GRUPA ROBOCZA ART. 29

17/PL

WP 247

# Opinia 01/2017 na temat proponowanego rozporządzenia w sprawie prywatności i łączności elektronicznej (2002/58/WE)

**Przyjęto w dniu 4 kwietnia 2017 r.**

**GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH**

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

**PRZYJMUJE NINIEJSZĄ OPINIĘ:**

**STRESZCZENIE**

Grupa Robocza z zadowoleniem przyjmuje wniosek Komisji Europejskiej z dnia 10 stycznia 2017 r. dotyczący rozporządzenia w sprawie prywatności i łączności elektronicznej. Grupa Robocza z zadowoleniem przyjmuje **wybór rozporządzenia** jako instrumentu regulacyjnego. W ten sposób zapewnia się jednakowe zasady w całej UE i przejrzystość na potrzeby zarówno organów nadzorczych, jak i organizacji. Ponadto przyczynia się to również do zapewnienia spójności z przepisami ogólnego rozporządzenia o ochronie danych. Spójność z tym rozporządzeniem dodatkowo zwiększa fakt, że na organ odpowiedzialny za egzekwowanie przepisów dotyczących prywatności i łączności elektronicznej wybrano **organ odpowiedzialny za monitorowanie przestrzegania przepisów RODO**.

Jednocześnie pozytywny jest wybór (utrzymanie) **uzupełniającego instrumentu prawnego**. Ochrona poufnej komunikacji i urządzenia końcowego ma szczególną specyfikę, której nie uwzględniono w RODO. Uzupełniające przepisy dotyczące tego rodzaju usług są zatem konieczne do zapewnienia odpowiedniej ochrony podstawowego prawa do prywatności i poufności komunikacji, w tym poufności urządzenia końcowego. W tym zakresie Grupa Robocza zdecydowanie popiera przyjęte w proponowanym rozporządzeniu **zasadnicze podejście** zakładające obowiązywanie **daleko idących zakazów i ściśle określonych wyjątków** oraz **ukierunkowane stosowanie pojęcia zgody**.

Grupa Robocza z zadowoleniem przyjmuje rozszerzenie zakresu stosowania proponowanego rozporządzenia, **aby obejmował również dostawców usług OTT**, czyli usług funkcjonalnie równoważnych bardziej tradycyjnym środkom komunikowania się, które w związku z tym mogą mieć podobny wpływ na prywatność i prawo do poufności komunikacji w przypadku osób w UE. Korzystny jest również fakt, że proponowane rozporządzenie wyraźnie obejmuje **treść i powiązane metadane**, oraz uznaje, że **metadane mogą ujawniać dane szczególnie chronione**.

Grupa Robocza odnotowuje jednak 4 kwestie budzące **głęboki niepokój**. Jeżeli chodzi o **śledzenie lokalizacji urządzenia końcowego, warunki, w których dopuszczalne jest analizowanie treści i metadanych, ustawienia domyślne urządzenia końcowego i oprogramowania oraz zapory** *cookie wall*, proponowane rozporządzenie obniżyłoby stopień ochrony zapewniony na podstawie RODO. W niniejszej opinii Grupa Robocza przedstawiła szczegółowe propozycje w celu zapewnienia, aby rozporządzenie w sprawie prywatności i łączności elektronicznej gwarantowało taki sam lub wyższy stopień ochrony stosowny dla szczególnie chronionych danych komunikacyjnych (zarówno treści, jak i metadanych).

Jeżeli chodzi o **śledzenie za pośrednictwem WiFi**, w zależności od okoliczności i celów gromadzenia danych tego rodzaju śledzenie na podstawie RODO może być uwarunkowane uzyskaniem zgody albo może być prowadzone wyłącznie pod warunkiem gromadzenia zanonimizowanych danych osobowych. W tym drugim przypadku spełnione muszą zostać 4 warunki: cel gromadzenia danych pochodzących z urządzenia końcowego ogranicza się do zwykłych obliczeń do celów statystycznych, śledzenie jest ograniczone pod względem czasu i miejsca do absolutnego minimum koniecznego do tego celu, po upływie takiego czasu dane zostaną bezzwłocznie usunięte lub zanonimizowane, a ponadto dostępne są skuteczne możliwości rezygnacji. Komisję Europejską zachęca się do promowania normy technicznej

dotyczącej automatycznego sygnalizowania przez urządzenia mobilne sprzeciwu wobec takiego śledzenia.

Jeżeli chodzi o **analizowanie treści i metadanych**, za punkt wyjścia należy przyjąć zakaz przetwarzania danych komunikacyjnych bez zgody wszystkich użytkowników końcowych (nadawców i odbiorców). Aby dostawcy mogli świadczyć usługi wyraźnie żądane przez użytkownika, takie jak na przykład funkcje wyszukiwania i indeksowania, lub usługi zamiany tekstu na mowę, należy przewidzieć wewnętrzny wyjątek dotyczący przetwarzania treści i metadanych do czysto osobistych celów samego użytkownika.

Jeżeli chodzi o **zgodę na śledzenie**, Grupa Robocza wzywa do wprowadzenia wyraźnego zakazu stosowania zapór *cookie wall*, tj. zakazu zmuszania użytkowników do wyrażenia zgody na śledzenie poprzez uzależnianie uzyskania przez użytkownika dostępu do usługi od wyrażenia takiej zgody.

Ponadto Grupa Robocza zaleca, aby urządzenia końcowe i oprogramowanie **w sposób domyślny musiały oferować ustawienia zapewniające ochronę prywatności** oraz aby wyraźnie dawały użytkownikom możliwość potwierdzenia albo zmiany tych domyślnych ustawień podczas instalacji. Wspomniane ustawienia muszą być łatwo dostępne podczas użytkowania. Użytkownicy muszą mieć możliwość zaznaczenia danej zgody w ustawieniach ich przeglądarki. Preferencje w zakresie ochrony nie powinny ograniczać się do ingerencji osób trzecich lub do plików cookie. Grupa Robocza stanowczo zaleca, aby stosowanie normy zakładającej ochronę przed śledzeniem było obowiązkowe.

Grupa Robocza określiła również inne kwestie budzące niepokój, związane na przykład z zakresem zastosowania, ochroną urządzenia końcowego i marketingiem bezpośrednim. Co więcej, Grupa Robocza wskazała kwestie warte wyjaśnienia, aby zapewnić lepszą ochronę użytkownikom końcowym i większą pewność prawa dla wszystkich zaangażowanych zainteresowanych stron.

# SPIS TREŚCI

## 1. WPROWADZENIE

1. Grupa Robocza Art. 29 (Grupa Robocza) z zadowoleniem przyjmuje proponowane rozporządzenie Komisji Europejskiej w sprawie prywatności i łączności elektronicznej (proponowane rozporządzenie, rozporządzenie w sprawie prywatności i łączności elektronicznej)[1], które ma zastąpić dyrektywę o prywatności i łączności elektronicznej[2].

2. Proponowane rozporządzenie posiada wiele pozytywnych aspektów, a jego wprowadzenie przez Komisję Europejską stanowi istotne dokonanie. Istnieje jednak możliwość udoskonalenia proponowanego rozporządzenia. Służyłoby to nie tylko lepszej ochronie użytkowników końcowych, ale również zapewnieniu większej pewności prawa z punktu widzenia wszystkich zaangażowanych zainteresowanych stron.

3. Grupa Robocza określiła zatem kilka kwestii budzących niepokój oraz zaleceń dotyczących wyjaśnień, do których Parlament Europejski i Rada powinny się odnieść w prowadzonej debacie na temat proponowanego rozporządzenia. W niniejszej opinii w pierwszej kolejności rozważono pozytywne aspekty proponowanego rozporządzenia, a następnie wskazano kwestie budzące niepokój i kwestie wymagające wyjaśnienia.

## 2. POZYTYWNE ASPEKTY PROPONOWANEGO ROZPORZĄDZENIA

*OGÓLNOUNIJNA HARMONIZACJA, UJEDNOLICENIE KAR I EGZEKWOWANIE PRZEPISÓW WYŁĄCZNIE PRZEZ ORGANY OCHRONY DANYCH*

4. Grupa Robocza z zadowoleniem przyjmuje **wybór rozporządzenia jako instrumentu regulacyjnego**. W ten sposób zapewnia się jednakowe zasady w całej UE (z pewnymi wyjątkami, które zostaną omówione poniżej). W ten sposób zapewnia się przejrzystość na potrzeby zarówno organów nadzorczych, jak i organizacji. Ponadto, mając na uwadze podstawowe znaczenie ogólnego rozporządzenia o ochronie danych (RODO)[3] z punktu widzenia proponowanego

[1] 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), 2017/0003 (COD): http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

[2] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002, s. 37-42: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32002L0058

[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 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U. L 119 z 4.5.2016, s. 1: http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679

rozporządzenia, wybór rozporządzenia zapewnia spójność między tymi dwoma instrumentami. Jednocześnie pozytywny jest **wybór (utrzymanie) uzupełniającego instrumentu prawnego**. Ochrona poufnej komunikacji i urządzenia końcowego ma szczególną specyfikę, której nie uwzględniono w RODO. Uzupełniające przepisy dotyczące tego rodzaju usług są zatem konieczne do zapewnienia odpowiedniej ochrony tego prawa podstawowego. W tym zakresie Grupa Robocza również **popiera przyjęte w proponowanym rozporządzeniu zasadnicze podejście zakładające obowiązywanie daleko idących zakazów i ściśle określonych wyjątków**, oraz jest zdania, że należy unikać wprowadzania wyjątków o charakterze otwartym na zasadach określonych w art. 6 RODO, a w szczególności art. 6 lit. f) RODO (wymóg prawnie uzasadnionego interesu).

5. Egzekwowanie przepisów proponowanego rozporządzenia przez organ **odpowiedzialny za monitorowanie przestrzegania przepisów RODO** dodatkowo zwiększy spójność między tymi dwoma instrumentami. Ze względu na związek między ochroną danych osobowych a ochroną poufnej komunikacji i urządzenia końcowego powierzenie egzekwowania przepisów proponowanego rozporządzenia temu samemu organowi nadzorczemu, który odpowiada za egzekwowanie przepisów RODO (motyw 38 i art. 18 proponowanego rozporządzenia) stanowi przydatne rozwiązanie. Ponadto orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (TSUE)[4] potwierdza, że ważne jest, aby organ nadzorczy był niezależny, jak określono w art. 7 karty. Z praktycznego punktu widzenia dla organów ochrony danych wiązałoby się to jednak z dużymi dodatkowymi nakładami pracy oraz brakiem pewności co do ich realizacji bez uzyskania dodatkowych środków budżetowych. Organy ochrony danych z zadowoleniem przyjmują zatem motyw 38 proponowanego rozporządzenia, który podkreśla, że każdy organ nadzorczy powinien dysponować dodatkowymi zasobami finansowymi i osobowymi, lokalami oraz infrastrukturą, które są niezbędne do skutecznej realizacji zadań wynikających z nowego rozporządzenia. Z zadowoleniem przyjmuje się również, że art. 18 ust. 2 stanowi podstawę prawną współpracy między organami nadzorczymi egzekwującymi przepisy proponowanego rozporządzenia a krajowymi organami regulacyjnymi ustanowionymi na podstawie dyrektywy ustanawiającej Europejski kodeks łączności elektronicznej[5].

