. silosie informacyjnym. Dlatego kwestie dostępu i przekazywania danych surowych (tj. danych, które nie były przetwarzane ani zmieniane od chwili ich zarejestrowania) generowanych przez wspomniane maszyny i procesy mają zasadnicze znaczenie dla ukształtowania się gospodarki opartej na danych i wymagają uważnej oceny.

[21] http://www.consilium.europa.eu/eu/en/press-releases/2016/12/15-euro-conclusions-final/

Kwestia dostępu do danych generowanych maszynowo omawiana jest w odniesieniu do szeregu sektorów, takich jak transport, rynki energetyczne, technologia smart living oraz sektor opieki i ochrony zdrowia.

Przed dokonaniem oceny obecnej sytuacji pod kątem dostępu do danych w UE należy ustalić, jakiego rodzaju dane są rozpatrywane w tym kontekście.

3.1. Rodzaj przedmiotowych danych

Ogólnie rzecz ujmując, dane można podzielić na osobowe i nieosobowe. Na przykład dane generowane przez domowe czujniki temperatury mogą mieć charakter osobowy, jeśli można przyporządkować je do danej osoby, natomiast dane dotyczące wilgotności gleby nie mają charakteru osobowego. Dane osobowe można przekształcić w dane nieosobowe w procesie anonimizacji. Jeśli dane uznawane są za osobowe[22], zastosowanie mają ramy prawne w zakresie ochrony danych, w szczególności ogólne rozporządzenie o ochronie danych.

Dane generowane maszynowo powstają bez bezpośredniego udziału człowieka poprzez procesy, aplikacje lub usługi komputerowe bądź czujniki przetwarzające informacje dostarczane przez wirtualne lub fizyczne urządzenia, oprogramowanie lub maszyny.

Dane generowane maszynowo mogą mieć charakter osobowy lub nieosobowy. Jeśli dane generowane maszynowo umożliwiają ustalenie tożsamości osoby fizycznej, uznawane są za osobowe, w następstwie czego wszystkie zasady dotyczące danych osobowych dopóty mają zastosowanie, dopóki dane nie zostaną całkowicie zanonimizowane (np. dane dotyczące lokalizacji z aplikacji mobilnych).

Motywem łączącym swobodę przepływu danych i pojawiające się kwestie dostępu do danych i ich przekazywania jest fakt, że przedsiębiorstwa i podmioty gospodarki opartej na danych mają styczność z danymi zarówno osobowymi, jak i nieosobowymi, oraz że w przepływie danych i zbiorach danych występują obydwa rodzaje. Każde działanie w ramach polityki musi uwzględniać tę rzeczywistość ekonomiczną i ramy prawne dotyczące ochrony danych osobowych przy jednoczesnym poszanowaniu podstawowych praw jednostek.

3.2. Ograniczony dostęp do danych

Aby ocenić kształtującą się sytuację, należy najpierw przeanalizować, w jaki sposób przedsiębiorstwa i inni uczestnicy rynku mogą uzyskać dostęp do dużych i różnorodnych zbiorów danych niezbędnych w gospodarce opartej na danych.

Według dostępnych źródeł[23] przedsiębiorstwa dysponujące dużą ilością danych na ogół wykorzystują głównie własne zasoby analityczne. W większości przypadków dane

22 Zgodnie z art. 4 ust. 1 ogólnego rozporządzenia o ochronie danych.

23 IDC, European Data Market Study (Badanie europejskiego rynku danych), pierwsze sprawozdanie okresowe, 2016; Impact Assessment support study on emerging issues of data ownership, interoperability, (re)usability and access to data, and liability, (Badanie wspomagające ocenę skutków dotyczące pojawiających się kwestii własności danych, interoperacyjności, ich wykorzystywania i ponownego wykorzystywania oraz dostępu do

generuje i analizuje to samo przedsiębiorstwo, a nawet jeśli analiza danych zlecana jest podwykonawcy, dalsze ponowne wykorzystanie danych może nie mieć miejsca. Ponadto niekiedy producenci, usługodawcy i inni uczestnicy rynku dysponujący danymi zachowują dane wygenerowane przez własne maszyny lub poprzez własne produkty i usługi dla siebie, tym samym potencjalnie ograniczając ich dalsze wykorzystanie na rynkach niższego szczebla. Wiele przedsiębiorstw nie korzysta ani nie przewiduje możliwości korzystania z łatwych w obsłudze interfejsów programowania aplikacji (Application Programming Interface, API)[24] (które określają właściwy sposób interakcji między różnymi aplikacjami), mogących służyć jako bezpieczny punkt początkowy dla nowych i innowacyjnych zastosowań danych, którymi dysponują przedsiębiorstwa.

