Opinia Europejskiego Komitetu Ekonomiczno-Społecznego

„Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)"

[COM(2017) 10 final – 2017/0003 (COD)]

(2017/C 345/23)

Sprawozdawca: **Laure BATUT**

Wniosek o konsultację	Parlament Europejski, 16.2.2017
	Rada Unii Europejskiej, 9.3.2017
Podstawa prawna	Artykuły 16 i 114 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego
Data przyjęcia przez sekcję	14.6.2017
Data przyjęcia na sesji plenarnej	5.7.2017
Sesja plenarna nr	527
Wynik głosowania	155/0/5
(za/przeciw/wstrzymało się)	

1. **Wnioski i zalecenia**

1.1. EKES głęboko ubolewa, że nakładanie się na siebie tekstów dotyczących ochrony danych, ich objętość i wzajemne przeplatanie się, a także konieczne dla ich zrozumienia ciągłe przechodzenie od jednego tekstu do drugiego uniemożliwiają ich lekturę poza kręgiem wtajemniczonych, ich wartość dodana zaś nie jest uchwytna dla obywatela, o którym zresztą nie mówi się w ogóle w całym projektowanym rozporządzeniu. Zaleca opublikowanie w internecie zwięzłej broszury, która przedstawi te teksty szerszej publiczności i uczyni je dostępnymi dla wszystkich.

1.2. EKES podkreśla, że spośród wariantów zaproponowanych w ocenie skutków Komisja wybrała ten, który przewiduje „wymierne" wzmocnienie prywatności. Czy to w celu zapewnienia równowagi z interesami przemysłu? Komisja nie określa, jakie elementy „daleko idącego" wzmocnienia prywatności szkodziłyby interesom przemysłu. Stanowisko to prowadzi do osłabienia wagi tekstu już na etapie projektu.

1.3. EKES zaleca Komisji, co następuje:

1) Uznać, że obecnie wszystko może stać się danymi i być przedmiotem komunikacji elektronicznej, co ma skutki dla prywatności osób fizycznych i prawnych.

2) Sprecyzować we wniosku (artykuły 5, 8 i 11) stosowanie Karty praw podstawowych Unii Europejskiej oraz praw człowieka, a także możliwość wprowadzania ograniczeń na mocy przepisów krajowych (motyw 26).

3) Zmienić artykuły 5 i 6 wniosku. Internet i telefonia komórkowa, umożliwiając łączność elektroniczną, są usługami świadczonymi w interesie ogólnym, do których dostęp musi być powszechny i które powinny być dostępne i przystępne cenowo, zaś konsumenci, by z nich korzystać, nie mogą być zmuszani do wyrażenia zgody na przetwarzanie ich danych wymaganych przez podmiot gospodarczy. W związku z tym należy przewidzieć obowiązek każdorazowego proponowania użytkownikowi możliwości odmowy w oparciu o zrozumiałe informacje (odmowy plików typu cookie, „monitorowania" itp.).

4) Wyraźnie określić, że *lex specialis* proponowane w celu uzupełnienia ogólnego rozporządzenia o ochronie danych jest zgodne z ogólnymi zasadami tego aktu prawnego i nie osłabia ustanowionego w nim poziomu ochrony oraz że wszelkie przetwarzanie, w tym pomiar liczby odsłon stron internetowych (*web audience measuring*), podlega zasadom ogólnego rozporządzenia o ochronie danych (artykuł 8).

5) Zapewnić stabilność regulacyjną obywatelom i przedsiębiorstwom, a w związku z tym doprecyzować tekst rozporządzenia i zakres środków wykonawczych w celu uniknięcia zbyt dużej liczby aktów delegowanych.

6) Opracować strategię, która pozwoli poinformować wszystkich konsumentów, że UE pozostaje wierna swym zasadom co do poszanowania praw człowieka i pragnie zapewnić poszanowanie prywatności nie tylko przez operatorów komunikacji elektronicznej, ale również przez dostawców usług OTT (over-the-top).

7) Nie dopuścić do tego, by dziedzina zdrowia stała się szerokim wyłomem pozwalającym na wykorzystanie prywatności i danych osobowych do celów handlowych przez operatorów komunikacji elektronicznej.