6. Ze względu na ścisły związek między proponowanym rozporządzeniem a RODO z zadowoleniem przyjmuje się również **dostosowanie kar przewidzianych w proponowanym rozporządzeniu do kar przewidzianych w RODO**. Działania objęte zakresem stosowania proponowanego rozporządzenia mają bardzo delikatny charakter, na przykład wiążą się z ingerencją w poufną komunikację i urządzenie końcowe. Poziom kar powinien być współmierny w tym szczególnie chronionym

[4] Zob. np. wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., C-362/14 (zasada „bezpieczna przystań"), pkt 41 i wyrok Trybunału Sprawiedliwości z dnia 21 grudnia 2016 r., Tele2/Watson, C-203/15 i C-698/15, pkt 123.

[5] Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady ustanawiającej Europejski kodeks łączności elektronicznej (Wersja przekształcona) 2016/0288 (COD) z 12.10.2016: http://eur-lex.europa.eu/legal-content/PL/ALL/?uri=comnat:COM_2016_0590_FIN

kontekście. Z tego również względu harmonizacja na poziomie UE ma duże znaczenie dla zapewnienia tego samego wysokiego stopnia ochrony w całym regionie. Artykuł 23 proponowanego rozporządzenia przewiduje skuteczne kary w przypadku naruszenia przepisów rozporządzenia, na poziomie podobnym do kar określonych w przypadku naruszenia przepisów RODO, z wyjątkiem określonych sytuacji (zob. uwaga 38).

7. Z zadowoleniem przyjmuje się również **usunięcie** w tym instrumencie **szczegółowych zasad zgłaszania naruszenia ochrony danych**, co zapobiega zbędnemu powielaniu wymogów w zakresie naruszenia ochrony danych przewidzianych w RODO.

8. **Z zadowoleniem przyjmuje się również fakt, że obecnie nacisk kładzie się na zapewnienie równego stopnia ochrony wszystkim użytkownikom końcowym**, co wynika z usunięcia w proponowanym rozporządzeniu rozróżnienia na „abonentów" i pozostałych użytkowników usług łączności elektronicznej.

*ROZSZERZENIE ZAKRESU STOSOWANIA W PORÓWNANIU Z ZAKRESEM STOSOWANIA DYREKTYWY O PRYWATNOŚCI I ŁĄCZNOŚCI ELEKTRONICZNEJ*

9. Grupa Robocza z zadowoleniem przyjmuje **rozszerzenie zakresu stosowania proponowanego rozporządzenia, aby obejmował również dostawców usług OTT**, czyli usług funkcjonalnie równoważnych bardziej tradycyjnym środkom komunikowania się, które w związku z tym mogą mieć podobny wpływ na prywatność i prawo do poufności komunikacji w przypadku obywateli UE. Grupa Robocza przede wszystkim z zadowoleniem przyjmuje fakt, że wszystkie kategorie usług OTT (OTT0, OTT1 i niektóre OTT2)[6] obecnie wchodzą w zakres stosowania rozporządzenia, gdyż obejmuje on nie tylko tradycyjne środki komunikowania się (OTT0), ale również usługi funkcjonalnie równoważne (OTT1), jak określono w art. 8 ust. 1 lit. c) proponowanego rozporządzenia. Pozytywnym aspektem jest również uwzględnienie, w uzupełnieniu definicji przewidzianych w dyrektywie ustanawiającej Europejski kodeks łączności elektronicznej, niektórych usług OTT2 uwzględniających wspomagającą komunikację interpersonalną i interaktywną, która jest nieodłącznie powiązana ze świadczoną usługą, np. w przypadku gier, aplikacji randkowych lub stron z recenzjami (art. 4 ust. 2 proponowanego rozporządzenia). Podobnie z zadowoleniem przyjmuje się **wyjaśnienie, że ochrona obejmuje również przesył komunikatów w trybie maszyna-maszyna**. Z motywu 12 wyraźnie wynika, że urządzenia komunikujące się ze sobą są objęte ochroną zapewnioną na podstawie proponowanego rozporządzenia. Jest to pożądane, gdyż tego rodzaju

[6] Aby zapoznać się z dalszym wyjaśnieniem tych pojęć, zob. BEREC, *Report on OTT Services*, BoR (16) 35, z dnia 29 stycznia 2016 r., s. 15 i 16:
http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services
Należy zwrócić uwagę, że w sprawozdaniu zauważono, że kategorie te służą jako pojęcia stosowane w debacie na temat przeglądu, i nie mają służyć jako pojęcia prawnicze.

komunikacja często obejmuje informacje chronione na podstawie praw dotyczących prywatności. Można by jednak doprecyzować zakres zastosowania (zob. uwaga 40h).

10. Korzystny jest również fakt, że **proponowane rozporządzenie wyraźnie obejmuje treść i powiązane metadane.** W motywie 14 wyjaśniono, że definicja „danych pochodzących z łączności elektronicznej" zawarta w art. 4 ust. 3 lit. a) ma być wystarczająco szeroka, aby objąć wszystkie treści i związane z nimi metadane, niezależnie od np. sposobów przekazywania sygnałów. Zaniepokojenie Grupy Roboczej budzi jednak uwaga 39, z której wynika że obecna definicja „danych pochodzących z łączności elektronicznej" nadal jest przedmiotem dyskusji. Zgodnie z takim rozszerzeniem zakresu Grupa Robocza uważa, że **uznanie, iż metadane mogą ujawniać bardzo wrażliwe dane** (zob. pkt 2.2 uzasadnienia; motyw 2) jest istotnym uzupełnieniem. Grupa Robocza z zadowoleniem przyjmuje fakt, że Komisja Europejska włączyła w ten sposób uwagi Trybunału Sprawiedliwości przedstawione w sprawach dotyczących praw cyfrowych w Irlandii i Tele2/Watson. Grupa Robocza Art. 29 docenia również **uznanie analizy treści za proces przetwarzania obarczony wysokim ryzykiem.** W motywie 19 i art. 6 ust. 3 lit. b) ustanowiono logiczne domniemanie prawne, zgodnie z którym skanowanie treści stanowi przetwarzanie obarczone wysokim ryzykiem w rozumieniu art. 35 RODO i, najwyraźniej bez względu na wysokie ryzyko szczątkowe, zawsze wymaga przeprowadzenia uprzednich konsultacji z (głównym) organem ochrony danych. Jednocześnie Grupa Robocza wyraziła obawy co do zakresu definicji „metadanych" oraz faktu, że analiza metadanych nie podlega temu samemu obowiązkowemu wymogowi dotyczącemu oceny skutków dla ochrony danych (zob. uwagi 33 i 46).

11. Mile widziane jest również ciągłe **uznawanie znaczenia anonimizacji**. W dyrektywie o prywatności i łączności elektronicznej środki anonimizacji odegrały już ważną rolę w zapewnianiu zgodności (np. art. 6 ust. 1 dyrektywy o prywatności i łączności elektronicznej, który stanowi, że dane o ruchu muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu). W art. 6 ust. 2 lit. c) i art. 6 ust. 3 lit. b) proponowanego rozporządzenia dopuszcza się wyjątek od zakazu przetwarzania metadanych, a treści są dopuszczalne na podstawie zgody, pod warunkiem że „ten cel lub te cele nie mogłyby być zrealizowane przez przetwarzanie informacji poddanych anonimizacji". Wymóg stosowania takich środków ochrony prywatności oprócz żądania zgody użytkowników chroni tych użytkowników przed nieuprawnionym przetwarzaniem. Jednocześnie Grupa Robocza jest jednak poważnie zaniepokojona tym, że przyjęcie takich technik anonimizacji nie będzie wymagane przy śledzeniu użytkowników za pomocą ich urządzeń przenośnych (zob. uwaga 17). Ponadto, nawet w przypadku stosowania środków anonimizacji dostawcy powinni zawsze przeprowadzać ocenę skutków dla ochrony danych (zob. uwagi 33 i 46), przy czym Grupa Robocza wzywa do przyjęcia dodatkowego zobowiązania do podawania do publicznej wiadomości sposobu anonimizacji i agregowania danych (zob. uwaga 42b).

12. Kolejnym pozytywnym aspektem jest **szerokie sformułowanie ochrony urządzeń końcowych**. W motywie 20 i art. 8 określono, że technologie wykorzystywane do uzyskania dostępu do urządzeń końcowych są nieistotne: jakakolwiek ingerencja w urządzenia końcowe, w tym wykorzystanie ich możliwości przetwarzania, wymaga

zgody użytkownika końcowego (z pewnymi wyjątkami). Komisja Europejska pomogła potwierdzić, że „pobieranie odbitek linii papilarnych przez urządzenie" objęte jest tym przepisem. Ponadto Grupa Robocza z zadowoleniem przyjmuje fakt, że niestosowanie się przez osobę trzecią do preferencji **wyrażonych w ustawieniach przeglądarki** danej osoby **jest wykonalne** zgodnie z motywem 22. Jest to pomocne w sytuacjach, gdy osoba trzecia (np. sieć reklamowa) nie przestrzega tych ustawień. Należy to jednak określić również w odpowiednim przepisie proponowanego rozporządzenia.

13. Ponadto z zadowoleniem należy przyjąć ciągłe **włączanie osób prawnych do zakresu proponowanego rozporządzenia** (zob. pkt 2.2 uzasadnienia; motywy 3, 33 i 42; art. 1, art. 15 i art. 16 ust. 5). Dzieje się tak już w przypadku dyrektywy o prywatności i łączności elektronicznej, ale ponieważ organy ochrony danych będą miały za zadanie egzekwowanie nowych przepisów, należy to szczególnie podkreślić. Pozwala to organom ochrony danych na podejmowanie działań w przypadkach, gdy osoby prawne są ofiarami naruszenia, np. gdy przedsiębiorstwa otrzymują spam lub ich wiadomości są monitorowane w sposób tajny. Zaniepokojenie Grupy Roboczej budzi jednak fakt, że stosowanie zgody wobec osób prawnych nie jest jasne (zob. uwaga 41a) oraz że nie do końca wiadomo, co oznacza termin „uzasadniony interes" osób prawnych w przypadku marketingu bezpośredniego (zob. uwaga 43c).