Dlatego też zakres wymiany danych pozostaje obecnie ograniczony. Rynki danych kształtują się powoli, ale nie są zbyt rozpowszechnione. Przedsiębiorstwom może brakować odpowiednich narzędzi i umiejętności potrzebnych do zmierzenia wartości ekonomicznej posiadanych przez nie danych i mogą one obawiać się utraty lub zmniejszenia swojej przewagi konkurencyjnej w chwili udostępnienia danych konkurentom.

3.3. Surowe dane generowane maszynowo: sytuacja prawna na poziomie unijnym i krajowym

Surowe dane generowane maszynowo nie podlegają ochronie na podstawie obowiązujących praw własności intelektualnej, ponieważ nie są uznawane za wynik wysiłku intelektualnego ani oryginalny utwór. Prawo *sui generis* ustanowione dyrektywą w sprawie ochrony prawnej baz danych (96/9/WE) – na podstawie którego twórcy baz danych mogą uniemożliwić ekstrakcję i ponowne wykorzystanie całości lub znaczącej części bazy danych – może zapewniać ochronę jedynie pod warunkiem, że stworzenie takiej bazy danych wymaga znaczących inwestycji w w celu uzyskania, weryfikacji lub prezentacji jej zawartości. W niedawno przyjętej dyrektywie w sprawie ochrony tajemnic przedsiębiorstwa (2016/943/UE), której transpozycja do prawa krajowego ma nastąpić do czerwca 2018 r., przewiduje się ochronę tajemnic przedsiębiorstwa przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem. Aby dane zostały uznane za „tajemnicę przedsiębiorstwa", należy podjąć środki w celu ochrony tajemnicy informacji stanowiącej „kapitał intelektualny przedsiębiorstwa".

Na podstawie przepisów prawa różnych państw członkowskich roszczenia prawne w przypadku danych powstają wyłącznie w sytuacji gdy dane te spełniają określone warunki pozwalające na uznanie prawa własności intelektualnej, prawa do bazy danych bądź tajemnicy przedsiębiorstwa. Jednak na szczeblu unijnym surowe dane generowane maszynowo na ogół nie spełniają odnośnych kryteriów.

Obecnie ani na poziomie krajowym, ani unijnym nie istnieją zatem całościowe ramy polityki w zakresie surowych danych generowanych maszynowo i nieuznawanych za dane osobowe oraz warunków ich ekonomicznego wykorzystania i wymiany handlowej.

---

danych i odpowiedzialności), pierwsze sprawozdanie okresowe, 2016; konferencja wysokiego szczebla DG ds. Sieci Komunikacyjnych, Treści i Technologii, 17 października 2016 r.

[24] Zob. na przykład https://developer.lufthansa.com/; https://data.sncf.com/api; https://api.tfl.gov.uk/; https://dev.blablacar.com/

Kwestia ta pozostawiona jest w znacznej mierze rozwiązaniom umownym. Zastosowanie obowiązującego ogólnego prawa zobowiązań i dostępnych w Unii instrumentów prawa w zakresie konkurencji mogłoby być wystarczającą odpowiedzią. Ponadto możliwe byłoby wprowadzenie dobrowolnych lub ramowych umów obejmujących określone sektory. Mimo to w przypadku nierównej pozycji negocjacyjnej różnych uczestników rynku rozwiązania czysto rynkowe mogą nie wystarczyć do zapewnienia uczciwych warunków sprzyjających innowacjom, ułatwienia wejścia na rynek nowym podmiotom i uniknięcia uzależnienia od jednego dostawcy.

3.4. Sytuacja w praktyce

W niektórych przypadkach producenci lub dostawcy usług mogą stać się faktycznymi „właścicielami" danych wygenerowanych przez ich maszyny lub procesy, nawet jeśli właścicielem maszyn jest użytkownik. Faktyczna kontrola nad danymi może stanowić źródło zróżnicowania i przewagi konkurencyjnej producenta. Może to jednak powodować problemy, ponieważ producent często uniemożliwia użytkownikowi autoryzację użycia danych przez osobę trzecią.