8) Zwrócić uwagę na gospodarkę dzielenia się, przekazywanie i wykorzystywanie danych w łączności elektronicznej za pośrednictwem platform, często znajdujących się poza UE.

9) Uwzględnić internet rzeczy, który jest bardzo inwazyjny i może otwierać drogę do naruszenia prywatności podczas transmisji danych w łączności elektronicznej.

10) Wziąć pod uwagę kolejny etap po przekazaniu danych i chronić dane przechowywane przez osoby, ponieważ większość tych danych ma charakter prywatny (niezależnie od interfejsu, w tym także w chmurze obliczeniowej).

11) Wyjaśnić zakres ochrony przekazywania danych między maszynami (M2M) i poświęcić tej kwestii artykuł, a nie jedynie motyw (12).

12) Aby pomóc obywatelom zorientować się w gąszczu tekstów i egzekwować własne prawa, stworzyć europejski portal (DG ds. Sprawiedliwości), dostępny dla wszystkich i łatwo zrozumiały, umożliwiający dostęp do przepisów europejskich i krajowych, do środków odwoławczych i do orzecznictwa (przykład: wyjaśnić treść motywu 25 i art. 12 i 13).

13) Przyznać organom nadzoru środki na wypełnianie ich zadań (Europejski Inspektor Ochrony Danych, organy krajowe).

14) Umożliwić konsumentom wniesienie powództwa zbiorowego na poziomie europejskim w celu dochodzenia ich praw, przyjmując nową dyrektywę, idącą dalej niż zalecenie C(2013) 401 i 3539 ([1]).

2. **Elementy kontekstu legislacyjnego**

2.1. Sieci łączności elektronicznej uległy znacznym przemianom od czasu wejścia w życie dyrektyw 95/46/WE i 2002/58/WE ([2]) w sprawie poszanowania prywatności w łączności elektronicznej.

2.2. **Ogólne rozporządzenie o ochronie danych przyjęte w 2016 r.** (rozporządzenie (UE) 2016/679) stało się podstawą działań i ustanowiło główne zasady, w tym w odniesieniu do danych sądowych i dotyczących postępowań karnych. Na mocy tego rozporządzenia dane osobowe mogą być gromadzone wyłącznie na ściśle określonych warunkach, w prawnie uzasadnionych celach i z zachowaniem poufności (art. 5 ogólnego rozporządzenia o ochronie danych).

2.2.1. Komisja przedstawiła w **październiku 2016 r.** wniosek dotyczący dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej ([3]) (o objętości 300 stron), który jeszcze nie został przyjęty, ale do którego odnosi się w przypadku niektórych definicji nieznajdujących się ani w ogólnym rozporządzeniu o ochronie danych, ani w omawianym tekście.

2.2.2. **Dwa wnioski ze stycznia 2017 r.** uściślają niektóre aspekty w oparciu o ogólne rozporządzenie o ochronie danych. Chodzi tu o wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady dotyczącego ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne (**COM(2017) 8 final**, sprawozdawca: Jorge Pegado Liz) oraz o omawiany tekst (**COM(2017) 10 final**) w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych.

2.3. Wszystkie trzy wspomniane teksty będą **miały zastosowanie od tej samej daty, tj. od 25 maja 2018 r.**, i mają na celu harmonizację praw i procedur kontroli.

2.4. Należy zauważyć, że w celu ułatwienia tego podejścia postanowiono w dziedzinie ochrony prywatności skorzystać z formy rozporządzenia europejskiego, a nie – jak wcześniej – dyrektywy.

([1]) IP/13/525 i notatka 13/531 DG ds. Sprawiedliwości z 11 czerwca 2013 r.

([2]) Dyrektywa 2002/58/WE zabrania w szczególności przesyłania niepożądanych wiadomości elektronicznych (spamu) (art. 13), wprowadzając, przy okazji nowelizacji w 2009 r., zasadę opt-in, zgodnie z którą podmiot gospodarczy musi uzyskać zgodę odbiorcy przed przesłaniem mu „komunikatów handlowych".