*UKIERUNKOWANE ZASTOSOWANIE POJĘCIA ZGODY*

14. Grupa Robocza z zadowoleniem przyjmuje inną kategorię ulepszeń związanych ze stosowaniem i interpretacją pojęcia zgody. Po pierwsze, z zadowoleniem przyjmuje się **wyjaśnienie, że dostęp do internetu i telefonia (komórkowa) stanowią podstawowe usługi, a dostawcy tych usług nie mogą „zmuszać" swoich klientów do wyrażenia zgody na przetwarzanie danych, które nie są konieczne do świadczenia przez nich podstawowej usługi.** W szczególności w motywie 18 zauważano, że podstawowe usługi dostępu szerokopasmowego do internetu i usługi komunikacji głosowej są uważane za usługi kluczowe, co oznacza, ze względu na zależność osób od dostępu do tych usług, że zgoda na przetwarzanie ich danych pochodzących z łączności do takich właśnie dodatkowych celów (np. przetwarzanie w celach reklamowych lub marketingowych) nie może być ważna. Jednocześnie Grupa Robocza obawia się, że wyjaśnienie to jest zbyt zawężone. Usługi świadczone przez dostawców usług OTT także można uznać za usługi kluczowe, przy czym w rozporządzeniu w sprawie prywatności i łączności elektronicznej należy również wyraźnie zakazać wyborów typu „wszystko albo nic" (ang. *take-it-or-leave-it*) w innych okolicznościach (zob. uwaga 20).

15. Ponadto pozytywny jest fakt, że **wymóg uzyskania zgody na umieszczenie danych osobowych osób fizycznych w spisach jest ujednolicony**. Zgodnie z art. 15 proponowanego rozporządzenia przetwarzanie danych w publicznych spisach jest dozwolone tylko za zgodą osób fizycznych i z możliwością wyrażenia sprzeciwu przysługującą osobom prawnym. Szerzej omówiono to w motywie 31, w którym zauważono, że zgoda ta musi być szczególna w odniesieniu do konkretnych kategorii danych osobowych, które mają zostać włączone do spisu. Grupa Robocza z zaniepokojeniem odnotowuje jednak, że proponowane rozporządzenie mogłoby wyraźniej określać, iż w celu stosowania funkcji wyszukiwania i zwrotnego wyszukiwania wymagana będzie oddzielna zgodna (zob. uwaga 37).

16. Docenia się również **nowy ukierunkowany wyjątek w odniesieniu do nieinwazyjnej ingerencji w urządzenia końcowe.** Grupa Robocza Art. 29 uważa za pomocne, że w proponowanym rozporządzeniu wyjaśnia się, iż zakaz nie ma zastosowania do pomiaru ruchu w sieci (w ramach drobnego wyjątku, zgodnie z którym taki pomiar jest przeprowadzany przez dostawcę usługi społeczeństwa informacyjnego wymaganej przez użytkownika końcowego, por. art. 8 ust. 1 lit. d) proponowanego rozporządzenia). Zob. dalszy motyw 21. Grupa Robocza sugeruje jednak korzystanie z bardziej neutralnej technologicznie definicji i wyjaśnienie sposobu stosowania tego wyjątku (zob. uwaga 25).

## 3. KWESTIE BUDZĄCE GŁĘBOKI NIEPOKÓJ

*PROPONOWANE ROZPORZĄDZENIE OSŁABIA OCHRONĘ W RAMACH RODO*

Jak wspomniano powyżej w proponowanym rozporządzeniu wprowadzono szereg kluczowych usprawnień. Istnieją jednak również kwestie budzące niepokój, o różnym stopniu powagi. W niniejszej sekcji Grupa Robocza omawia cztery kwestie, którymi jest

**wysoce zaniepokojona**. Są to przepisy, które **obniżają poziom ochrony zapewniany przez RODO**.

17. **Zawarte w rozporządzeniu zobowiązania do śledzenia lokalizacji urządzenia końcowego powinny być zgodne z wymogami określonymi w RODO.** W art. 8 ust. 2 lit. b) proponowanego rozporządzenia wymaga się jedynie zamieszczenia zawiadomienia i wdrożenia środków bezpieczeństwa w celu zgromadzenia informacji wysyłanych przez urządzenie końcowe. W art. 8 ust. 2 lit. b) stwierdza się również, że osoba odpowiedzialna za gromadzenie takich informacji musi określić wszelkie działania, jakie mogą podjąć użytkownicy końcowi, aby wstrzymać lub ograniczyć do minimum takie gromadzenie. W ten sposób po zapoznaniu się z art. 8 ust. 2 lit. b) można odnieść wrażenie, że organizacje mogą gromadzić informacje wysyłane przez urządzenie końcowe w celu śledzenia fizycznych ruchów osób fizycznych (takie jak „śledzenie za pośrednictwem WiFi" lub „śledzenie za pośrednictwem Bluetooth") bez zgody danej osoby fizycznej. Strona gromadząca takie dane mogłaby faktycznie zastosować się do tego wymogu za pomocą zawiadomienia informującego użytkowników o konieczności wyłączenia urządzeń, jeżeli nie chcą być śledzeni. Takie podejście byłoby sprzeczne z podstawowym celem polityki telekomunikacyjnej Komisji Europejskiej polegającym na zapewnieniu szybkiego dostępu do mobilnej łączności internetowej i jednoczesnym zapewnieniu wszystkim Europejczykom silnej ochrony prywatności ponad granicami i przy niskich kosztach.

    Ponadto proponowane rozporządzenie nie nakłada żadnych wyraźnych ograniczeń co do zakresu gromadzenia danych ani późniejszych czynności przetwarzania. W tym kontekście należy zauważyć, że adresy MAC stanowią dane osobowe, nawet po podjęciu środków bezpieczeństwa takich jak haszowanie. W przypadku nienałożenia dalszych wymogów lub ograniczeń poziom ochrony tych danych osobowych na mocy proponowanego rozporządzenia jest znacznie niższy od poziomu ochrony zapewnianego na mocy RODO, zgodnie z którym takie śledzenie powinno być uczciwe i zgodne z prawem, a także przejrzyste. W motywie 25 mało pomocnie stwierdza się, że część funkcji śledzenia za pośrednictwem WiFi nie wiąże się z dużym zagrożeniem dla prywatności, inne zaś tak, np. śledzenie osób przez dłuższy czas. Chociaż Grupa Robocza docenia uznanie faktu, że to ostatnie wiąże się z dużym zagrożeniem dla prywatności, nie zaleca wcześniejszego podejmowania decyzji dotyczących tego, czy niektóre pozostałe funkcje nie stwarzają dużego zagrożenia dla prywatności, bez dalszej oceny okoliczności i proporcjonalności przetwarzania. Taką ocenę należy przeprowadzić z uwzględnieniem następujących warunków dotyczących nieanonimowego śledzenia za pośrednictwem WiFi.

    W zależności od okoliczności i celów gromadzenia danych, na podstawie RODO tego rodzaju śledzenie może podlegać konieczności uzyskania zgody albo może być prowadzone wyłącznie pod warunkiem gromadzenia zanonimizowanych danych osobowych. Takiej anonimizacji najlepiej dokonuje się niezwłocznie po zgromadzeniu danych. Jeżeli niezwłoczna anonimizacja nie jest możliwa ze względu na cele, dla których gromadzi się dane, dane te mogą być przetwarzane w okresie, w którym nie są poddawane anonimizacji, wyłącznie po spełnieniu następujących warunków; (i) cel gromadzenia danych musi być ograniczony do zwykłych obliczeń do celów statystycznych (zob. przykłady poniżej), (ii) śledzenie jest ograniczone pod względem czasu i miejsca do absolutnego minimum koniecznego do tego celu, (iii) po upływie takiego czasu dane zostają bezzwłocznie usunięte lub zanonimizowane oraz (iv) konieczne jest zapewnienie skutecznej możliwości rezygnacji. We

wszystkich okolicznościach administratorzy muszą oczywiście spełnić wymóg dostarczenia odpowiednich informacji.

Grupa Robocza obawia się, że potencjalna oferta indywidualnej rezygnacji skierowana do każdej organizacji gromadzącej takie dane stanowiłaby niedopuszczalne obciążenie dla obywateli, biorąc pod uwagę zwiększone wdrażanie takich technologii śledzących przez zarówno organizacje sektora prywatnego, jak i organizacje sektora publicznego. W związku z tym Grupa Robocza wzywa prawodawcę europejskiego do promowania opracowania norm technicznych dla urządzeń w celu automatycznego sygnalizowania braku zgody na takie śledzenie i zapewnienia stosowania się do takiego sygnału.

Na przykład na mocy RODO zgoda prawdopodobnie byłaby wymagana w przypadku gromadzenia i przechowywania przez administratorów danych pośrednio możliwych do zidentyfikowania adresów MAC urządzeń (WiFi lub Bluetooth) oraz w przypadku obliczania lokalizacji użytkownika w celu śledzenia jego lokalizacji przez dłuższy czas, np. w wielu sklepach. Dotyczy to w szczególności sytuacji, gdy takie śledzenie odbywa się w miejscach publicznych, w których użytkownicy mają uzasadnione oczekiwania, że nie zostaną zidentyfikowani ani nie będą śledzeni w przypadku gromadzenia adresów MAC przechodniów. Zgodę taką można na przykład uzyskać za pomocą aplikacji, która zachęca użytkowników do udostępniania swojej lokalizacji w określonych obszarach w zamian za oferty handlowe, lub poprzez oferowanie punktów odprawy w określonych lokalizacjach lub poprzez moduł zgody w punktach dostępu WiFi.