Różni uczestnicy rynku, którzy kontrolują dane, w zależności od specyfiki danego rynku, mogą zatem wykorzystywać luki prawne lub wątpliwości natury prawnej opisane powyżej, narzucając użytkownikom niesprawiedliwe standardowe warunki umów lub stosując środki techniczne, takie jak formaty zamknięte lub szyfrowanie. Chociaż niektóre państwa członkowskie rozszerzyły zakres stosowania ochrony konsumentów przewidziany w dyrektywie w sprawie nieuczciwych warunków w umowach konsumenckich na transakcje typu B2B, inne tego nie uczyniły. W rezultacie użytkownicy i przedsiębiorcy mogą na przykład być zmuszani do podpisywania umów o użyciu danych na zasadzie wyłączności. Porozumienia o dobrowolnym udostępnianiu danych byłyby możliwe, ale ich wynegocjowanie wiązałoby się ze znaczącymi kosztami transakcyjnymi po stronie słabszych podmiotów w przypadku nierównej pozycji negocjacyjnej lub ze względu na wysokie koszty porady prawnej.

3.5. Przyszłe unijne ramy prawne w zakresie dostępu do danych

Możliwość zapewnienia dostępu do danych generowanych maszynowo badają obecnie niektóre państwa członkowskie, które mogą zdecydować się na samodzielne uregulowanie tej kwestii. Brak skoordynowanego podejścia rodzi ryzyko rozdrobnienia i zaszkodziłby rozwojowi unijnej gospodarki opartej na danych i realizacji transgranicznych usług i technologii w zakresie danych na rynku wewnętrznym.

Dlatego Komisja zamierza podjąć dialog z państwami członkowskimi i innymi zainteresowanymi stronami w celu przeanalizowania możliwości utworzenia unijnych ram prawnych w zakresie dostępu do danych. W opinii Komisji dialog ten powinien koncentrować się na najskuteczniejszych sposobach osiągnięcia następujących celów:

- **Zwiększenie dostępu do anonimowych danych generowanych maszynowo:** W wyniku udostępniania, ponownego wykorzystywania i agregowania dane

generowane maszynowo stają się źródłem tworzenia wartości, innowacji i różnorodności modeli biznesowych[25].

- **Ułatwianie i nagradzanie procesu udostępniania danych:** Wszelkie przyszłe rozwiązania powinny sprzyjać efektywnemu dostępowi do danych, uwzględniając na przykład możliwe różnice w sile przetargowej między uczestnikami rynku.

- **Ochrona inwestycji i aktywów:** Wszelkie przyszłe rozwiązania powinny także uwzględniać zasadny interes uczestników rynku inwestujących w opracowanie produktu, zapewniać sprawiedliwy zwrot z inwestycji i tym samym wspierać innowacyjność. Jednocześnie powinny również zapewnić sprawiedliwy podział korzyści między posiadaczy danych[26], podmioty przetwarzające dane i dostawców aplikacji w obrębie łańcuchów wartości.

- **Zapobieganie ujawnianiu danych poufnych:** Wszelkie przyszłe rozwiązania powinny ograniczać ryzyko ujawnienia informacji poufnych, w szczególności istniejącym lub potencjalnym konkurentom. W tym kontekście powinny także umożliwić odpowiednią klasyfikację danych przed dokonaniem oceny, czy określone dane mogą zostać udostępnione.

- **Ograniczenie efektów „lock-in”:** Należy uwzględnić także nierówną siłę przetargową przedsiębiorstw i osób prywatnych. Należy unikać sytuacji uzależnienia od jednego dostawcy, zwłaszcza w przypadku MŚP i osób prywatnych.

Podejmując dialog z zainteresowanymi stronami, Komisja zamierza omówić następujące możliwości rozwiązania problemu dostępu do danych generowanych maszynowo, które różnią się między sobą poziomem działania:

- **Wytyczne dotyczące środków zachęty przedsiębiorstw do udostępniania danych:** Aby ograniczyć skutki obowiązywania odmiennych przepisów krajowych i zapewnić większą pewność prawa przedsiębiorstwom, Komisja mogłaby wydać wytyczne dotyczące sposobu, w jaki prawa kontroli danych nieosobowych powinny być formułowane w umowach. Wytyczne byłyby oparte na obowiązujących przepisach, w szczególności wymogach dotyczących przejrzystości i uczciwości określonych w prawie marketingowym i konsumenckim UE, dyrektywie w sprawie ochrony tajemnic przedsiębiorstwa i przepisach prawa autorskiego, zwłaszcza dyrektywie w sprawie ochrony prawnej baz danych. Komisja zamierza zainicjować ocenę dyrektywy w sprawie ochrony prawnej baz danych w 2017 roku.

- **Wsparcie procesu opracowania rozwiązań technicznych umożliwiających rzetelną identyfikację i wymianę danych:** Możliwość wyraźnej identyfikacji źródeł danych stanowi niezbędny warunek rzeczywistej kontroli danych na rynku. Określenie wiarygodnych i możliwie znormalizowanych protokołów trwałej identyfikacji źródeł danych może okazać się niezbędne, aby wzbudzić zaufanie

[25] W przypadku danych osobowych zastosowanie ma ogólne rozporządzenie o ochronie danych.