([3]) COM (2016) 590 final z 12.10.2016 – Wniosek Komisji w sprawie dyrektywy Parlamentu Europejskiego i Rady ustanawiającej Europejski kodeks łączności elektronicznej, s. 2 (Dz.U. C 125 z 21.4.2017, s. 56).

3. **Wprowadzenie**

3.1. Społeczeństwo obywatelskie pragnie wiedzieć, czy w świecie cyfrowym, którego zaczątki obserwujemy, Unia wnosi wartość dodaną zapewniającą istnienie obszarów, w których bez obaw będzie mogło rozwijać się życie prywatne.

3.2. Generowane w sposób ciągły dane sprawiają, że wszystkich użytkowników można wszędzie śledzić i zidentyfikować. Przetwarzanie danych w ośrodkach fizycznych, najczęściej zlokalizowanych poza Europą, budzi obawy.

3.3. Duże zbiory danych (tzw. Big Data) stały się walutą. Pozwalają one, dzięki inteligentnemu przetwarzaniu, „sprofilować" i „utowarowić" osoby fizyczne i prawne oraz zarabiać pieniądze, często bez wiedzy użytkowników.

3.4. Przede wszystkim jednak pojawienie się nowych podmiotów w sektorze przetwarzania danych – poza dostawcami dostępu do internetu – powinno prowadzić do zmiany przepisów.

4. **Streszczenie wniosku Komisji**

4.1. Za pomocą omawianego tekstu Komisja pragnie wprowadzić równowagę między konsumentami i przemysłem:

— zezwala na wykorzystywanie danych przez podmioty gospodarcze, umożliwiając użytkownikom końcowym zachowanie kontroli poprzez wyraźne wyrażenie zgody,

— wymaga, by podmioty gospodarcze informowały, co zrobią z tymi danymi,

— wybiera trzeci wariant w odniesieniu do oceny skutków, który przewiduje „wymierne" wzmocnienie prywatności, a nie czwarty, w którym proponuje się „daleko idące" wzmocnienie.

4.2. Wniosek ma na celu wdrożenie rozporządzenia o ochronie danych, mającego zastosowanie ogólne, tak samo jak zasada poufności danych osobowych i prawo do usunięcia danych, i dotyczy w szczególności kwestii prywatności i ochrony danych osobowych w telekomunikacji; proponuje się w nim wprowadzenie bardziej wymagających zasad w zakresie ochrony prywatności, a także skoordynowanych kontroli i sankcji.

4.3. Wniosek nie ustanawia specjalnych środków dotyczących „wyłomów" w ochronie danych osobowych powodowanych przez samych użytkowników, ale potwierdza w pierwszych artykułach (art. 5) zasadę poufności komunikacji elektronicznej.

4.4. Dostawcy mogą przetwarzać treść łączności elektronicznej:

— w celu świadczenia usługi na rzecz użytkownika końcowego, który wyraził na to zgodę,

— na rzecz wszystkich zainteresowanych uczestników końcowych [art. 6 ust. 3 lit. a) i b)], którzy wyrazili na to zgodę.

4.5. Mają oni obowiązek usuwania lub anonimizacji treści po ich odebraniu przez adresatów.

4.6. Zgodnie z art. 4 ust. 11 ogólnego rozporządzenia o ochronie danych „zgoda" osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, przez co osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwala na przetwarzanie dotyczących jej danych osobowych.

4.7. W projekcie utrzymano wymóg **wyraźnie wyrażonej zgody**, określony w ogólnym rozporządzeniu o ochronie danych, przy czym ciężar dowodu spoczywa na podmiotach gospodarczych.

4.8. „Przetwarzanie" odbywa się na podstawie tej zgody. Administrator danych „musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych" (art. 7 ust. 1 ogólnego rozporządzenia o ochronie danych).

4.9. Pewne ograniczenia (praw i obowiązków) w zakresie zachowania poufności mogą zostać wprowadzone na mocy prawa UE lub prawa krajowego w celu zapewnienia ochrony interesu publicznego lub realizacji inspekcji.

4.10. Osoby fizyczne muszą wyrazić swoją zgodę w odniesieniu do umieszczenia ich danych osobowych w publicznie dostępnym elektronicznym spisie numerów, a przy tym otrzymują środki służące weryfikowaniu takich danych i ich poprawianiu (art. 15).