Jedynie w ograniczonej liczbie przypadków administratorzy danych mogliby przetwarzać informacje przesłane przez urządzenie końcowe do celów śledzenia ruchów fizycznych, bez zgody osób fizycznych. Przykładem takiej sytuacji mogłoby być liczenie klientów znajdujących się w danej lokalizacji lub gromadzenie przesłanych danych po obu stronach punktu kontroli bezpieczeństwa w celu wyświetlenia czasu oczekiwania. W obu przypadkach dane musiałyby jednak zostać usunięte lub zanonimizowane od razu po osiągnięciu celu statystycznego. Oznacza to, że adresy MAC urządzeń osób odwiedzających przebywających w określonej lokalizacji np. w sklepie, muszą być anonimizowane niezwłocznie po zebraniu, bez stałego miejsca przechowywania adresów MAC oraz w sposób wykluczający możliwość ponownej identyfikacji. W przypadku obliczania czasu oczekiwania adresy MAC musiałyby zostać usunięte lub zanonimizowane, jak tylko dane przestałyby być istotne dla obliczania czasu oczekiwania (np. ponieważ odwiedzający przeszedł na drugą stronę kontroli bezpieczeństwa lub ponieważ opuścił kolejkę).
Ponadto administrator danych musiałby przestrzegać wymogów dotyczących minimalizacji danych (np. zakaz całodobowego śledzenia, gdy cel ogranicza się do godzin otwarcia sklepu lub okresowego pobierania próbek). Administratorzy danych muszą również podjąć inne środki łagodzące w celu zapewnienia, aby nie miało to wpływu na prawa użytkowników do prywatności, lub miało bardzo niewielki wpływ np. w celu ochrony prywatności osób żyjących w pobliżu punktu gromadzenia danych.

Wybór przedstawiony w art. 8 ust. 2 proponowanego rozporządzenia, który dotyczy zwykłego wymogu powiadamiania, jest tym bardziej zastanawiający, z uwagi na wniosek zawarty w motywie 20, z którego wynika, że informacje związane z urządzeniem użytkownika końcowego mogą być również zbierane zdalnie na potrzeby identyfikacji i śledzenia oraz że takie przetwarzanie – zgodnie z proponowanym rozporządzeniem – może poważnie naruszać prywatność tych użytkowników końcowych. Ponadto obowiązek ten nie wykracza poza obowiązek gromadzenia informacji przewidziany już w art. 13 i 14 RODO. Poważne naruszenie prywatności poprzez śledzenie jest dodatkowo potęgowane przez potencjalny dostęp innych osób do gromadzonych danych np. możliwość identyfikowania przez organy ścigania użytkowników końcowych na podstawie przechowywanych adresów MAC wysyłanych przez ich urządzenia mobilne.

18. **Konieczne jest opracowanie warunków, w których dopuszczalne jest analizowanie treści i metadanych.**

W art. 6 proponowanego rozporządzenia przewiduje się różne poziomy ochrony metadanych i treści. Grupa Robocza Art. 29 nie popiera tej różnicy: obie kategorie danych uznaje się za bardzo wrażliwe. Metadane i treści należy zatem objąć tak samo wysokim poziomem ochrony. Za punkt wyjścia należy zatem przyjąć zakaz przetwarzania metadanych i treści bez zgody wszystkich użytkowników końcowych (tj. nadawców i odbiorców).

W zależności jednak od celów można zezwolić na pewien rodzaj przetwarzania bez zgody, jeżeli jest to ściśle niezbędne do tych celów:

- dostawcy mogą przetwarzać dane pochodzące z łączności elektronicznej do celów wspomnianych w art. 6 ust. 1 lit. a) i b) oraz art. 6 ust. 2 lit. a) i b) proponowanego rozporządzenia[7];
- należy wyjaśnić, że niektóre techniki wykrywania/filtrowania oraz techniki ograniczania botnetów także można uznać za ściśle niezbędne do wykrywania lub powstrzymywania nadużyć w zakresie usług łączności elektronicznej (art. 6 ust. 2 lit. b). Jeżeli chodzi o filtrowanie spamu, użytkownicy końcowi otrzymujący spam powinni mieć możliwość rezygnacji w poszczególnych przypadkach, o ile jest to technicznie możliwe;
- należy wyjaśnić, że analiza danych pochodzących z łączności elektronicznej prowadzona na potrzeby obsługi klienta może również podlegać wyjątkowi „konieczne w celu naliczania opłat" (por. art. 6 ust. 2 lit. b)). Odpowiednie metadane mogą być przechowywane do czasu zakończenia okresu, w jakim można zgodnie z prawem zakwestionować rachunek lub w jakim można egzekwować płatność zgodnie z prawem krajowym. Odpowiednie dane (takie

[7] W odniesieniu do konieczności spełnienia obowiązkowych wymogów dotyczących jakości usług, o których mowa w art. 6 ust. 2 lit. a) proponowanego rozporządzenia, dostawcy powinni uwzględniać warunki opisane w rozporządzeniu (UE) 2015/2120 (EECS), w szczególności w art. 3 oraz motywach 10 i 13–15. Na podstawie tego przepisu dostawcy mogą być zobowiązani do przetwarzania danych pochodzących z łączności w celu wykrywania i filtrowania złośliwego oprogramowania i oprogramowania szpiegującego oraz mogą dokonywać kompresji danych.

jak adres URL) mogą być zatrzymywane jedynie na żądanie użytkownika końcowego i wówczas przez okres absolutnie konieczny do rozwiązania sporu dotyczącego opłat (co oznacza, że art. 7 ust. 3 powinien zostać zmieniony);

- powinna istnieć możliwość przetwarzania danych pochodzących z łączności elektronicznej do celów świadczenia usług wyraźnie wymaganych przez użytkownika końcowego, takich jak funkcje wyszukiwania lub indeksowania słów kluczowych, funkcje asystentów wirtualnych, funkcje przetwarzania tekstu na mowę i usługi tłumaczeniowe. Wymaga to wprowadzenia zwolnienia z obowiązku przeprowadzania analizy takich danych wyłącznie do użytku indywidualnego (użytku danego gospodarstwa domowego) oraz użytku indywidualnego związanego z pracą[8]. Byłoby to zatem możliwe bez zgody wszystkich użytkowników końcowych, ale mogłoby nastąpić również za zgodą użytkownika końcowego ubiegającego się o świadczenie takiej usługi. Taka szczególna zgoda uniemożliwiłaby również dostawcy wykorzystywanie tych danych do innych celów.

Oznacza to, że analiza treści lub metadanych do wszystkich innych celów, takich jak analityka, profilowanie, reklama behawioralna lub inne cele ukierunkowane na osiągnięcie (komercyjnych) korzyści przez dostawcę, wymaga uzyskania zgody od wszystkich użytkowników końcowych, których dane byłyby przetwarzane. Jeżeli chodzi o te sytuacje, w proponowanym rozporządzeniu należy wyjaśnić, że sam fakt wysłania wiadomości e-mail lub innego rodzaju osobistego komunikatu przez inną usługę użytkownikowi końcowemu, który osobiście wyraził zgodę na przetwarzanie jego treści lub metadanych (przykładowo podczas rejestrowania się do usługi pocztowej), nie stanowi ważnej zgody wyrażonej przez nadawcę.

Ponadto należy wyjaśnić, że przetwarzanie danych osób niebędących zaangażowanymi użytkownikami końcowymi (np. zdjęcia lub opisu osoby trzeciej w ramach wymiany pomiędzy dwoma osobami) również musi być zgodne ze wszystkimi właściwymi przepisami RODO.

19. **Urządzenia końcowe i oprogramowanie muszą w sposób *domyślny* zniechęcać do niezgodnej z prawem ingerencji w nie, zapobiegać tego rodzaju ingerencji oraz jej zakazywać, a także zapewniać informacje dotyczące możliwych wariantów.** Chociaż w proponowanym rozporządzeniu zobowiązuje się dostawców oprogramowania umożliwiającego łączność elektroniczną do „zapewnienia możliwości" zapobiegania ograniczonej formie ingerencji w urządzenie końcowe, a po instalacji zobowiązuje się dostawców oprogramowania do wymagania od użytkownika końcowego wyrażenia zgody na ustawienia (art. 10 ust. 1 i 2), tego rodzaju wybór nie jest jednoznaczny z *domyślną ochroną prywatności.* Poza tym

[8] Podczas gdy w motywie 13 proponowanego rozporządzenia wyraźnie wyklucza się sieci firmowe z zakresu tego rozporządzenia, ten nowy wyjątek dotyczący użytku indywidualnego powinien również dotyczyć wykorzystania usług w chmurze przez pracowników do celów związanych z pracą, takich jak wyszukiwanie w wiadomościach e-mail.

„możliwość” zapobiegania określonej ingerencji już obecnie istnieje i jak dotąd nie doprowadziła ona do wystarczającego rozwiązania problemu nieuzasadnionego śledzenia. Z tego właśnie powodu zgodnie z RODO dokonano świadomego wyboru polityki w celu wprowadzenia zasad ochrony danych i uwzględnienia ochrony prywatności już w fazie projektowania oraz domyślnej ochrony prywatności (art. 25 RODO). W proponowanym rozporządzeniu podważono te zasady w odniesieniu do danych komunikacyjnych i danych przechowywanych w urządzeniach. Jednocześnie w dyrektywie 2014/53/UE w sprawie urządzeń radiowych[9] (wskazanej w motywie 10) przewidziano jedynie bardzo ograniczony obowiązek w zakresie bezpieczeństwa, zgodnie z którym „urządzenia radiowe mają wbudowane systemy zabezpieczające w celu zapewnienia ochrony danych osobowych i prywatności użytkownika i abonenta” (art. 3 ust. 3 lit. e)). Nie może on zastąpić domyślnych ustawień prywatności zgodnie z proponowanym rozporządzeniem. W tym zakresie warto również zauważyć, że w badaniu Eurobarometr dotyczącym prywatności i łączności elektronicznej opublikowanym w grudniu 2016 r. stwierdzono, że „[b]lisko siedem na dziesięć osób (69%) całkowicie się zgadza, że domyślne ustawienia przeglądarki powinny wstrzymywać przekazywanie ich danych”[10]. Grupa Robocza powzięła osobną wątpliwość w odniesieniu do ustawień przeglądarki i definicji „osób trzecich”. Zob. uwaga 24. Ponadto należy pamiętać, że przepis ten nie dotyczy wyłącznie przeglądarek wykorzystywanych w komputerach, lecz odnosi się również do innych rodzajów oprogramowania umożliwiających komunikację (w tym systemów operacyjnych, aplikacji i interfejsów oprogramowania przeznaczonych do urządzeń podłączonych do internetu rzeczy). Podsumowując, urządzenia końcowe i oprogramowanie muszą *w sposób domyślny* oferować ustawienia zapewniające ochronę prywatności oraz poprowadzić użytkowników przez menu konfiguracyjne, aby mogli oni zmienić te ustawienia domyślne po zakończeniu instalacji. Wspomniane menu konfiguracyjne powinny być zawsze łatwo dostępne podczas użytkowania. Grupa Robocza zachęca ustawodawcę europejskiego do wyjaśnienia zakresu stosowania art. 10 w tej kwestii.