[26] Podmiot zarządzający i zachowujący dane generowane maszynowo w praktyce.

do systemu. Także interfejsy programowania aplikacji (API) mogą pomóc w stworzeniu ekosystemu deweloperów aplikacji i algorytmów zainteresowanych danymi, którymi dysponują przedsiębiorstwa. Interfejsy programowania aplikacji mogą ułatwić przedsiębiorstwom i organom publicznym identyfikację różnych rodzajów ponownego wykorzystania danych, którymi dysponują, a także czerpanie z nich korzyści. Na tej podstawie można byłoby przeanalizować możliwość szerszego wykorzystania otwartych, znormalizowanych i odpowiednio udokumentowanych interfejsów programowania aplikacji poprzez wytyczne techniczne, w tym określenie i rozpowszechnienie najlepszych praktyk dla przedsiębiorstw i organów sektora publicznego. Rozwiązanie mogłoby obejmować tworzenie danych dostępnych w formatach nadających się do odczytu maszynowego i dostarczanie powiązanych z nimi metadanych.

- **Standardowe postanowienia umowne:** Standardowe zasady opisywałyby wzorcowe zapisy umowne dotyczące danych, z należytym uwzględnieniem trwającej kontroli sprawności ogólnego funkcjonowania dyrektywy w sprawie nieuczciwych warunków w umowach konsumenckich. Mogłoby im towarzyszyć wprowadzenie kontroli uczciwości stosunków umownych B2B[27], w wyniku których zostałyby unieważnione zapisy umowne zanadto odbiegające od standardowych. Mogłyby także zostać uzupełnione zbiorem zalecanych standardowych warunków umownych opracowanych przez zainteresowane strony. Powyższe rozwiązania mogłyby ograniczyć bariery prawne dla małych przedsiębiorstw i zmniejszyć nierówności w pozycji negocjacyjnej, wciąż zapewniając jednak znaczną swobodę umów.

- **Dostęp do danych w interesie publicznym i w celach naukowych:** Organy publiczne otrzymywałyby dostęp do danych, jeśli byłoby to podyktowane „interesem ogólnym” i znacząco ułatwiłoby działanie sektora publicznego, na przykład dostęp urzędów statystycznych do danych biznesowych czy optymalizacja systemów zarządzania ruchem drogowym na podstawie danych dostarczanych z samochodów osobowych w czasie rzeczywistym. Dostęp urzędów statystycznych do danych biznesowych najprawdopodobniej przyczyniłby się do zwolnienia podmiotów gospodarczych z obowiązku składania sprawozdań statystycznych. Podobnie dostęp do danych z różnych źródeł i możliwość ich łączenia ma zasadnicze znaczenie w badaniach naukowych w dziedzinach takich jak medycyna, nauki społeczne i nauki o środowisku.

- **Prawo producenta danych:** Prawo do używania i zezwalania na użycie danych nieosobowych mogłoby zostać przyznane „producentowi danych”, tj. właścicielowi lub długotrwałemu użytkownikowi (tj. najemcy) urządzenia. Celem takiego rozwiązania byłoby wyjaśnienie sytuacji prawnej i zapewnienie producentowi danych większego wyboru, umożliwiając użytkownikom wykorzystanie ich danych i tym samym uwolnienie danych generowanych maszynowo. Mimo to należałoby jasno określić stosowne wyjątki, w szczególności udzielenie niewyłącznego dostępu do danych producentowi lub organom publicznym, na przykład do zarządzania ruchem drogowym lub w celu ochrony środowiska. W przypadku danych osobowych zachowane zostanie prawo

[27]. Oczywiście należałoby wyznaczyć inne referencyjne poziomy nieuczciwości dla umów B2B i B2C, uwzględniając wyższy stopień swobody umów w stosunkach typu B2B.

osób fizycznych do wycofania zgody w dowolnym momencie po zezwoleniu na użycie danych. Dane osobowe musiałyby zostać zanonimizowane w taki sposób, aby ustalenie tożsamości osoby było niemożliwe, zanim możliwe byłoby zezwolenie na dalsze wykorzystywanie danych przez osobę trzecią. Ogólne rozporządzenie o ochronie danych w dalszym ciągu ma zastosowanie do wszelkich danych osobowych (nie tylko generowanych maszynowo) przed poddaniem ich anonimizacji.