4.11. Prawo do wyrażenia sprzeciwu pozwala użytkownikowi na zablokowanie wykorzystania jego danych powierzonych stronom trzecim (np. handlowcom) oraz za każdym razem, gdy wysyłana jest wiadomość (art. 16). Nowe przepisy zapewnią użytkownikom większą kontrolę nad ich parametrami (pliki typu cookie, identyfikatory), a niepożądane komunikaty (spam, wiadomości, SMS-y, połączenia telefoniczne) mogą zostać zablokowane w przypadku braku zgody użytkownika.

4.12. W sprawie identyfikacji połączeń i blokowania połączeń niepożądanych (artykuły 12 i 14) w rozporządzeniu podkreśla się, że prawa te posiadają również osoby prawne.

4.13. Struktura systemu kontroli jest zgodna z przepisami ogólnego rozporządzenia o ochronie danych (rozdziały VI o organach nadzorczych i VII dotyczący współpracy między organami nadzorczymi).

4.13.1. Nad przestrzeganiem zasad poufności będą musiały czuwać państwa członkowskie i ich krajowe organy odpowiedzialne za ochronę danych osobowych. Pozostałe organy nadzorcze mogą, w ramach wzajemnej pomocy, formułować zastrzeżenia, zgłaszane ewentualnie krajowym organom nadzorczym. Organy nadzorcze współpracują ze sobą oraz z Komisją Europejską, stosując mechanizm spójności (art. 63 ogólnego rozporządzenia o ochronie danych).

4.13.2. Nad jednolitym stosowaniem omawianego rozporządzenia czuwa Europejska Rada Ochrony Danych (art. 68 i 70 ogólnego rozporządzenia o ochronie danych).

Może ona publikować wytyczne, zalecenia i najlepsze praktyki w celu wspierania stosowania rozporządzenia.

4.14. Istnieją środki zaradcze dla osób fizycznych i prawnych będących użytkownikami końcowymi w razie naruszenia ich interesów; osoby te mogą uzyskać rekompensatę z tytułu poniesionej szkody.

4.15. Przewidziane administracyjne kary pieniężne powinny być odstraszające, ponieważ w razie naruszenia rozporządzenia mogą sięgać 10 000 000 EUR, a w przypadku przedsiębiorstwa – 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa (art. 23); państwa członkowskie ustanawiają przepisy dotyczące sankcji w przypadku braku administracyjnej kary pieniężnej i informują o tym Komisję.

4.16. Nowy tekst w sprawie poszanowania prywatności i wykorzystywania danych osobowych będzie **obowiązywać od dnia 25 maja 2018 r.**, zatem od tego samego dnia, co ogólne rozporządzenie o ochronie danych z 2016 r., rozporządzenie w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz projekt dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej [wersja przekształcona, COM(2016) 590 final], jeśli zostaną przyjęte.

4.17. Zakres stosowania lex specialis wdrażającego ogólne rozporządzenie o ochronie danych:

— ***ratione iuris*: podstawa prawna**

Opiera się ona na artykułach 16 (ochrona danych) i 114 (jednolity rynek) TFUE, lecz również na artykułach 7 i 8 Karty praw podstawowych Unii Europejskiej. Rozporządzenie ma uzupełnić rozporządzenie ogólne o ochronie danych w odniesieniu do danych, które można uznać za dane osobowe.

— ***ratione personae*: podmioty**

To użytkownicy końcowi, osoby fizyczne i prawne, określone w projekcie Europejskiego kodeksu łączności elektronicznej, w stosunku do wszystkich dostawców usług komunikacyjnych, nie tylko tradycyjnych dostawców, ale przede wszystkim nowych podmiotów, których nowe usługi nie zapewniają odpowiednich gwarancji użytkownikom. Techniki stosowane w przypadku usług OTT (komunikatory, SMS-y, połączenia VoIP, wielorakie interfejsy itp.) sprawiają, że znajdują się one obecnie poza zakresem stosowania istniejących przepisów.

