Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Zaufanie, prywatność i bezpieczeństwo konsumentów i przedsiębiorstw w internecie rzeczy”

(opinia z inicjatywy własnej)

(2018/C 440/02)

Sprawozdawca: **Carlos TRIAS PINTÓ**

Współsprawozdawca: **Dimitris DIMITRIADIS**

Decyzja Zgromadzenia Plenarnego	15.2.2018
Podstawa prawna	Art. 29 ust. 2 regulaminu wewnętrznego
	Opinia z inicjatywy własnej
Sekcja odpowiedzialna	Sekcja Jednolitego Rynku, Produkcji i Konsumpcji
Data przyjęcia przez sekcję	4.9.2018
Data przyjęcia na sesji plenarnej	19.9.2018
Sesja plenarna nr	537
Wynik głosowania	182/3/2
(za/przeciw/wstrzymało się)	

1. **Wnioski i zalecenia**

1.1. Internet rzeczy dzięki sieci wzajemnych połączeń osób i przedmiotów oferuje szeroki wachlarz możliwości dla obywateli i przedsiębiorstw. Musi temu jednak towarzyszyć szereg gwarancji i kontroli w celu zapewnienia harmonijnego wprowadzania internetu rzeczy.

1.2. Mając na uwadze, że jednym z filarów internetu rzeczy jest zasada podejmowania decyzji w sposób zautomatyzowany bez interwencji człowieka, należy dopilnować, by decyzje te nie naruszały praw konsumentów, nie wiązały się z żadnego rodzaju ryzykiem natury etycznej ani nie były sprzeczne z podstawowymi zasadami i prawami człowieka.

1.3. EKES apeluje do instytucji europejskich i państw członkowskich, aby:

1.3.1. czuwały nad ochroną bezpieczeństwa i prywatności poprzez opracowanie odpowiednich ram regulacyjnych obejmujących rygorystyczne środki monitorowania i kontroli;

1.3.2. jasno określiły odpowiedzialność wszystkich podmiotów w łańcuchu dostaw produktu oraz powiązane przepływy informacji, aby zapobiec lukom prawnym w wypadku, gdy w tym samym czasie zaangażowanych jest kilku producentów i dystrybutorów;

1.3.3. wprowadziły odpowiednie zasoby i skuteczne mechanizmy koordynacji między Komisją Europejską a państwami członkowskimi w celu zagwarantowania spójnego i zharmonizowanego stosowania zarówno przepisów poddawanych nowelizacji, jak i nowych regulacji, przy jednoczesnym uwzględnieniu kontekstu międzynarodowego;

1.3.4. monitorowały rozwój nowych technologii związanych z internetem rzeczy, by gwarantować wysoki poziom bezpieczeństwa, pełną przejrzystość i dostępność na sprawiedliwych zasadach;

1.3.5. promowały europejskie i międzynarodowe inicjatywy w zakresie normalizacji w celu zagwarantowania niezawodności, dostępności, odporności i utrzymania produktów;

1.3.6. sprawowały nadzór nad rynkami i zapewniły równe szanse dla wdrażania internetu rzeczy, unikając koncentracji transnarodowej siły gospodarczej w kontekście nowych podmiotów technologicznych;

1.3.7. zobowiązały się do promowania działań ukierunkowanych na uświadamianie i budowanie zdolności w zakresie kompetencji cyfrowych w połączeniu z podstawowymi badaniami naukowymi i innowacjami w tejże dziedzinie;

1.3.8. zapewniły pełne wdrożenie i skuteczne wykorzystywanie alternatywnych metod rozwiązywania sporów – zarówno w trybie offline, jak i online (ADR i ODR);

1.3.9. zapewniły istnienie, wdrożenie i sprawne funkcjonowanie europejskiego systemu roszczeń zbiorowych, który umożliwi wstrzymanie praktyk i uzyskanie odszkodowania także w wypadku, gdy korzystanie z internetu rzeczy powoduje szkody lub straty o charakterze zbiorowym – tego rodzaju możliwość przewidziana jest w nowym ładzie dla konsumentów.