- **Dostęp w zamian za wynagrodzenie:** Możliwe byłoby opracowanie ram prawnych potencjalnie opartych na pewnych kluczowych zasadach, na przykład na sprawiedliwych, rozsądnych i niedyskryminujących warunkach (FRAND), dla podmiotów dysponujących danymi, takich jak producenci, dostawcy usług i inne podmioty, aby umożliwić dostęp w zamian za wynagrodzenie do tych danych po poddaniu ich anonimizacji. Należałoby uwzględnić przy tym zasadny interes tych podmiotów, jak również konieczność ochrony tajemnic przedsiębiorstwa. Przydatne byłoby także opracowanie różnych zasad dostępu dla różnych sektorów lub modeli biznesowych w celu uwzględnienia specyfiki poszczególnych branż. Na przykład w niektórych przypadkach pożądanym rozwiązaniem zarówno dla przedsiębiorstw, jak i społeczeństwa byłby powszechny dostęp do danych (pełny lub niepełny).

Komisja przeprowadzi konsultacje z zainteresowanymi stronami na tematy opisane powyżej w celu zgromadzenia większej ilości informacji na temat funkcjonowania rynków danych w poszczególnych sektorach i przeanalizowania możliwych rozwiązań. W związku z tym niezbędne jest przeprowadzenie szerokiej dyskusji na poziomie makro w celu omówienia możliwych rozwiązań i uniknięcia niezamierzonych skutków ubocznych, które zahamowałyby rozwój innowacji lub ograniczyły konkurencję. Ponadto z odpowiednimi zainteresowanymi stronami w ramach łańcucha wartości danych zostaną przeprowadzone dyskusje dotyczące poszczególnych sektorów.

4. ODPOWIEDZIALNOŚĆ

Kolejna kwestia dotyczy zastosowania obowiązujących obecnie zasad odpowiedzialności w gospodarce opartej na danych w odniesieniu do produktów i usług opartych na nowych technologiach, takich jak internet rzeczy, fabryki jutra bądź autonomiczne systemy połączone. Internet rzeczy to gwałtownie rozwijająca się sieć przedmiotów codziennego użytku, takich jak zegarki, pojazdy lub termostaty, które są połączone z internetem. Autonomiczne systemy połączone, takie jak pojazdy bezzałogowe, działają bez udziału człowieka i potrafią zrozumieć i interpretować otoczenie. Wspomniane nowe technologie wykorzystują czujniki rejestrujące wiele rodzajów danych często niezbędnych do działania produktu lub usługi.

Wszystkie powyższe innowacje prawdopodobnie przyczynią się do większego bezpieczeństwa i lepszej jakości życia, pozostaje jednak nieuchronne ryzyko błędów konstrukcyjnych, awarii lub dokonania manipulacji urządzenia. Przyczyną może być przesłanie błędnych danych przez czujnik, na przykład w wyniku wadliwego oprogramowania, problemów z łącznością bądź nieprawidłowego działania maszyny. Ze względu na charakter tych systemów precyzyjne ustalenie źródła problemu, który spowodował szkody, może nastręczać trudności, w związku z czym nasuwa się pytanie,

jak zagwarantować, że systemy te są bezpieczne dla użytkowników, tak aby ograniczyć występowanie szkód, oraz kogo należy obarczyć odpowiedzialnością za powstałą szkodę.

Dlatego kwestia ustalenia kryteriów odpowiedzialności, jasnych dla użytkowników i producentów wspomnianych urządzeń, ma kluczowe znaczenie dla ukształtowania się gospodarki opartej na danych.

4.1. Unijne zasady dotyczące odpowiedzialności

W prawie cywilnym rozróżniane są zasadniczo dwa rodzaje odpowiedzialności prawnej: umowna, w którym to przypadku odpowiedzialność za szkodę wynika ze stosunku umownego między stronami, oraz pozaumowna[28], w przypadku której odpowiedzialność powstaje poza stosunkiem umownym. Istotnym rodzajem odpowiedzialności pozaumownej jest odpowiedzialność za produkty wadliwe. Na szczeblu unijnym dyrektywa w sprawie odpowiedzialności za produkty wadliwe (85/374/EWG) ustanawia zasadę odpowiedzialności na zasadzie ryzyka: gdy konsument ponosi szkodę z tytułu wadliwego produktu, producent może ponosić odpowiedzialność nawet w przypadku braku winy lub zaniedbania z jego strony. Zastosowanie postanowień dyrektywy może stwarzać trudności lub wątpliwości[29] w odniesieniu do internetu rzeczy i autonomicznych systemów połączonych (np. robotyki) ze względu na: charakterystykę tych systemów, na przykład skomplikowany łańcuch wartości produktu lub usługi, pełny współzależności między dostawcami, producentami i osobami trzecimi; niepewność dotyczącą natury prawnej urządzeń internetu rzeczy, tj. czy należy uznać je za produkty, usługi czy produkty powstające w wyniku sprzedaży usługi; oraz autonomiczny charakter tych technologii.