— ***ratione materiae*: dane**

Wniosek nie zawiera przepisu dotyczącego przechowywania danych w chmurze obliczeniowej, pozostawiając państwom członkowskim podjęcie odpowiednich kroków zgodnie z art. 23 ogólnego rozporządzenia o ochronie danych dotyczącym ograniczeń prawa do sprzeciwu i z orzecznictwem Trybunału Sprawiedliwości (zob. pkt 1.3 uzasadnienia).

Użytkownik będzie musiał wyrazić zgodę na przechowywanie danych i metadanych generowanych w systemach (data, godzina, lokalizacja itp.), w przeciwnym wypadku dane te muszą zostać zanonimizowane lub usunięte.

— ***ratione loci*: gdzie?**

Podmioty dokonują czynności przetwarzania danych w państwach członkowskich albo jedna z ich jednostek organizacyjnych znajdująca się w jednym z państw członkowskich będzie uznawana za „główną” do celów kontroli; krajowe organy nadzorcze będą odgrywały swoją rolę, a Europejski Inspektor Ochrony Danych (EIOD) będzie nadzorować cały proces.

4.18. Cele UE: jednolity rynek cyfrowy

— Jednym z celów jednolitego rynku cyfrowego jest stworzenie warunków dla bezpiecznych usług cyfrowych i wzbudzenie zaufania użytkowników z myślą o rozwoju m.in. handlu elektronicznego i innowacji, a tym samym zwiększaniu zatrudnienia i wzrostu (uzasadnienie, pkt 1.1).

— Omawiany projekt rozporządzenia zmierza również do pewnej harmonizacji między tekstami oraz spójności między państwami członkowskimi.

— Co trzy lata Komisja przeprowadzać będzie ocenę stosowania omawianego rozporządzenia i przedstawiać ją Parlamentowi Europejskiemu, Radzie i EKES-owi (art. 28).

5. **Uwagi ogólne**

5.1. Komitet z zadowoleniem przyjmuje stworzenie jednocześnie w całej UE spójnego zbioru zasad mających na celu ochronę praw osób fizycznych i prawnych związanych z korzystaniem z danych cyfrowych za pomocą komunikacji elektronicznej.

5.1.1. Z satysfakcją przyjmuje też fakt, że UE odgrywa swoją rolę jako obrońca praw obywateli i konsumentów.

5.1.2. Podkreśla, że choć celem jest ujednolicenie, interpretacja wielu pojęć spoczywa na państwach członkowskich, co przekształca rozporządzenie w rodzaj dyrektywy, która pozostawia wiele miejsca na handlowe wykorzystanie danych prywatnych. W szczególności dziedzina zdrowia jest otwartą bramą dla gromadzenia ogromnych ilości danych osobowych.

5.1.3. Art. 11 ust. 1, art. 13 ust. 2, art. 16 ust. 4 i 5 oraz art. 24 zawierają raczej przepisy, które można by nazwać środkami dotyczącymi „transpozycji" i które nadawałyby się do dyrektywy, lecz nie do rozporządzenia. Zbyt dużą swobodę pozostawiono podmiotom gospodarczym z myślą o poprawie jakości usług (artykuły 5 i 6). Omawiane rozporządzenie powinno stanowić integralną część wniosku w sprawie dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej [COM(2016) 590 final].

5.1.4. EKES głęboko ubolewa, że nakładanie się na siebie tych tekstów, ich objętość i wzajemne przeplatanie się uniemożliwiają ich lekturę poza kręgiem wtajemniczonych. Niezbędne jest bowiem ciągłe przechodzenie od jednego tekstu do drugiego i z powrotem, a wartość dodana nie jest widoczna dla obywateli. Te trudności w lekturze i złożoność wniosku są sprzeczne z duchem programu sprawności i wydajności regulacyjnej (REFIT) i z celem „lepszego stanowienia prawa", a ponadto spowodują trudności w interpretacji, a także luki w ochronie danych.