20. **Rozporządzenie w sprawie prywatności i łączności elektronicznej powinno wyraźnie zakazywać praktyki *cookie walls*,** tj. praktyki polegającej na odmowie dostępu do strony internetowej lub usługi do chwili wyrażenia zgody przez osoby fizyczne na ich śledzenie na innych stronach internetowych lub w ramach innych usług. Jak już zauważono w poprzednich opiniach Grupy Roboczej dotyczących dyrektywy o prywatności i łączności elektronicznej[11], tego rodzaju podejścia zmuszające użytkowników do przyjęcia lub odrzucenia wszystkich warunków bez możliwości negocjacji, na zasadzie „wszystko albo nic”, rzadko są uzasadnione[12].

[9] Dyrektywa 2014/53/UE w sprawie urządzeń radiowych.

[10] Zob. badanie Eurobarometr Flash 443, sprawozdanie dotyczące prywatności i łączności elektronicznej (opublikowane w grudniu 2016 r.), s. 5.

[11] Zob. np. WP240 (przegląd prywatności i łączności elektronicznej); s. 16; WP 208 (wyłączenie spod zasady pozyskiwania zgody), s. 5.

[12] Stanowisko to pozostaje bez uszczerbku dla art. 7 ust. 4 RODO, który może również wykluczać „wybory typu »wszystko albo nic«” w innych stosownych przypadkach.

Jeżeli wykorzystywanie możliwości przetwarzania i przechowywania, jakie daje urządzenie końcowe, lub gromadzenie informacji z urządzenia końcowego użytkowników końcowych umożliwia śledzenie aktywności użytkownika na przestrzeni czasu lub w ramach szeregu usług (np. na różnych stronach internetowych lub w różnych aplikacjach), tego rodzaju czynności przetwarzania mogą poważnie naruszyć prywatność takich użytkowników. Biorąc pod uwagę kluczowe znaczenie internetu w zapewnieniu prawa podstawowego do wolności wypowiedzi, w tym prawa do dostępu do informacji, możliwość uzyskania dostępu do treści online przez osoby fizyczne nie powinna zależeć od wyrażenia przez nie zgody na śledzenie ich aktywności na różnych urządzeniach i stronach internetowych / w ramach różnych aplikacji. W przyszłym rozporządzeniu w sprawie prywatności i łączności elektronicznej należy zatem wskazać, że dostęp do treści na przykład stron internetowych i aplikacji nie może zależeć od wyrażenia zgody na tego rodzaju inwazyjne czynności przetwarzania, niezależnie od zastosowanej technologii śledzenia, takiej jak pliki cookie, pobieranie odbitek linii papilarnych przez urządzenie, dodawanie niepowtarzalnych identyfikatorów lub inne techniki monitorowania. Konieczność ustanowienia tego rodzaju zakazu podkreślono w ostatnim badaniu Eurobarometr dotyczącym prywatności i łączności elektronicznej, w którym stwierdzono, że „[b]lisko dwie trzecie respondentów uznaje za nieakceptowalne monitorowanie ich aktywności online w zamian za uzyskanie nieograniczonego dostępu do określonej strony internetowej (64%)".

21. Podsumowując, w odniesieniu do czterech wymienionych powyżej punktów, **proponowane rozporządzenie powinno spełnić swoją obietnicę zapewnienia poziomu ochrony równego RODO lub wyższego niż RODO.** W motywie 5 stwierdzono – jako okoliczność faktyczną – że proponowane rozporządzenie nie obniża poziomu ochrony przysługującego na mocy RODO. Jak stanowi proponowane rozporządzenie w obecnym brzmieniu, jest to jednak błędne stwierdzenie, w szczególności w odniesieniu do śledzenia urządzeń (uwaga 17), brakującej zasady domyślnej ochrony prywatności (uwaga 19) i zgody (uwaga 18). Jest to szczególnie istotne, ponieważ w tym samym motywie zauważono, że proponowane rozporządzenie będzie stanowiło „*lex specialis* względem ogólnego rozporządzenia o ochronie danych, uszczegóławia je i uzupełnia w kwestii danych pochodzących z łączności elektronicznej, które można zakwalifikować jako dane osobowe". Grupa Robocza sugeruje, by w tekście rozporządzenia w sprawie prywatności i łączności elektronicznej wyjaśniono co najmniej, że:

    (i) zakazy przewidziane w rozporządzeniu w sprawie prywatności i łączności elektronicznej są nadrzędne względem pozwoleń na mocy RODO (np. zakaz ingerencji przewidziany w art. 5 rozporządzenia w sprawie prywatności i łączności elektronicznej jest nadrzędny względem przysługujących dostawcom usługi łączności elektronicznej praw do dalszego przetwarzania danych osobowych zgodnie z art. 5 ust. 1 lit. b) i art. 6 ust. 4 RODO);

    (ii) w przypadku zezwolenia na przetwarzanie na mocy dowolnego wyjątku (w tym zgody) od zakazów ustanowionych w rozporządzeniu w sprawie prywatności i łączności elektronicznej przetwarzanie to – w zakresie, w jakim dotyczy danych osobowych – wciąż musi być zgodne ze wszystkimi właściwymi przepisami RODO;

(iii) w przypadku zezwolenia na przetwarzanie na mocy dowolnego wyjątku od zakazów ustanowionych w rozporządzeniu w sprawie prywatności i łączności elektronicznej wszelkie inne przetwarzanie na mocy RODO jest zakazane, w tym przetwarzanie w innym celu na podstawie art. 6 ust. 4 RODO. Nie uniemożliwiłoby to administratorom zwracania się o dodatkową zgodę na nowe operacje przetwarzania. Nie uniemożliwiłoby to również prawodawcom ustanowienia dodatkowych, ograniczonych i szczególnych wyjątków w rozporządzeniu w sprawie prywatności i łączności elektronicznej, na przykład w celu umożliwienia przetwarzania do celów naukowych lub statystycznych zgodnie z art. 89 RODO lub ochrony „żywotnych interesów" osób fizycznych zgodnie z art. 6 lit. d) RODO.

Ponadto sposób wykładni rozporządzenia w sprawie prywatności i łączności elektronicznej powinien zapewniać, by gwarantowało ono taki sam – a w stosownych przypadkach wyższy – poziom ochrony co RODO.

## 4. INNE NIEPOKOJĄCE KWESTIE

Oprócz kwestii wskazanych powyżej Grupa Robocza Art. 29 jest **zaniepokojona** następującymi kwestiami.

*NALEŻY ROZSZERZYĆ ZAKRES TERYTORIALNY I ZAKRES PRZEDMIOTOWY*

22. **Termin „metadane" zdefiniowano w zbyt zawężający sposób.** Obecnie jest on zdefiniowany w art. 4 lit. c) jako „dane przetwarzane w sieci łączności elektronicznej do celów przesyłania, dystrybuowania lub wymiany treści łączności elektronicznej" (dodano podkreślenie). Zastosowanie terminu „sieć" wydaje się sugerować, że wyłącznie dane wygenerowane podczas świadczenia usług w „dolnej" warstwie sieci kwalifikowałyby się jako „metadane". Mogłoby to oznaczać, że dane wygenerowane podczas świadczenia usługi OTT byłyby wyłączone z tego zakresu. Byłoby to niepożądane i prawdopodobnie również niezamierzone, biorąc pod uwagę zamiar rozszerzenia zakresu stosowania proponowanego rozporządzenia na dostawców usług OTT. Aby rozwiązać ten problem, należy zmienić definicję „metadanych pochodzących z łączności elektronicznej", aby obejmowała ona wszystkie dane przetwarzane do celów przesyłania, dystrybuowania lub wymiany treści łączności elektronicznej.

23. Kolejną niepokojącą kwestią jest fakt, że **terytorialny zakres stosowania proponowanego rozporządzenia w odniesieniu do organizacji nieposiadających jednostki organizacyjnej w UE obejmuje wyłącznie dostawców usługi łączności elektronicznej.** Zgodnie z proponowanym rozporządzeniem dostawca usługi łączności elektronicznej nieposiadający siedziby w UE powołuje na piśmie swojego przedstawiciela w Unii (art. 3 ust. 2). W motywie 9 wskazano również, że rozporządzenie miałoby zastosowanie do przetwarzania przez dostawców usługi łączności elektronicznej niezależnie od miejsca przetwarzania. Grupa Robocza z zadowoleniem przyjmuje to wyjaśnienie. Ponieważ brzmienie tego motywu ogranicza się do dostawców usług łączności elektronicznej, niepewne jest jednak, w jakim stopniu ten terytorialny zakres stosowania obejmuje inne rodzaje stron

(przykładowo stron ingerujących w informacje przekazywane przez urządzenie końcowe użytkowników końcowych lub gromadzących takie informacje, por. art. 3 ust. 1 lit. c) w związku z art. 8 proponowanego rozporządzenia). Grupa Robocza sugeruje zatem zmianę art. 3 ust. 2 i art. 3 ust. 5, aby uwzględnić dostawców publicznie dostępnych spisów numerów, dostawców oprogramowania umożliwiającego łączność elektroniczną i osoby wysyłające materiały handlowe do celów marketingu bezpośredniego lub gromadzące (inne) informacje dotyczące urządzenia końcowego użytkowników końcowych lub przechowywane w takim urządzeniu, niezależnie od tego, czy ich działalność jest ukierunkowana na użytkowników w UE (por. motyw 8 proponowanego rozporządzenia)[13].

*NALEŻY WZMOCNIĆ OCHRONĘ URZĄDZENIA KOŃCOWEGO*

Inna kategoria obaw dotyczy niewystarczającej ochrony urządzenia końcowego w proponowanym rozporządzeniu.