1.4. Konsumenci będą nabierać zaufania do internetu rzeczy dzięki ścisłemu przestrzeganiu odnośnych przepisów oraz przekazywaniu informacji na temat najlepszych praktyk biznesowych w dziedzinie prywatności i bezpieczeństwa. Zatem zadaniem instytucji jest powiązanie tych praktyk z zasadą społecznej odpowiedzialności przedsiębiorstw oraz strategiami społecznie odpowiedzialnych inwestycji.

1.5. Pozytywne oddziaływanie internetu rzeczy pod względem społecznym i gospodarczym będzie rosło, w miarę jak będzie on w coraz większym stopniu odpowiednio powiązany z rozwojem polityki społeczno-środowiskowej w kontekście gospodarki współpracy, gospodarki o obiegu zamkniętym i gospodarki opartej na funkcjonalności.

2. **Tło i kontekst**

2.1. Gwałtowny rozwój internetu w ciągu ostatnich 15 lat jest przyczyną zmian w każdej dziedzinie życia codziennego i ma wpływ na różne nawyki konsumentów. Przewiduje się, że w ciągu najbliższych dziesięciu lat rewolucja, jaką jest internet rzeczy, obejmie swoim zasięgiem sektory energetyki, rolnictwa i hodowli zwierząt oraz transportu, a także dziedziny gospodarki i życia społecznego o bardziej tradycyjnym charakterze, co oznacza, że należy opracować zintegrowane strategie polityczne, które w inteligentny sposób podejmą kwestię tego przełomu technologicznego.

2.2. Zgodnie z koncepcją internetu rzeczy, która zrodziła się w Massachusetts Institute of Technology (MIT), świat mają wypełniać urządzenia całkowicie połączone między sobą w taki sposób, by mogły w zautomatyzowany sposób wspólnie przeprowadzać różne procesy interoperacyjne. Natomiast Unia Europejska przygotowuje się do zajęcia się konwergencją cyfrową i nowymi wyzwaniami związanymi z internetem rzeczy – począwszy od uruchomienia planu „i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia” ([1]) po niedawny plan działania w zakresie internetu rzeczy (zob. dokument pt. „Advancing the Internet of Things in Europe” towarzyszący komunikatowi z 2016 r. „Cyfryzacja europejskiego przemysłu. Pełne wykorzystanie możliwości jednolitego rynku cyfrowego” ([2])).

2.3. EKES wielokrotnie wypowiadał się na temat czwartej rewolucji przemysłowej, której oznaką jest konwergencja technologii cyfrowych, fizycznych i biologicznych. Zwraca tu zwłaszcza uwagę na opinię z 2017 r. ([3]) Internet rzeczy jest faktycznie obszarem, w którym z powodzeniem wykorzystuje się najbardziej zaawansowane formy sztucznej inteligencji i w którym wystawia się na próbę zasady określone przez EKES, zwłaszcza zasadę kontroli przez człowieka.

2.4. Urządzenia w internecie rzeczy często nie są objęte normami uwierzytelniania potrzebnymi do utrzymania bezpieczeństwa danych użytkownika. Może to prowadzić do problemów, ponieważ urządzenia, dane i podmioty należące do łańcucha dostaw są narażone na naruszenia bezpieczeństwa.

2.5. Wyłaniające się technologie takie jak łańcuch bloków mogą rozwiązać problemy w zakresie bezpieczeństwa i zaufania: można wykorzystywać je w celu śledzenia pomiarów danych pochodzących z czujników, nie tylko by zapobiegać powielaniu tych danych w złych zamiarach, ale również by zachować integralność i identyfikowalność zmian; technologia rozproszonego rejestru może pozwalać na identyfikację urządzeń w internecie rzeczy oraz bezpieczne i pozbawione błędów uwierzytelnianie i przesyłanie danych; czujniki w internecie rzeczy można wykorzystywać do wymiany danych za pośrednictwem łańcucha bloków zamiast podmiotów trzecich; wykorzystanie inteligentnych umów pozwala na autonomiczne działanie urządzeń oraz zachowanie indywidualnej tożsamości i integralności danych; zmniejsza się koszty tworzenia i funkcjonowania z powodu braku pośredników; ponadto urządzenia działające w internecie rzeczy w łańcuchu bloków dostarczają historię połączonych urządzeń, która jest bardzo przydatna do rozwiązywania ewentualnych problemów ([4]).