Komisja zainicjowała szeroką ocenę dyrektywy w sprawie odpowiedzialności za produkty wadliwe w celu sprawdzenia jej ogólnego funkcjonowania i zweryfikowania, czy jej zasady, opracowane z myślą o zupełnie innym środowisku, znajdują zastosowanie w przypadku nowych technologii, takich jak internet rzeczy bądź autonomiczne systemy połączone.

4.2. Możliwe dalsze działania

Celem Komisji jest zwiększenie pewności prawa dotyczącego odpowiedzialności w odniesieniu do nowych technologii, a tym samym stworzenie warunków sprzyjających innowacyjności. Oprócz obecnych działań[30] można przeanalizować różne rozwiązania, między innymi:

---

[28] Unijne zasady odpowiedzialności dotyczą wyłącznie odpowiedzialności pozaumownej.

[29] Odniesienia do odpowiedzialności na zasadzie ryzyka w przypadku produktów wadliwych pojawiają się w aktach prawnych dotyczących bezpieczeństwa produktów, na przykład w dyrektywie dotyczącej udostępniania na rynku urządzeń radiowych (2014/53/UE), przepisach dotyczących urządzeń medycznych, dyrektywie w sprawie maszyn (2006/42/WE) i dyrektywie w sprawie ogólnego bezpieczeństwa produktów (2001/95/WE).

[30] Komisja mogłaby wydać wytyczne dotyczące zastosowania unijnych zasad odpowiedzialności w odniesieniu do internetu rzeczy i robotyki.

- **Rozwiązania odnoszące się do stwarzania ryzyka i zarządzania ryzykiem:** W ramach tych rozwiązań odpowiedzialność ponosiliby uczestnicy rynku stwarzający poważne ryzyko dla innych lub uczestnicy rynku, którzy mają największe możliwości ograniczenia lub uniknięcia ryzyka.

- **Dobrowolne lub obowiązkowe systemy ubezpieczeniowe:** Systemom tym mogłyby towarzyszyć wspomniane wyżej rozwiązania w zakresie odpowiedzialności. Wyrównywałyby one straty poniesione przez poszkodowane strony (np. konsumenta). Takie rozwiązanie musiałoby zapewniać ochronę prawną inwestycjom dokonanym przez przedsiębiorstwo przy jednoczesnej reasekuracji poszkodowanych w zakresie sprawiedliwego odszkodowania lub odpowiedniego ubezpieczenia w przypadku szkody.

Wszelkie rozwiązania musiałyby uwzględniać działania osoby wykorzystującej technologię i precyzyjniej określić rolę użytkowników wspomnianej technologii.

Komisja przeprowadzi konsultacje z zainteresowanymi stronami na temat adekwatności obecnie obowiązujących w UE zasad dotyczących odpowiedzialności w odniesieniu do internetu rzeczy i autonomicznych systemów połączonych, a także na temat możliwych rozwiązań w celu pokonania obecnych trudności w ustalaniu odpowiedzialności. Równolegle prowadzone są konsultacje społeczne na temat ogólnej oceny zastosowania dyrektywy w sprawie odpowiedzialności za produkty wadliwe. Komisja oceni wyniki i rozważy możliwe drogi działania.

5. MOŻLIWOŚĆ PRZENOSZENIA, INTEROPERACYJNOŚĆ I NORMY

Inne kwestie wyłaniające się w gospodarce opartej na danych dotyczą możliwości przenoszenia danych nieosobowych, interoperacyjności usług w celu umożliwienia wymiany danych oraz odpowiednich norm technicznych umożliwiających przenoszenie danych.

5.1. Możliwość przenoszenia danych nieosobowych

Możliwość przenoszenia danych oznacza, że konsumenci i przedsiębiorcy mogą bez problemu przenosić swoje dane między systemami. Zasadniczo wiąże się to z niskimi kosztami dostosowawczymi, a tym samym z niewielkimi barierami wejścia, w obszarze gospodarki opartej na danych. Ogólne rozporządzenie o ochronie danych nadaje osobom fizycznym prawo do otrzymywania danych osobowych dostarczonych dostawcy usług w uporządkowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, a także prawo do przesłania ich innemu dostawcy[31].