24. Po pierwsze, **w proponowanym rozporządzeniu błędnie sugeruje się, że można wyrazić ważną zgodę za pośrednictwem niespecyficznych ustawień przeglądarki.** Grupa Robocza uznaje stwierdzenie, że użytkownicy końcowi są obecnie zasypywani prośbami o wyrażenie zgody (motyw 22). Ustawienia przeglądarki (i porównywalne ustawienia oprogramowania) mają do odegrania określoną rolę w rozwiązaniu tego problemu. Ponieważ ogólne ustawienia przeglądarki nie są przeznaczone do wykorzystywania w przypadku stosowania technologii śledzenia w pojedynczym konkretnym przypadku, nie są one jednak właściwe do wyrażenia zgody zgodnie z art. 7 i motywem 32 RODO (ponieważ zgoda nie jest wystarczająco świadoma i konkretna).
Użytkownik końcowy musi mieć możliwość wyrażenia osobnej zgody na śledzenie do różnych celów (takich jak udostępnienie w mediach społecznościowych lub reklamowanie) na każdej stronie internetowej lub w każdej aplikacji. Administrator danych odpowiedzialny za szereg stron internetowych lub aplikacji może również zwracać się o wyrażenie zgody dotyczącej wszystkich innych stron lub aplikacji pozostających pod jego kontrolą, o ile tego rodzaju prośba o wyrażenie zgody zostanie przedstawiona osobno.
Ponadto administrator musi się wywiązać ze wszystkich pozostałych obowiązków związanych z wyrażaniem zgody, w tym obowiązku dostarczenia użytkownikom odpowiednich informacji. W przypadku zarówno przeglądarek, jak i administratorów danych, oznacza to, że dotknięte wadą nieważności byłoby zaoferowanie przez nich jedynie wariantu „zaakceptowania wszystkich plików cookie", ponieważ uniemożliwiłby on wyrażenie przez użytkowników wymaganej każdorazowej zgody. Przeglądarki powinny jednak umożliwić użytkownikom dokonanie świadomego

[13] Zob. art. 3 ust. 2 RODO: „Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z: a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii". Obowiązek ten mógłby również obejmować wyjątki zgodnie z linią określoną w art. 27 ust. 2 RODO.

i przemyślanego wyboru zaakceptowania wszystkich plików cookie, a zatem zapobiec pojawianiu się na odwiedzanych stronach internetowych jakichkolwiek przyszłych próśb o wyrażenie szczególnej zgody.

Grupa Robocza zdecydowanie zaleca, by w rozporządzeniu w sprawie prywatności i łączności elektronicznej nałożono obowiązek wdrożenia mechanizmów technicznych w przeglądarkach, takich jak norma ochrony przed śledzeniem, aby zapewnić użytkownikom rzeczywisty wybór i rzeczywistą kontrolę nad ingerencją w ich urządzenia[14].

Co nawet istotniejsze, rozporządzenie w sprawie prywatności i łączności elektronicznej powinno zapewniać, by zarówno wybór w odniesieniu do przechowywania informacji w urządzeniu, jak i sygnału ochrony przed śledzeniem przekazywanego przez przeglądarkę był akceptowany jako prawnie wiążące wyrażenie zgody lub odmowy przez wszystkich administratorów danych. Pozostaje to bez uszczerbku dla przyszłych wskazówek Grupy Roboczej dotyczących przestrzegania normy ochrony przed śledzeniem, miedzy innymi zasady ograniczenia celu, po zakończeniu opracowywania normy (planowanym na koniec 2017 r.).

Dorozumiane rodzaje wyrażenia „zgody", takie jak kliknięcie strony internetowej lub przewinięcie strony, nie mogą zastąpić wyborów dotyczących przechowywania i sygnału ochrony przed śledzeniem. Istotna korzyść stosowania tej normy polega na tym, że nie jest ona ograniczona do technologii śledzenia plików cookie, lecz odnosi się również do innych rodzajów śledzenia, takich jak pobieranie odbitek linii papilarnych.

Wprowadzenie prawnie wiążącego obowiązku przestrzegania tej normy rozwiąże również inny problem związany z obecnym zastosowaniem terminu „osoby trzecie" w art. 10. Strona internetowa lub aplikacja co do zasady zawierają wiele elementów, zarówno związanych z samą stroną internetową, jak i elementów zewnętrznych. Kod zewnętrzny może zostać uruchomiony również w kontekście odwiedzonej strony internetowej, podczas gdy przesyła raporty do serwera osoby trzeciej. Trwały plik cookie może być obsługiwany przez administratora w sytuacji, gdy użytkownik odwiedza na przykład portal społecznościowy. Odnośny portal społecznościowy mógłby również zostać uznany za osobę trzecią wówczas, gdy użytkownik ten odwiedza inną stronę internetową zawierającą element interakcji z tym portalem społecznościowym. We wszystkich tych przypadkach niezależnie od tego, czy sytuacja dotyczy „dostępu do" czy też „przechowywania" informacji w urządzeniu użytkownika końcowego, stanowi ona ingerencję w urządzenie, na dokonanie której wymagane jest wyrażenie zgody (o ile nie ma zastosowania jeden z wyjątków). W ramach normy ochrony przed śledzeniem problem ten rozwiązano dzięki zastosowaniu terminów „dotyczący całej strony" i „dotyczący całego internetu". Aby poprawić pewność prawa wszystkich zainteresowanych stron, należy zatem zmienić brzmienie odniesienia do „osób trzecich" w rozporządzeniu w sprawie prywatności i łączności elektronicznej w celu uwzględnienia wszystkich podmiotów, z którymi urządzenie wchodzi w interakcję (ponieważ przechowują one informacje w urządzeniu lub mają do nich dostęp).

[14] Zob.: https://www.w3.org/TR/tracking-compliance/. W pkt 7 wyjaśniono model wyjątków oraz rozróżnienie między wyjątkami dotyczącymi całej strony a wyjątkami dotyczącymi całej sieci. Pkt 6 zawiera nadające się do odczytu maszynowego informacje, które administratorzy danych mogą dostarczyć w kontekście wymogu udzielenia informacji w celu uzyskania zgody.

Aby uzyskać zgodność normy ochrony przed śledzeniem z wysokim poziomem ochrony poufności komunikacji i ochrony danych przyznanym na mocy karty, w rozporządzeniu w sprawie prywatności i łączności elektronicznej należy określić, że prośby o śledzenie dotyczące całego internetu – w przeciwieństwie do próśb o śledzenie dotyczących całej strony – należy przedstawiać osobno, przy czym użytkownikom powinna przysługiwać swoboda uwzględnienia lub odrzucenia takich próśb. Ponadto aby chronić użytkowników przed częstymi prośbami o wyrażenie zgody, rozporządzenie w sprawie prywatności i łączności elektronicznej powinno zapewnić, by odmowa wyrażenia zgody na śledzenie dotyczące całego internetu przez konkretną organizację (za pośrednictwem normy ochrony przed śledzeniem lub osobnej listy zablokowanych) uniemożliwiała organizacji zwracanie się z przyszłymi prośbami o wyrażenie zgody przez okres co najmniej 6 miesięcy. Zasada ta nie wyklucza możliwości, by organizacja bezpośrednio odwiedzana przez użytkownika (tj. jako administrator) zwracała się z prośbą o wyrażenie zgody na własnej stronie internetowej (tj. z prośbą o wyrażenie zgody dotyczącej całej strony). W praktyce oznacza to, że przykładowo strona zapewniająca strumieniową transmisję wideo obsługująca trwałe pliki cookie może zwrócić się z prośbą o wyrażenie zgody wówczas, gdy użytkownik ten odwiedza stronę zapewniającą strumieniową transmisję wideo, lecz nie może się ponownie zwrócić z prośbą o wyrażenie zgody w okresie 6 miesięcy, jeżeli użytkownik odmówił wyrażenia zgody i odwiedza inne strony internetowe zawierające filmy wideo obsługiwane ze strony internetowej zapewniającej transmisję strumieniową.

25. Ponadto **brzmienie wyjątku dotyczącego „pomiaru odbiorców w sieci web" jest nieprecyzyjne.** W art. 8 ust. 1 lit. d) proponowanego rozporządzenia przewidziano wyjątek dotyczący pomiaru odbiorców w sieci web. Pierwszą niepokojącą kwestią jest fakt, że termin ten nie został zdefiniowany i można go pomylić z profilowaniem użytkownika. W definicji należy wskazać expressis verbis, że niedopuszczalne jest stosowanie przedmiotowego wyjątku do jakichkolwiek celów związanych z profilowaniem. Wyjątek ten powinien mieć zastosowanie wyłącznie do analityki użytkowania koniecznej do przeprowadzenia analizy dostarczenia usługi żądanej przez użytkownika, lecz nie do analityki użytkownika (tj. analizy zachowania możliwych do zidentyfikowania użytkowników strony internetowej, aplikacji lub urządzenia). W związku z tym danego wyjątku nie można stosować w okolicznościach, gdy dane można powiązać z pozwalającymi na identyfikację danymi użytkownika, które są przetwarzane przez dostawcę lub innych administratorów danych. Ponadto jego opis wskazuje na bardzo specyficzne dla danej technologii zastosowanie. Termin „pomiar odbiorców w sieci web" powinien zatem zostać na nowo zdefiniowany w sposób neutralny technologicznie w celu włączenia również podobnych informacji analitycznych dotyczących użytkowania pochodzących z aplikacji, urządzeń do noszenia na ciele i urządzeń podłączonych do internetu rzeczy.

Grupa Robocza sugeruje czerpanie inspiracji z wyjątku niderlandzkiego, który ma zastosowanie, gdy jest to ściśle niezbędne do uzyskania informacji na temat jakości technicznej lub skuteczności świadczonej usługi społeczeństwa informacyjnego oraz nie ma wpływu na prywatność abonenta lub zaangażowanego użytkownika

końcowego lub ma niewielki wpływ (por. art. 11.7a ust. 3 lit. b) niderlandzkiej ustawy telekomunikacyjnej). Wyjątek ten uwzględnia fakt, że większość danych zebranych za pośrednictwem analityki stron internetowych lub aplikacji to nadal dane osobowe. Oznacza to, że przetwarzanie tych danych również podlega RODO. Sugeruje to na przykład, że analityka użytkowania może być również przeprowadzana przez zewnętrzną organizację, ale tylko wtedy, gdy:
(i) organizacja ta działa jako przetwarzający;
(ii) zawarto umowę o przetwarzaniu zgodnie z RODO;
(iii) zastosowana technologia analityczna uniemożliwia ponowną identyfikację, w tym m.in. anonimizację adresów IP od użytkowników;
(iv) określone pliki cookie lub inne dane stosowane do celów analitycznych można wykorzystać wyłącznie w odniesieniu do danej strony internetowej, aplikacji lub urządzenia do noszenia na ciele i nie można powiązać z innymi danymi pozwalającymi na identyfikację;
(v) użytkownicy mają prawo do rezygnacji (zob. również uwagi 17 i 50 w niniejszej opinii).

Nawet jeżeli zgoda nie byłaby wymagana w przypadku spełnienia tych warunków, administratorzy danych muszą nadal dostarczać użytkownikom odpowiednie informacje, np. za pomocą pól reprezentujących status śledzenia w funkcji „ochrona przed śledzeniem”[15].