([1]) COM(2005) 229 final.
([2]) COM(2016) 180 final.
([3]) „Sztuczna inteligencja: wpływ sztucznej inteligencji na jednolity rynek (cyfrowy), produkcję, konsumpcję, zatrudnienie i społeczeństwo” (Dz.U. C 288 z 31.8.2017, s. 1).
([4]) Zob.: Khwaja Shaik, „Why blockchain and IoT are best friends”, https://www.ibm.com/us-en/?lnk=m; na temat innowacji w europejskim sektorze finansowym zob. Dz.U. C 246 z 28.7.2017, s. 8.

2.6. Z drugiej strony opracowuje się technologie rozproszonego rejestru na potrzeby wymiany informacji i wartości między urządzeniami w internecie rzeczy. Nie zezwalają one na eksplorację danych, lecz wykorzystują architekturę zainspirowaną pojęciem matematycznym, jakim jest skierowany graf acykliczny (DAG), która pozwala na uniknięcie prowizji oraz sprzyja zwiększaniu pojemności sieci odpowiednio do wzrostu liczby użytkowników.

2.7. Stoimy przed zjawiskiem o olbrzymim potencjale gospodarczym ([5]) i społecznym, które stwarza wielkie możliwości, ale również poważne zagrożenia związane z ukrytym ryzykiem, ma charakter multidyscyplinarny i przekrojowy i dotyczy w równym stopniu przedsiębiorstw i konsumentów oraz organów administracji i obywateli. W związku z tym zajmując się tą kwestią, należy przyjąć wspólne podejście, a jednocześnie zwracać uwagę na wszystkie aspekty charakterystyczne dla danych warunków. W tym kontekście wystarczy wspomnieć, że ONZ szacuje, że w 2020 r. 50 mld urządzeń będzie połączonych ze sobą za pomocą aplikacji konsumenckich w telewizorach, lodówkach, kamerach monitoringu, pojazdach itd.

2.8. Aplikacje internetu rzeczy przynoszą już korzyści gospodarcze i społeczne w zglobalizowanym świecie, co oznacza m.in. powstawanie usług w większym stopniu reagujących na warunki społeczno-gospodarcze, krótsze cykle sprzężenia zwrotnego, naprawy na odległość, wsparcie przy podejmowaniu decyzji, lepszy przydział zasobów czy zdalne sterowanie usługami. Jednocześnie występuje szereg powiązanych czynników o bardzo wrażliwym charakterze, takich jak: prywatność i bezpieczeństwo, asymetria informacji i przejrzystość transakcji, złożony charakter odpowiedzialności, blokowanie produktów i systemów oraz rozwój produktów hybrydowych, które mogą mieć wpływ na kwestie własności i narażać konsumentów na wykorzystywanie umów na odległość przy jednoczesnym osłabianiu gwarancji.

2.9. Istotne wyzwania natury prawnej dla UE i jej państw członkowskich wynikają z faktu, że wiele ze specyficznych cech internetu rzeczy (wysoki stopień złożoności i wzajemnych zależności, element autonomii, komponenty dotyczące generowania lub przetwarzania danych oraz wymiar otwarty) łączy się z innymi nowymi technologiami cyfrowymi, takimi jak łańcuch bloków, drukowanie przestrzenne i przetwarzanie w chmurze. Zdaniem EKES-u dokument roboczy służb Komisji ([6]) w sprawie odpowiedzialności za nowe technologie cyfrowe stanowi krok we właściwym kierunku.

2.10. Podsumowując, maksymalizacja korzyści i zminimalizowanie ryzyka w odniesieniu do internetu rzeczy wymagają dostarczania dostępnych, przejrzystych, zwięzłych i precyzyjnych informacji – w szczególności należy wspierać włączenie cyfrowe konsumentów najbardziej podatnych na zagrożenia i zapewnienie im łączności cyfrowej przez projektowanie w pełni identyfikowalnych produktów i usług objętych zintegrowanymi normami w zakresie zaufania, prywatności i bezpieczeństwa.