Jeśli chodzi jednak o dane nieosobowe, obecnie nie istnieją żadne zobowiązania pozwalające zagwarantować choćby w minimalnym stopniu możliwość przenoszenia danych, nawet w przypadku rozpowszechnionych usług online, takich jak hosting w chmurze. Wynika to częściowo z tego, że wprowadzenie możliwości przenoszenia danych może nastręczać trudności technicznych i wiązać się z dużymi kosztami,

[31] Art. 20.

ponieważ różni dostawcy tego samego rodzaju usług mogą przechowywać dane w różny sposób.

Aby przenoszenie danych nieosobowych odbywało się w rozsądny sposób, należałoby także uwzględnić szeroko pojęte kwestie zarządzania danymi, w tym przejrzystość dla użytkowników, kontrolę dostępu i interoperacyjność, co umożliwiłoby połączenie różnych platform w sposób pobudzający innowacyjność.

5.2. Interoperacyjność

Kwestie możliwości przenoszenia danych są często blisko powiązane z interoperacyjnością danych, która umożliwia wielu usługom cyfrowym płynną wymianę danych, ułatwioną dzięki odpowiednim specyfikacjom technicznym. Dyrektywa w sprawie informacji sektora publicznego i powiązane z nią wytyczne (w tym europejskie ramy interoperacyjności) podkreślają znaczenie zgodności obszernych, zorganizowanych metadanych z przyjętymi słownikami w celu ułatwienia wyszukiwania i interoperacyjności. Dyrektywa ustanawiająca infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE) oraz jej rozporządzenia w zakresie interoperacyjności i wytyczne dotyczące usług w zakresie danych przestrzennych i danych, w tym danych obserwacyjnych pozyskiwanych przez czujniki, obecnie mają zastosowanie do danych przestrzennych sektora publicznego[32].

W przypadku platform internetowych interoperacyjność danych ułatwia nie tylko zmianę, ale także jednoczesne wykorzystanie wielu platform (tzw. *multi-homing*) oraz szeroką wymianę danych pomiędzy platformami, co może przyczynić się do większej innowacyjności gospodarki cyfrowej.

5.3. Normy

Skutecznym zasadom w zakresie możliwości przenoszenia danych muszą towarzyszyć odpowiednie normy techniczne umożliwiające w znaczący sposób technologicznie neutralne przenoszenie danych. Komisja zobowiązała się[33] do poparcia odpowiednich norm w celu zwiększenia interoperacyjności, możliwości przenoszenia danych i bezpieczeństwa usług w chmurze poprzez skuteczniejsze włączenie prac ruchu na rzecz swobodnego dostępu do oprogramowania w proces ustanawiania norm na szczeblu europejskim. Przykłady takiego podejścia obejmują specyfikację TOSCA dla aplikacji do przechowywania w chmurze, mającą na celu zwiększenie możliwości przenoszenia i zarządzania operacyjnego w odniesieniu do aplikacji i usług w chmurze[34], a także specyfikacje techniczne i wytyczne rozporządzeń wykonawczych INSPIRE[35].

[32] Dane generowane maszynowo stanowią „dane przestrzenne”, ponieważ czujniki zazwyczaj przesyłają także ich bezpośrednią lub pośrednią pozycję (lokalizację).

[33] COM(2016) 176 final: Priorytety w normalizacji ICT na jednolitym rynku cyfrowym.

[34] https://www.oasis-open.org/committees/tosca

[35] Przepisy związane z dyrektywą INSPIRE: http://inspire.ec.europa.eu/inspire-legislation/26

5.4. Możliwe dalsze działania

Możliwe dalsze działania w celu rozwiązania powyższych kwestii obejmują:

- **Opracowanie zaleceń dotyczących warunków umów ułatwiających zmianę dostawców usług:** Ponieważ możliwość przenoszenia danych i zmiana dostawców usług w zakresie danych są wzajemnie powiązane, można rozważyć opracowanie standardowych warunków umownych zobowiązujących dostawcę usług do zapewnienia możliwości przeniesienia danych klienta.

- **Opracowanie dodatkowych praw do przenoszenia danych:** Na podstawie prawa do przenoszenia danych, określonego w ogólnym rozporządzeniu o ochronie danych, i proponowanych zasad dotyczących umowy o dostarczaniu treści cyfrowych, można wprowadzić dodatkowe prawa do przenoszenia danych nieosobowych, w szczególności obejmujące stosunki typu B2B, przy należytym uwzględnieniu wyników trwającej kontroli sprawności kluczowych przepisów prawa dotyczącego wprowadzania wyrobów na rynek oraz prawa konsumenckiego UE[36].