5.1.5. Tytułem przykładu, wniosek w sprawie rozporządzenia nie zawiera definicji pojęcia „operatora". Trzeba odwołać się do projektu Europejskiego kodeksu łączności elektronicznej ([4]), który nie wszedł jeszcze w życie, a który zmieni przepisy w tym sektorze w ramach jednolitego rynku cyfrowego, a mianowicie dyrektywę ramową 2002/21/WE ze zmianami, dyrektywę w sprawie zezwoleń 2002/20/WE ze zmianami, dyrektywę w sprawie usługi powszechnej 2002/22/WE ze zmianami, dyrektywę w sprawie dostępu 2002/19/WE ze zmianami, rozporządzenie (WE) nr 1211/2009 ustanawiające Organ Europejskich Regulatorów Łączności Elektronicznej, decyzję w sprawie widma radiowego 676/2002/WE, decyzję (2002/622/WE) ustanawiającą zespół ds. polityki w zakresie widma radiowego i decyzję 243/2012/UE ustanawiającą wieloletni program dotyczący polityki w zakresie widma radiowego (RSPP). Podstawowym punktem odniesienia pozostaje oczywiście ogólne rozporządzenie o ochronie danych (zob. pkt 2.2), które omawiany wniosek ma uzupełnić i któremu jest on podporządkowany.

5.2. EKES zwraca szczególną uwagę na treść art. 8 dotyczącego ochrony informacji przechowywanych w urządzeniach końcowych i możliwych wyjątków, mającego fundamentalne znaczenie, ponieważ daje on społeczeństwu informacyjnemu możliwości dostępu do danych osobowych. Zwraca także uwagę na treść art. 12 dotyczącego ograniczenia identyfikacji rozmów przychodzących i wychodzących. Oba te artykuły są mało przystępne dla laika.

5.2.1. Dyrektywa z 1995 r. (art. 2) definiowała „dane osobowe" jako „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (»osoby, której dane dotyczą«)". Omawiane rozporządzenie rozszerza ochronę danych na metadane i ma odtąd zastosowanie zarówno do osób fizycznych, jak i do osób prawnych. Wypada ponownie podkreślić, że cel projektu jest dwojaki: z jednej strony ma on zapewnić ochronę danych osobowych, z drugiej swobodny przepływ danych pochodzących z łączności elektronicznej i usług łączności elektronicznej w obrębie Unii (art. 1).

([4]) COM(2016) 590 i załączniki 1–11 z 12.10.2016 (Dz.U. C 125 z 21.4.2017, s. 56).

5.2.2. EKES podkreśla, że dążenie do ochrony danych osób prawnych (art. 1 ust. 2) będzie kolidowało z innymi tekstami, w których nie ma o niej mowy: nie wspomina się tam wyraźnie, że przepisy te powinny mieć zastosowanie w ich przypadku (zob. ogólne rozporządzenie o ochronie danych, dane w instytucjach UE).

5.3. EKES zastanawia się, czy rzeczywistym celem wniosku nie jest większy nacisk na art. 1 ust. 2 – zagwarantowanie „swobodnego przepływu danych pochodzących z łączności elektronicznej i usług łączności elektronicznej w obrębie Unii", którego to przepływu wniosek nie ogranicza ani nie zabrania z przyczyn związanych z poszanowaniem życia prywatnego i komunikowania się osób fizycznych – zamiast rzeczywistego zapewnienia, zgodnie z art. 1 ust. 1, „prawa do poszanowania życia prywatnego i komunikowania się oraz prawa do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych".

5.4. Wszystko opiera się na wyrażeniu zgody przez osobę fizyczną lub prawną. W związku z tym, według EKES-u, użytkownicy powinni być poinformowani, wyedukowani i zachować ostrożność, gdyż po wyrażeniu przez nich zgody dostawca będzie mógł w większym stopniu przetwarzać treści i metadane w celu maksymalizacji korzyści i możliwości działania. Ile osób wie, przed zaakceptowaniem pliku cookie, że jest on używany do śledzenia aktywności? Edukacja użytkowników do korzystania z ich praw, a także kwestie anonimizacji lub szyfrowania powinny być priorytetami w tym rozporządzeniu.

6. **Uwagi szczegółowe**

6.1. Dane osobowe powinny być zestawiane tylko przez podmioty, które same przestrzegają bardzo rygorystycznych warunków i których cele są znane i uprawnione (zgodnie z ogólnym rozporządzeniem o ochronie danych).