3. **Zaufanie konsumentów i przedsiębiorców do internetu rzeczy**

3.1. Internet rzeczy to złożony ekosystem pozwalający na łączenie między sobą urządzeń pochodzących od różnych producentów, dystrybutorów lub twórców oprogramowania, co może powodować trudności przy ustalaniu odpowiedzialności w sytuacji naruszenia przepisów lub wystąpienia szkód materialnych lub innych szkód wyrządzonych osobom trzecim bądź systemom spowodowanych przez wadliwe produkty lub przez produkty, które poprzez sieć zostały użyte niezgodnie z swym przeznaczeniem przez osoby trzecie, z wyłączeniem użytkowników końcowych. Możliwe jest również, że wielu z operatorów uczestniczących w globalnym łańcuchu wartości danego produktu nie posiada wystarczającej wiedzy i doświadczenia w zakresie bezpieczeństwa lub ochrony danych w odniesieniu do urządzeń w sieci.

3.2. W związku z tym konieczne jest nowe podejście do odpowiedzialności ukierunkowane na zagwarantowanie objęcia konsumentów i przedsiębiorstw pobierających aplikacje internetu rzeczy ochroną w środowisku, w którym prawidłowo skonfigurowane produkty mogą ulec uszkodzeniu lub stać się niebezpieczne w wyniku incydentów w zakresie bezpieczeństwa cyfrowego lub w wyniku ich niedozwolonego i niezgodnego z przeznaczeniem użycia (np. przez hakerów). Środowisko to powinno uprzedzać zautomatyzowane decyzje mogące zaszkodzić podstawom etycznym i powszechnie uznawanym prawom człowieka, zapobiegać im i chronić przed nimi.

([5]) Przedsiębiorstwo Digital McKinsey szacuje, że internet rzeczy może mieć skutki ekonomiczne o wartości rzędu 3,9–11,1 bln USD rocznie.

([6]) SWD(2018) 137.

3.3. Komitet przyjmuje z zadowoleniem przegląd stosowania dyrektywy z 1985 r. w sprawie odpowiedzialności za szkody spowodowane przez produkty wadliwe ([7]) oraz niedawne utworzenie wielostronnej grupy ekspertów ds. odpowiedzialności i nowych technologii w celu zagwarantowania należytej równowagi między interesami producentów i konsumentów. Nowe ramy odpowiedzialności powinny wyraźnie obejmować identyfikowalność odpowiedzialności i bezpieczeństwa zarówno w obrębie łańcucha wartości produktu, jak i podczas szacowanego cyklu eksploatacji, a także uwzględniać zrównoważoność jako nowy czynnik zobowiązujący do uaktualniania produktu, jego usprawniania i przenoszenia oraz zapewnienia jego kompatybilności, ponownego wykorzystania, naprawy lub dostosowania.

3.4. W kontekście internetu rzeczy należy również wziąć w szczególności pod uwagę ustalenie odpowiedzialności wszystkich podmiotów profesjonalnych w łańcuchu dostaw produktu i zapobiec lukom prawnym w przypadku współuczestnictwa różnych producentów i dystrybutorów. EKES uważa, że koniecznie należy jasno określić procedury przeznaczone do stosowania przez konsumentów w każdym przypadku, promując alternatywne metody rozwiązywania sporów (ADR).

3.5. EKES podkreśla znaczenie informacji przedkontraktowych, przejrzystych klauzul umownych i jasnych instrukcji obsługi urządzeń. Należy wyraźnie wskazać na możliwe powiązane ryzyko oraz zabezpieczenia.

3.6. Należy zapewnić interoperacyjność i kompatybilność urządzeń i powiązanego oprogramowania, aby zapobiec problemom i umożliwić konsumentom porównywanie dostawców. EKES podkreśla, że ma to kluczowe znaczenie również dla stworzenia równych szans dla dużych przedsiębiorstw i MŚP.

3.7. Komitet zaleca także poszanowanie neutralności sieci i wzywa Komisję do rygorystycznego monitorowania zachowań rynkowych.

4. **Prywatność konsumentów w internecie rzeczy**

4.1. Zdolność konsumentów do sprawdzenie ich danych osobowych i ustawień prywatności uległa poprawie wraz z nowym ogólnym rozporządzeniem o ochronie danych (RODO) ([8]). Użytkownik danego urządzenia powinien mieć kontrolę nad sposobem wykorzystania generowanych przez niego danych i uprawnieniami dostępu do nich, biorąc pod uwagę, że różnorodność danych oraz ich agregacja i powiązanie z innymi danymi stanowią poważne zagrożenie dla prywatności w ekosystemie internetu rzeczy.