26. Rozporządzenie w sprawie prywatności i łączności elektronicznej **powinno zapewniać wąsko i precyzyjnie sformułowane wyjątki od wymogów uzyskania zgody.** Brzmienie wyjątku od obowiązku uzyskania zgody w odniesieniu do ingerowania w urządzenia, który przedstawiono w art. 8 ust. 1 lit. c), jest niemal identyczne z obecnym brzmieniem art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej: „jest to szczególnie niezbędne w celu dostarczania usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika”, ale bez żadnego wyjaśnienia pominięto kluczowe słowo „szczególnie”. Budzi to niepokój z dwóch powodów. Po pierwsze, przepis zawarty w dyrektywie o prywatności i łączności elektronicznej już doprowadził do szerokiej dyskusji między organami nadzorczymi i organizacjami na temat jego zakresu, a skreślenie słowa „szczególnie” zapewni jeszcze mniejszą pewność prawa. Jest to niepokojące również dlatego, że Grupa Robocza przedstawiła już wytyczne dotyczące interpretacji terminu „szczególnie” w tym kontekście. Grupa Robocza zaproponowała następujące wyjaśnienie w opinii w sprawie wyłączenia zapisywania plików cookie spod zasady pozyskiwania zgody (WP 194):
„Plik cookie jest konieczny do zaoferowania użytkownikowi (lub abonentowi) konkretnej funkcji: funkcja nie będzie dostępna przy wyłączonej obsłudze plików cookie, zaś użytkownik (lub abonent) wyraźnie zażądał tej funkcji, jako części usługi społeczeństwa informacyjnego”[16].

[15] Zob.: Tracking Preference Expression (DNT), projekt redakcyjny z dnia 7 marca 2016 r.

[16] Opinia 04/2012 w sprawie wyłączenia zapisywania plików cookie spod zasady pozyskiwania zgody Grupy Roboczej Art. 29, WP 294, przyjęta w dniu 7 czerwca 2012 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_pl.pdf

Ponadto Grupa Robocza wyjaśniła, że:

„Pliki cookie »osób trzecich« przeważnie nie są »ściśle niezbędne« dla użytkownika odwiedzającego stronę, gdyż zwykle odnoszą się do usługi innej niż ta, której użytkownik »wyraźnie zażądał«[17]".
Grupa Robocza dodała, że korzystanie z wtyczek społecznościowych skierowanych do osób niebędących użytkownikami platformy ani strony internetowej również nie byłoby uważane za ściśle niezbędne.

Ponadto, podczas gdy w art. 6 ust. 1 lit. b) proponowanego rozporządzenia zezwala się na przetwarzanie danych pochodzących z łączności elektronicznej, o ile jest to „konieczne" do celów bezpieczeństwa, w motywie 49 RODO wymaga się, aby było to bezwzględnie niezbędne. Pominięcie słowa „bezwzględnie" mogło nie być zamierzone, ponieważ w motywie 21 proponowanego rozporządzenia wspomniano, że zgoda na ingerencję nie powinna być wymagana, gdy ingerencja jest „absolutnie" niezbędna. Proponowane rozporządzenie zapewnia jednak możliwość dalszego wyjaśnienia, że warunek konieczności w kontekście tego rozporządzenia powinien być interpretowany ściśle w odniesieniu do wszystkich wyjątków. Grupa Robocza proponuje zatem, aby w odniesieniu do wszystkich wyjątków przedstawionych w art. 6 i art. 8 ust. 1 proponowanego rozporządzenia dodano słowo „absolutnie" przed „konieczne".

Z drugiej strony rozporządzenie w sprawie prywatności i łączności elektronicznej powinno wyraźnie dopuszczać możliwość ingerowania w urządzenia w celu zainstalowania aktualizacji zabezpieczeń. Przesyłanie aktualizacji zabezpieczeń przez internet jest preferowaną metodą instalowania aktualizacji zabezpieczeń na większości urządzeń użytkowników końcowych. Instalowanie aktualizacji uważa się za ingerencję w urządzenie końcowe. Zapewnienie aktualnych zabezpieczeń na tych urządzeniach stanowi uzasadniony interes. Zasadniczo dostawca poprawek zabezpieczeń powinien zatem móc zainstalować absolutnie konieczne aktualizacje zabezpieczeń bez zgody użytkownika końcowego. Nie jest jednak pewne, czy w przypadku takiej ingerencji można skorzystać z wyjątku od zakazu ingerencji dotyczącego „społeczeństwa informacyjnego" (art. 8 ust. 1 lit. c)). Należy wyjaśnić, że instalacja aktualizacji zabezpieczeń jest dozwolona w ramach tego wyjątku, ale tylko w takim zakresie, w jakim (i) aktualizacje zabezpieczeń są dyskretnie pakowane i w żaden sposób nie zmieniają funkcji oprogramowania zainstalowanego na urządzeniu (z uwzględnieniem interakcji z innym oprogramowaniem lub innymi ustawieniami wybranymi przez użytkownika), (ii) użytkownik końcowy jest informowany z wyprzedzeniem o każdej instalowanej aktualizacji oraz (iii) użytkownik końcowy może wyłączyć automatyczną instalację takich aktualizacji.

## *MARKETING BEZPOŚREDNI*

[17] *Ibid.*

Inną kategorią budzącą obawy jest niewystarczająca ochrona przed marketingiem bezpośrednim.

27. Po pierwsze, niepokojące jest to, że **zakres marketingu bezpośredniego jest zbyt ograniczony**. W art. 4 ust. 3 lit. f) proponowanego rozporządzenia „komunikaty marketingu bezpośredniego" definiuje się jako „wszelkie formy reklamowania, pisemne lub ustne, przesyłane jednemu zidentyfikowanemu lub dającemu się zidentyfikować użytkownikowi końcowemu usług łączności elektronicznej lub większej ich liczbie". Użycie słowa „przesyłane" sugeruje wykorzystanie łączności technologicznej, co oznacza, że z konieczności wiąże się ono z przekazywaniem komunikatów, podczas gdy większość przypadków reklamowania w sieci (poprzez platformy społecznościowe lub na stronach internetowych) nie wiąże się z „przesyłaniem" reklam w ścisłym znaczeniu tego słowa. Zostało to dodatkowo podkreślone przykładami przedstawionymi w tej definicji (SMS, wiadomość e-mail) i w motywie 33. Wszystkie przykłady odnoszą się do stosunkowo tradycyjnych form komunikacji marketingowej, a nawet wtedy wykorzystanie – dosyć tradycyjnych – systemów wywoływania nie jest zapewne objęte ich zakresem. Artykuł i motyw należy zmienić, aby uwzględnić wszystkie reklamy *przesłane lub przedstawione* jednemu zidentyfikowanemu lub dającemu się zidentyfikować użytkownikowi końcowemu lub większej ich liczbie bądź do nich *skierowane*. Ponadto należy zapewnić, aby reklamy behawioralne (bazujące na profilach użytkowników końcowych) również uznawano za komunikaty marketingu bezpośredniego skierowywane do „jednego zidentyfikowanego lub dającego się zidentyfikować użytkownika końcowego lub większej ich liczby" (jako że takie reklamy są skierowane do konkretnych, dających się zidentyfikować użytkowników).

    Co więcej, w ramach proponowanego zakresu „komunikatów marketingu bezpośredniego" ochrona na mocy art. 16 ust. 1 byłaby ograniczona do wiadomości zawierających materiały reklamowe i nie ustrzegłaby osób fizycznych przed innymi wiadomościami przesyłanymi, kierowanymi lub przedstawianymi do celów marketingowych (takimi jak wiadomości najnowszej generacji wymagające zgody, promowanie poglądów politycznych lub preferencji wyborczych, wspieranie organizacji charytatywnych lub innych organizacji nienastawionych na zysk lub ogólna promocja organizacji). Ponadto w dalszym ciągu jako metodę marketingu bezpośredniego wykorzystuje się faksy, chociaż nie wspomniano o nich w definicji. Art. 4 ust. 3 lit. f) powinien zatem obejmować wszystkie formy reklamowania, pozyskiwania lub promowania, także w odniesieniu do organizacji nienastawionych na zysk, oraz powinien wyraźnie uwzględniać faksy obok wiadomości e-mail i SMS (zob. także sugestię wymagającą wyjaśnienia w uwadze 43 lit. a)). Co więcej, w motywie 32 stwierdza się, że marketing bezpośredni obejmuje wiadomości wysłane przez partie polityczne, aby promować swoje partie. Motyw ten należy zaktualizować, tak aby uwzględniał polityków i kandydatów startujących w wyborach, którzy promują swoją kandydaturę.

28. Po drugie, **wycofanie zgody na marketing bezpośredni nie jest nieodpłatne ani równie łatwe jak jej wyrażenie.** Należy wyjaśnić możliwość wycofania zgody na mocy proponowanego rozporządzenia, aby zapewnić spójność i poprawić ochronę odbiorców. Art. 16 ust. 6 proponowanego rozporządzenia stanowi obecnie, że

odbiorcy marketingu bezpośredniego muszą otrzymać „informacje niezbędne odbiorcom do wykonania ich prawa do wycofania w łatwy sposób zgody na dalsze otrzymywanie komunikatów marketingowych" (podkreślenie dodane). Powyższe znajduje potwierdzenie w motywie 34. Z motywu 70 RODO wynika jednak, że osoby, których dane dotyczą, na mocy RODO powinny nie tylko mieć prawo wnieść w łatwy sposób sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, ale także prawo do dokonania tego „nieodpłatnie". Termin ten występuje także w art. 16 ust. 2 proponowanego rozporządzenia, ale jedynie w odniesieniu do opcji rezygnacji z marketingu bezpośredniego na podstawie danych kontaktowych uzyskanych w związku ze sprzedażą.

Art. 7 ust. 3 RODO stanowi, że wycofanie zgody musi być równie łatwe jak jej wyrażenie, a osoby fizyczne powinny móc w dowolnym momencie wycofać zgodę. Ponadto w opinii 4/2010 w sprawie FEDMA (WP 174) Grupa Robocza uznała już znaczenie zaoferowania „prostej, skutecznej, bezpłatnej, bezpośredniej i łatwo dostępnej metody, która umożliwi rezygnację" z marketingu bezpośredniego[18]. Ta norma dotycząca cofnięcia zgody powinna zostać włączona do przepisów dotyczących marketingu bezpośredniego w proponowanym rozporządzeniu. To samo dotyczy wymogu określonego w art. 7 ust. 3 RODO, zgodnie z którym wycofanie zgody powinno być równie łatwe w dowolnym momencie jak jej wyrażenie.