- **Doświadczenia dotyczące norm ograniczone do poszczególnych sektorów:** Aby wypracować zdrowe podejście do zasad przenoszenia danych utrwalonych poprzez normy, można zastosować metody doświadczalne ograniczone do poszczególnych sektorów. Zazwyczaj wiązałyby się one z udziałem wielu zainteresowanych stron, m.in. podmiotów ustanawiających normy, przedstawicieli branży, środowiska technicznego i organów publicznych.

Komisja przeprowadzi konsultacje dotyczące tych zagadnień z zainteresowanymi stronami i na tej podstawie ustali, czy dalsze działania są niezbędne, być może w formie działań opisanych powyżej, realizowanych pojedynczo lub w połączeniu.

6. DOŚWIADCZENIA I TESTY

Doświadczenia odgrywają ważną rolę w badaniu pojawiających się kwestii w gospodarce opartej na danych. Przeanalizowana zostanie możliwość wykorzystania funduszy programu „Horyzont 2020” do sfinansowania tego rodzaju prób i eksperymentów.

Przed wyciągnięciem wniosków na temat stosowności możliwych rozwiązań w zakresie dostępu do danych i odpowiedzialności należy zorganizować we współpracy z zainteresowanymi stronami odpowiednią próbę, która podda te zagadnienia weryfikacji w warunkach rzeczywistych. Potrzebne jest ogólnoeuropejskie rozwiązanie powstałe w oparciu o współpracę i doświadczenia państw członkowskich.

Taka próba mogłaby dotyczyć pojazdów współpracujących, połączonych i zautomatyzowanych[37], ze względu na transgraniczny wymiar tego sektora.

[36] http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm

[37] Zob. COM (2016) 766 z 30.11.2016 r.

W kilku państwach członkowskich trwają prace nad systemami współpracującymi i wyższymi poziomami automatyzacji[38]. Projekty te umożliwiają połączenie pojazdów ze sobą nawzajem i z elementami infrastruktury drogowej, takimi jak sygnalizacja świetlna lub znaki drogowe. Ponadto Komisja zamierza we współpracy z grupą zainteresowanych państw członkowskich stworzyć ramy prawne dotyczące przeprowadzania eksperymentów na podstawie zharmonizowanych zasad dostępu do danych i odpowiedzialności. Aby umożliwić dostęp do wystarczająco dużej objętości danych, próby powinny wykorzystywać sieć 5G współdziałającą płynnie z już rozmieszczonymi technologiami na zasadzie komplementarności[39].

Kolejne interesujące doświadczenie dotyczyć będzie sektora geoprzestrzennego w związku z kształtowaniem się nowego ekosystemu danych, tworzonego wokół unijnego programu obserwacji i monitorowania Ziemi Copernicus, trzeciego największego dostawcy danych na świecie. Komisja opracowuje innowacyjne rozwiązania w celu wsparcia rozwoju aplikacji opartych na programie Copernicus i innych danych przestrzennych, w szczególności w zakresie dostępu do danych, interoperacyjności i przewidywalności.

7. WNIOSKI

Aby zbudować gospodarkę opartą na danych, Unia Europejska potrzebuje ram polityki, które umożliwiłyby wykorzystywanie danych w obrębie całego łańcucha wartości w celach naukowych, społecznych i przemysłowych. W tym celu Komisja inicjuje dialog obejmujący szerokie grono interesariuszy, dotyczący kwestii poruszanych w niniejszym komunikacie. Pierwszy krok w procesie dialogu będą stanowiły konsultacje społeczne. Kwestie dostępu do danych i odpowiedzialności zostaną zweryfikowane w warunkach rzeczywistych w obszarze pojazdów współpracujących, połączonych i zautomatyzowanych.

Jeśli chodzi o swobodny przepływ danych, Komisja będzie kontynuowała prace nad tym zagadnieniem zgodnie z podejściem opisanym powyżej w celu pełnego wdrożenia zasady swobodnego przepływu danych na terytorium UE, również w ramach niezbędnych i stosownych akcji kontrolnych. Ponadto Komisja będzie w dalszym ciągu monitorowała i gromadziła informacje, w razie potrzeby podejmując dalsze inicjatywy w odniesieniu do swobodnego przepływu danych.

Na podstawie wyników dialogu z zainteresowanymi stronami Komisja zadecyduje także, czy konieczne będą dalsze działania w związku z przedstawionymi zagadnieniami i zaproponuje stosowne rozwiązania. W tym zakresie pewną rolę mogą odegrać doświadczenia w warunkach rzeczywistych.

[38] Zob. COM (2016) 766: Europejska strategia na rzecz współpracujących inteligentnych systemów transportowych.

[39] Zob. COM (2016) 588: Sieć 5G dla Europy: plan działania.