4.2. Należy mieć na uwadze wpływ, jaki wielość produktów, usług i podmiotów może mieć na prywatność i na ochronę danych, gdy są one przesyłane w sposób niezależny w ramach wzajemnych połączeń. Podobnie w przypadku przetwarzania lub ponownego opracowania informacji na podstawie początkowo bezpiecznych danych można uzyskać szczegółową wiedzę na temat zwyczajów, lokalizacji, zainteresowań i preferencji jednostek, co zwiększa dostępność i możliwość śledzenia profilu użytkownika.

4.3. Należy za pomocą gwarancji prawnych zapewnić pełną zdolność użytkowników do korzystania z prawa do prywatności i ochrony danych osobowych bez jakichkolwiek ograniczeń, aby w ten sposób uniknąć potencjalnych szkód, takich jak praktyki dyskryminacyjne, natrętny marketing, utrata prywatności czy naruszanie bezpieczeństwa. Natomiast konsumenci muszą posiadać informacje na temat wartości gospodarczej ich danych i być w stanie zastrzec sobie prawo do udostępniania ich.

4.4. Zgodnie z RODO przedsiębiorstwa i organy regulacyjne powinny okresowo dokonywać przeglądu zakresu gromadzenia danych osobowych i oceniać, w jakim stopniu przetwarzane dane są proporcjonalne i konieczne do realizacji usługi. Aspekty i wpływ prywatności należy oceniać na każdym etapie opracowywania, projektowania i rozwoju połączonego produktu i ekosystemu sieciowego, w którym ten produkt funkcjonuje (uwzględnianie ochrony prywatności już w fazie projektowania). W związku z tym zasady ochrony prywatności w fazie projektowania oraz domyślnej ochrony prywatności muszą być systematycznie stosowane w internecie rzeczy.

4.5. Oznacza to, że należy ustalić wyjściowo konfigurację dowolnego połączonego produktu na najwyższym poziomie ochrony prywatności (w fazie projektowania i domyślnie), aby uniknąć niepożądanego śledzenia zachowania użytkowników i wykonywanych przez nich czynności.

([7]) COM(2018) 246 final.
([8]) Rozporządzenie obowiązuje od dnia 25 maja 2018 r.

4.6. W każdym przypadku konsumenci powinni posiadać wiarygodne informacje na temat gromadzonych danych, osób mających do nich dostęp i celu, do którego te dane mają być wykorzystywane w czasie interakcji z produktem lub usługą, a także na temat mającej zastosowanie polityki prywatności. Muszą też wiedzieć, czy zastosowane algorytmy mają wpływ na jakość usługi, jej cenę lub dostęp do niej.

5. **Bezpieczeństwo konsumentów i przedsiębiorców w internecie rzeczy**

5.1. Wzajemne połączenia urządzeń charakteryzujące ekosystem internetu rzeczy mogą pobudzać rozwój nielegalnych lub niepożądanych praktyk technologicznych, co uczyni z internetu rzeczy przestrzeń podatną na zagrożenia i na rozprzestrzenianie się tej słabości niczym wirusa. Dlatego należy zapewniać bezpieczeństwo w sposób zintegrowany w obrębie każdego z komponentów systemu.

5.2. Oferty produktów i aktualizacje powiązane z cyberbezpieczeństwem muszą być uzasadnione i nie tylko zapewniać ochronę poszczególnych urządzeń, lecz także uwzględniać ryzyko dla bezpieczeństwa wynikające z wzajemnych połączeń z innymi urządzeniami w internecie rzeczy, a normy jakości bezpieczeństwa nie mogą ulegać pogorszeniu wraz ze wzrostem liczby urządzeń.

5.3. W tym kontekście wniosek dotyczący rozporządzenia w sprawie Agencji UE ds. Cyberbezpieczeństwa ([9]) zawiera ramy certyfikacji technologii informacyjno-komunikacyjnych, co umożliwi zdefiniowanie dobrowolnych schematów certyfikacji bezpieczeństwa i etykietowania dla różnych rodzajów produktów, w tym produktów funkcjonujących w internecie rzeczy. Choć EKES z zadowoleniem przyjmuje wprowadzenie tego środka, wyraża ubolewanie, że nie jest on obowiązkowy.