6.2. Komitet ponownie ubolewa nad „zbyt licznymi wyjątkami i ograniczeniami, naruszającymi głoszone zasady prawa do ochrony danych osobowych" ([5]). Znakiem rozpoznawczym Unii Europejskiej powinna pozostać równowaga między wolnością a bezpieczeństwem, nie zaś równowaga między podstawowymi prawami człowieka a przemysłem. Grupa Robocza Art. 29 w analizie projektu rozporządzenia (WP 247 z 4 kwietnia 2017 r., opinia 1/2017, pkt 17) krytycznie zaznaczyła, że prowadzi on do obniżenia poziomu ochrony określonego w ogólnym rozporządzeniu o ochronie danych, w szczególności jeśli chodzi o lokalizację urządzenia końcowego i brak ograniczenia zakresu gromadzenia danych, i nie wprowadza domyślnej ochrony prywatności (pkt 19).

6.3. Dane są jakby przedłużeniem tożsamości osoby, cieniem tożsamości (Shadow-ID). Dane należą do osoby, która je generuje, ale po ich przetworzeniu przestaje mieć na nie wpływ. Co się tyczy przechowywania i przekazywania danych, każde państwo zachowuje swe kompetencje i nie ma harmonizacji ze względu na możliwości ograniczenia praw, jakie otwiera omawiany wniosek. Komitet zwraca uwagę na ryzyko rozbieżności wynikające z faktu, że ograniczenia praw pozostawiono do stosowania według uznania państwom członkowskim.

6.4. Pojawia się pytanie odnoszące się w szczególności do osób pracujących w przedsiębiorstwach: Do kogo należą dane generowane przez te osoby w trakcie pracy? I jak są chronione?

6.5. Struktura kontroli nie jest zbyt jasna ([6]); mimo nadzoru sprawowanego przez Europejską Radę Ochrony Danych zabezpieczenia przed arbitralnością nie wydają się być wystarczające, a czas potrzebny, aby procedury doprowadziły do nałożenia sankcji, nie został oszacowany.

6.6. **EKES apeluje, by stworzono europejski portal**, w którym byłyby gromadzone i aktualizowane wszystkie przepisy europejskie i krajowe, prawa, środki odwoławcze, orzecznictwo, elementy praktyczne, aby pomóc obywatelom i konsumentom w odnalezieniu drogi przez gąszcz przepisów i praktyk, tak by mogli korzystać ze swoich praw. Portal ten powinien być inspirowany przynajmniej przepisami dyrektywy (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego oraz zasadami ujętymi w motywach 12, 15 i 21 wniosku dotyczącego dyrektywy zwanej europejskim aktem w sprawie dostępności 2015/0278 (COD) i powinien oferować łatwo dostępne i zrozumiałe treści wszystkim użytkownikom końcowym. EKES jest gotów uczestniczyć w kolejnych fazach opracowywania tego portalu.

6.7. W art. 22 brak jest odniesienia do „powództw zbiorowych", jak EKES zauważył już w swojej opinii w sprawie Europejskiego kodeksu łączności elektronicznej.

([5]) Dz.U. C 125 z 21.4.2017, s. 56 oraz Dz.U. C 110 z 9.5.2006, s. 83.

([6]) Rozdział IV omawianego rozporządzenia odsyła do warunków określonych w rozdziale VII, w szczególności do art. 68 ogólnego rozporządzenia o ochronie danych.

6.8. Ograniczenie materialnego zakresu stosowania (art. 2 ust. 2), rozszerzenie uprawnień do przetwarzania danych bez zgody właściciela (art. 6 ust. 1 i 2) i nierealistyczna idea uzyskiwania zgody od WSZYSTKICH zainteresowanych użytkowników (art. 6 ust. 3 lit. b)) oraz art. 8 ust. 1, 2 i 3), ograniczenia praw, jakie mogą zastosować państwa członkowskie, jeśli uznają, że stanowią one środek „konieczny, właściwy i proporcjonalny" – to przepisy, których treść może być interpretowana na tyle sposobów, że okazuje się sprzeczna z rzeczywistą ochroną prywatności. Ponadto szczególną uwagę należy zwrócić na ochronę danych dotyczących małoletnich.