5.4. Środki z zakresu cyberbezpieczeństwa powinny obejmować ryzyko związane z wszelkimi formami podatności na zagrożenia, w szczególności ryzyko hakowania, nieuprawnionego dostępu lub nieprawidłowego wykorzystania, a także ryzyko związane ze środkami płatniczymi i oszustwami finansowymi. W tym względzie EKES popiera uprawnienia nadane wielostronnej grupie ekspertów ds. odpowiedzialności i nowych technologii.

5.5. Należy również wziąć pod uwagę bezpieczeństwo osobiste konsumentów w związku z zagrożeniami takimi jak bliskość urządzeń, korzystanie ze wspólnych pasm częstotliwości, narażenie na pole elektromagnetyczne lub możliwe interferencje z połączonymi istotnymi urządzeniami. EKES apeluje, by stosować środki w zakresie nadzoru i zapobiegawczego wycofania z użytkowania w przypadku zagrożeń mających wpływ na zdrowie i bezpieczeństwo konsumentów lub ich interesy osobiste i finansowe.

5.6. Przedsiębiorstwa powinny przyjmować standardy najlepszych praktyk, takie jak uwzględnianie bezpieczeństwa w fazie projektowania i bezpieczeństwo domyślne, oraz poddawać się niezależnym ocenom zewnętrznym. W przypadku incydentów w zakresie bezpieczeństwa lub naruszeń danych przedsiębiorstwa będą miały obowiązek ich zgłaszania, łącznie z informacjami dotyczącymi odpowiedzialności za szkody i niewykonania zobowiązań wynikających z przepisów.

5.7. Przedsiębiorstwa muszą udzielać konsumentom prostych i dostępnych informacji, które umożliwią im podejmowanie odpowiednich decyzji i stosowanie bezpiecznych praktyk. Trzeba także zapewnić niezbędne aktualizacje dotyczące bezpieczeństwa przez cały cykl życia produktu.

5.8. Należy zająć się kwestią braku spójnych norm dotyczących sieci w internecie rzeczy. Konieczne jest rozwijanie zaawansowanych technologii szerokopasmowych i technologii nowej generacji w celu ulepszenia obecnej infrastruktury.

6. **Propozycje działań w ramach polityki publicznej** ([10])

6.1. Organy publiczne wykonujące swoje zadania na różnych obszarach Unii Europejskiej muszą aktywnie uczestniczyć w opracowywaniu strategii politycznych i planów działania w zakresie internetu rzeczy w celu osiągnięcia równowagi interesów poszczególnych zainteresowanych stron, a także przewidywać problemy i przeciwdziałać możliwym szkodliwym skutkom. EKES proponuje, aby:

6.1.1. tworzyć środowiska testowe (tzw. piaskownice), czyli fizyczne przestrzenie, klastry itp. do celów przeprowadzania projektów pilotażowych i prób koncepcyjnych; ich celem powinno być testowanie nie tylko technologii, ale również modelów regulacji ([11]);

([9]) Zob. COM(2017) 477 final.
([10]) Zob. Grupa Banku Światowego, „Internet of Things: The New Government-to-Business Platform".
([11]) Zob. https://ec.europa.eu/digital-single-market/en/news/eu-and-eea-member-states-sign-cross-border-experiments-cooperative-connected-and-automated.

6.1.2. finansować infrastrukturę technologiczną umożliwiającą rozwój innowacyjnych projektów dotyczących internetu rzeczy w ramach nowego programu „Horyzont Europa";

6.1.3. wyznaczać niezależne instytuty i agencje jako podmioty ułatwiające i nadzorujące realizowanie projektów z dziedziny internetu rzeczy; EKES przyjmuje z zadowoleniem środki przyjęte w tej dziedzinie w rozporządzeniu z 2017 r. w sprawie cyberbezpieczeństwa i wzywa Komisję, by skutecznie wspierała procesy standaryzacji w branży cyfrowej za pomocą odpowiednich środków budżetowych ([12]);

6.1.4. pobudzać platformy współpracy publiczno-prywatnej oraz partnerstwa angażujące społeczność naukową, przemysł i konsumentów;

6.1.5. zachęcać do inwestowania w rozwój lokalnych modeli biznesowych czerpiących korzyści z internetu rzeczy i ułatwiać zajmowanie się tak skomplikowanymi kwestiami jak ochrona i własność danych;

6.1.6. przeprowadzać działania z zakresu budowania zdolności w środowisku biznesowym w kontekście współodpowiedzialności; należy zagwarantować, aby uwzględnianie bezpieczeństwa i ochrony prywatności w fazie projektowania i domyślnie miało zastosowanie do produktów i usług technologii informacyjno-komunikacyjnych zgodnie z zasadą tzw. należytej staranności, zalecanej w nowym rozporządzeniu w sprawie cyberbezpieczeństwa; w związku z tym EKES z zadowoleniem przyjmuje planowane opracowanie **kodeksów postępowania** w celu uzupełnienia rozporządzenia;

6.1.7. promować europejskie i międzynarodowe inicjatywy w dziedzinie standaryzacji w celu zagwarantowania, że systemy internetu rzeczy będą posiadały najważniejsze cechy, czyli niezawodność, bezpieczeństwo, dostępność, odporność, możliwość utrzymania i użyteczność; szczególnie istotna jest standaryzacja w celu szybkiej realizacji procesów produkcji przemysłowej o wysokim poziomie cyfryzacji;

6.1.8. zapewnić użytkownikom internetu rzeczy, zwłaszcza najsłabszym grupom czy osobom mieszkającym na obszarach słabo zaludnionych, przystępny cenowo dostęp wysokiej jakości;

6.1.9. promować programy uświadamiające i edukacyjne w celu ułatwienia korzystania z internetu rzeczy przez przedsiębiorstwa i konsumentów oraz umożliwienia im zdobycia niezbędnych zdolności i kompetencji ([13]), przy czym szczególną uwagę należy zwrócić na grupy znajdujące się w niekorzystnym położeniu oraz na kwestie różnorodności;

6.1.10. rozpocząć inicjatywy w dziedzinie edukacji z myślą o należytym zapobieganiu, mając na uwadze wczesną inicjację dzieci w środowiskach cyfrowych;

6.1.11. rozpocząć analizy i badania diagnostyczne dotyczące wpływu internetu rzeczy w takich obszarach jak nowe modele zrównoważonej produkcji i konsumpcji.

6.1.12. zapewnić pełne wdrożenie i skuteczne wykorzystywanie alternatywnych metod rozwiązywania sporów – zarówno w trybie offline, jak i online (ADR i ODR);

6.1.13. zapewnić istnienie, wdrożenie i sprawne funkcjonowanie europejskiego systemu roszczeń zbiorowych, który umożliwi wstrzymanie praktyk i uzyskanie odszkodowania także w wypadku, gdy korzystanie z internetu rzeczy powoduje szkody lub straty o charakterze zbiorowym – tego rodzaju możliwość przewidziana jest w nowym ładzie dla konsumentów.

6.2. Ponadto EKES wzywa Komisję do oceny zasad bezpośrednio lub pośrednio związanych z internetem rzeczy i, tam gdzie to konieczne, poprawy obowiązującego prawodawstwa. W związku z tym ***nowy ład dla konsumentów*** powinien również koncentrować się na wzajemnie połączonych urządzeniach, sieciach i ich bezpieczeństwie, a także na danych związanych z takimi urządzeniami.

6.3. Na koniec EKES zwraca uwagę na znaczenie wprowadzenia mechanizmów współpracy i koordynacji między państwami członkowskimi w celu skutecznego i jednolitego stosowania planowanych przepisów oraz z myślą o porozumieniach, które UE musi zawierać poza swoim terytorium z uwagi na lokalizację przedsiębiorstw i dostawców. Szczególny nacisk należy tu położyć na wymianę najlepszych praktyk. Należy koordynować politykę międzynarodową w zakresie transgranicznych przepływów danych, aby zaangażowane państwa mogły ustanowić równie wysokie normy w zakresie ochrony w ramach zarówno rzeczowego, jak i procesowego prawa krajowego.

Bruksela, dnia 19 września 2018 r.

Luca JAHIER
Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego

([12]) Dz.U. C 197 z 8.6.2018, s. 17.
([13]) Dz.U. C 434 z 15.12.2017, s. 36.