6.9. EKES pozytywnie ocenia prawo osób do kontrolowania łączności elektronicznej, o którym mowa w art. 12, jednak odnotowuje szczególnie hermetyczne brzmienie tego artykułu, który wydaje się stawiać wyżej korzystanie z połączeń telefonicznych „nieznanych" lub „ukrytych", tak jak gdyby anonimowość była zalecana, gdy tymczasem zasadą powinna być identyfikacja rozmów.

6.10. Niezamawiane materiały (art. 16) i marketing bezpośredni są już objęte zakresem dyrektywy w sprawie nieuczciwych praktyk handlowych ([7]). System ten powinien domyślnie działać na zasadzie opt-in (akceptacja), a nie opt-out (odmowa).

6.11. Komisja ma dokonywać oceny co trzy lata; jednak w odniesieniu do sektora cyfrowego okres ten jest zbyt długi. Po dwóch ocenach środowisko cyfrowe będzie już całkowicie zmienione. Jednakże przekazanie uprawnień (art. 25), które można rozszerzyć, powinno odbywać się na czas określony, ewentualnie z możliwością przedłużenia.

6.12. Prawo powinno chronić prawa użytkowników (art. 3 TUE), przy jednoczesnym zapewnieniu stabilności prawnej niezbędnej do prowadzenia działalności gospodarczej. Komitet wyraża ubolewanie, że przepływ danych między maszynami (M2M) nie został uwzględniony we wniosku: trzeba w tym wypadku sięgnąć do kodeksu łączności elektronicznej (wniosek dotyczący dyrektywy, art. 2 i 4).

6.12.1. Internet rzeczy ([8]) przekształci BigData (duże zbiory danych) w HugeData (wielkie zbiory danych), a następnie w AllData (środowisko oparte w całości na danych). Jest to klucz do przyszłych fal innowacji. Maszyny, duże i małe, porozumiewają się między sobą i przekazują sobie dane osobowe (nasz zegarek rejestruje rytm naszego serca i przekazuje go do komputera naszego lekarza itd.). Wiele podmiotów cyfrowych uruchomiło własną platformę przeznaczoną dla przedmiotów połączonych z siecią: Amazon, Microsoft, Intel, a we Francji Orange i La Poste.

6.12.2. Internet rzeczy może łatwo stać się obiektem szkodliwych włamań, a ilość informacji osobowych, które mogą być gromadzone na odległość, stale wzrasta (geolokalizacja, dane medyczne, strumień wideo i audio). Braki w dziedzinie ochrony danych interesują m.in. zakłady ubezpieczeń, które zaczynają proponować swoim klientom, by wyposażali się w przedmioty połączone i odpowiedzialnie postępowali.

6.13. Wielu gigantów internetu dąży do przekształcenia swej początkowej aplikacji w platformę: tym samym należy odróżnić aplikację Facebook od platformy Facebook, umożliwiającej programistom tworzenie aplikacji dostępnych poprzez profil użytkownika. Z kolei Amazon był początkowo aplikacją internetową wyspecjalizowaną w sprzedaży online. Obecnie zaś jest platformą umożliwiającą stronom trzecim – zarówno osobom prywatnym, jak i wielkim korporacjom – sprzedaż produktów z wykorzystaniem zasobów Amazona: jego reputacji, logistyki itp. Wszystko to wymaga przekazywania danych osobowych.

6.14. W sektorze gospodarki dzielenia się powstaje coraz więcej platform, które „za pomocą środków elektronicznych umożliwia[ją] kontakt pomiędzy licznymi posiadaczami towarów lub usług oraz dużą liczbą użytkowników" ([9]). Podczas gdy są one cenione ze względu na ich działalność i tworzone miejsca pracy, EKES zastanawia się, w jaki sposób przekazywanie generowanych przez nie danych może być kontrolowane, zarówno w ramach stosowania ogólnego rozporządzenia o ochronie danych, jak i omawianego rozporządzenia.

Bruksela, dnia 5 lipca 2017 r.

Georges DASSIS
Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego

([7]) Dz.U. L 149 z 11.6.2005, s. 22, art. 8 i 9.
([8]) Opinia WP247/17 z 1.4.2017, pkt 19 (Dz.U. C 12 z 15.1.2015, s. 1).
([9]) Dz.U. C 125 z 21.4.2017, s. 56.