29. W związku z powyższym **należy wyjaśnić, w jaki sposób można wycofać zgodę lub zrezygnować z połączeń wykonywanych w ramach marketingu bezpośredniego**. Na podstawie art. 16 ust. 4 proponowanego rozporządzenia państwa członkowskie mogą wybrać system oparty na mechanizmie rezygnacji w odniesieniu do połączeń głosowych w ramach marketingu. Rozporządzenie w sprawie prywatności i łączności elektronicznej *powinno* określać ustalenia dotyczące wycofania zgody i rezygnacji z połączeń marketingowych. Zgodnie z motywem 36 państwa członkowskie powinny móc ustanowić lub utrzymać krajowe systemy rezygnacji. Na podstawie tego przepisu państwa członkowskie mogłyby nawet dopuścić do sytuacji, w której użytkownik musiałby zrezygnować z poszczególnych dostawców łączności elektronicznej. Stosowanie takiego przepisu nie chroni użytkowników przed naruszeniami związanymi z nieuzasadnioną komunikacją[19] ani nie zapewnia mechanizmu zgodnego z RODO umożliwiającego w łatwy sposób wycofanie zgody w dowolnym momencie. W rozporządzeniu *należy* zatem określić, że każde państwo członkowskie musi utworzyć krajowy rejestr „nieoddzwaniania". Ponadto w rozporządzeniu należy wskazać, że odbiorcy połączeń głosowych powinni mieć do wyboru dwie możliwości wycofania zgody: podczas przyszłych połączeń

[18] Opinia 4/2010 na temat europejskiego kodeksu postępowania Europejskiej Federacji Stowarzyszeń Marketingu Bezpośredniego (FEDMA) w sprawie ochrony danych osobowych wykorzystywanych w marketingu bezpośrednim Grupy Roboczej Art. 29 (WP 174), przyjęta w dniu 13 lipca 2010 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_pl.pdf

[19] Na przykład w Zjednoczonym Królestwie operator telekomunikacyjny BT zarejestrował 31 mln uciążliwych połączeń w tygodniu. Zob.: http://www.bbc.com/news/business-38635921

z danego przedsiębiorstwa lub organizacji oraz możliwość zarejestrowania w trakcie takich połączeń w krajowym rejestrze „nieoddzwaniania".

30. Inną kwestią budzącą niepokój jest **używanie fałszywych tożsamości, gdy wysyłanie komunikatów marketingu bezpośredniego nie jest w sposób wyraźny zabronione.** W motywie 34 zauważa się, że należy zakazać „maskowania tożsamości i korzystania z fałszywej tożsamości, fałszywych adresów zwrotnych lub numerów przy wysyłaniu niezamówionych informacji handlowych do celów marketingu bezpośredniego". W art. 16 ust. 4 stwierdza się jednak, że użytkownicy końcowi są informowani o „tożsamości osoby prawnej lub fizycznej, w której imieniu przekazywane są komunikaty". Obowiązek informowania odbiorców o tożsamości powinien zostać uzupełniony wyraźnym zakazem stosowania ukrytych lub fałszywych adresów kontaktowych do celów marketingu bezpośredniego.

31. Ten punkt odnosi się do kolejnej kwestii budzącej niepokój: **wymogu podania prefiksu dla połączeń wykonywanych w ramach marketingu bezpośredniego, który przedstawiono jako alternatywę dla wymogu identyfikacji rozmów przychodzących.** Zgodnie z art. 16 ust. 3 zezwala się na połączenia w ramach marketingu bezpośredniego, jeżeli rozmówca albo (i) podaje identyfikator linii, pod którą można się skontaktować z osobą fizyczną lub prawną wykonującą połączenie (art. 16 ust. 3 lit. a)), albo (ii) podaje konkretny kod lub prefiks umożliwiający rozpoznanie, że połączenie jest połączeniem marketingowym (art. 16 ust. 3 lit. b)). Chociaż Grupa Robocza z zadowoleniem przyjmuje obowiązek określony w art. 16 ust. 3 lit. b) dotyczący stosowania prefiksu, uważa, że wymóg ten nie odnosi się do tej samej kwestii, której dotyczy obowiązek identyfikacji rozmów przychodzących określony w art. 16 ust. 3 lit. a). Chociaż wymóg prefiksowania ma na celu umożliwienie odbiorcy wcześniejsze zidentyfikowanie połączenia jako połączenie marketingowe (oraz wdrożenie środków blokujących takie połączenia), wymóg identyfikacji rozmów przychodzących ma na celu zapewnienie odbiorcom (i organom nadzorczym) środków do identyfikowania i kontaktowania się z inicjatorem połączeń marketingowych. Ma to szczególne znaczenie jeżeli chodzi o połączenia zautomatyzowane, w przypadku których występuje znaczący brak równowagi między możliwościami marketera w zakresie nawiązywania uciążliwych połączeń a możliwościami odbiorcy w zakresie ich unikania. Wymogi te nie mogą zatem stanowić rozwiązań alternatywnych, lecz muszą się wzajemnie uzupełniać.

*HARMONOGRAM*

32. Grupa Robocza Art. 29 pochwala Komisję Europejską za uznanie konieczności wprowadzenia w życie proponowanego rozporządzenia wraz z RODO w maju 2018 r. w celu uniknięcia niespójności między tymi dwoma aktami ustawodawczymi. Nadal jednak niepokoi fakt, że jest to ambitny harmonogram, który wymaga również opracowania Europejskiego kodeksu łączności elektronicznej. W związku z tym Grupa Robocza Art. 29 wzywa wszystkie zainteresowane strony uczestniczące w procesie legislacyjnym do przestrzegania terminu wyznaczonego na maj 2018 r.

*INNE KWESTIE BUDZĄCE OBAWY*

W niniejszej sekcji omówiono szereg dodatkowych kwestii budzących obawy.

33. Po pierwsze, Grupa Robocza Art. 29 jest zaniepokojona **sugestią, że dopuszcza się stosowanie nieukierunkowanych środków zatrzymywania danych.** W uzasadnieniu zauważono, że zgodnie z proponowanym rozporządzeniem państwa członkowskie mogą utrzymać lub stworzyć krajowe ramy zatrzymywania danych, które przewidują m.in. środki ukierunkowanego zatrzymywania danych (pkt 1.3). W następstwie orzeczenia w sprawie Tele2/Watson[20] oczywiste jest, że na mocy karty nie dopuszcza się do stosowania ram zatrzymywania danych przewidujących jakiekolwiek inne niż ukierunkowane zatrzymywanie danych (a nawet wtedy podlegają one ważnym warunkom takim jak nadzór) oraz że uogólniony dostęp do metadanych będzie musiał być postrzegany jako naruszający istotę art. 7 w taki sam sposób, jak uogólniony dostęp do treści komunikacji elektronicznej (por. Trybunał Sprawiedliwości Unii Europejskiej, Schrems oraz motyw 94). Z takiego sformułowania zdania wynika, że państwa członkowskie dysponują pewnym polem manewru, jeżeli chodzi o środki zatrzymywania danych, które de facto nie istnieje. W związku z tym **metadane nie są objęte wystarczającym poziomem ochrony** w proponowanym rozporządzeniu. Jak wynika z uwagi 10 Grupa Robocza Art. 29 z zadowoleniem przyjęła uznanie faktu, że metadane mogą ujawniać bardzo wrażliwe dane. Metadane określone w proponowanym rozporządzeniu nie są objęte ochroną, która powinna wynikać z tego uznania. Z uwagi na wrażliwość metadanych, w szczególności przed dokonaniem analizy na mocy art. 6 ust. 2 lit. c), należy przeprowadzić ocenę skutków dla ochrony danych (zob. również uwaga 46).

34. Po drugie, **proponowane rozporządzenie nadmiernie rozszerzyłoby możliwości w zakresie zatrzymywania danych**. Art. 11 proponowanego rozporządzenia odnosi się do art. 23 ust. 1 lit. a)–e) RODO, jeżeli chodzi o opis celów, dla których państwa członkowskie mogą ograniczyć obowiązki i prawa przewidziane w art. 5–8 rozporządzenia. W RODO nie przewiduje się takich ograniczeń w odniesieniu do szczególnych kategorii danych, zgodnie z wysokim ryzykiem na jakie narażone są osoby, których dane dotyczą. Chociaż w art. 15 dyrektywy o prywatności i łączności elektronicznej zezwala się obecnie na stosowanie podobnego ograniczenia, cele są bardziej ograniczone. Na mocy nowego proponowanego rozporządzenia możliwe byłoby wprowadzenie nowych ograniczeń służących „wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom" (art. 23 ust. 1 lit. d) RODO) oraz „innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu" (art. 23 ust. 1 lit. e) RODO). Cele te są nie tylko nowe w porównaniu z dyrektywą o prywatności i łączności elektronicznej, ostatni cel określony w art. 23 ust. 1 lit. d) i cały cel określony w art. 23 ust. 1 lit. e) sformułowano bardzo szeroko. Proponuje się zatem usunięcie odniesienia do art. 23

[20] ECLI:EU:C:2016:970: http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203

ust. 1 lit. a)–e) RODO, a zamiast tego wymienienie tylko celów obecnie wspomnianych w art. 15 dyrektywy o prywatności i łączności elektronicznej.

35. **Obowiązek informowania użytkowników o ryzyku w zakresie bezpieczeństwa ma minimalistyczny zakres**. Grupa Robocza z zadowoleniem przyjmuje fakt, że dostawcy usług muszą informować użytkowników o ryzyku w zakresie bezpieczeństwa i środkach eliminujących tego rodzaju ryzyko, takich jak szyfrowanie (art. 17 i motyw 37). Tytuł tego przepisu brzmi jednak: „Informacje o wykrytym ryzyku w zakresie bezpieczeństwa". Fakt, że w tytule jest mowa o wykrytym ryzyku sugeruje, że przepis ten dotyczy wyłącznie (potencjalnych) naruszeń bezpieczeństwa, podczas gdy w treści tego przepisu i motywu zwraca się większą uwagę na ogólne kształcenie użytkowników końcowych. Przykładowo jeżeli dostawca usług wykryje, że urządzenie użytkownika jest zainfekowane złośliwym oprogramowaniem i stało się częścią botnetu, wydaje się, że przepis ten nakłada na dostawcę bezpośredni obowiązek poinformowania użytkownika o wynikających z tego zagrożeniach. Można byłoby jednak doprecyzować zakres stosowania tego przepisu, przy czym nie powinien on być ograniczony do tego konkretnego scenariusza. Przepis ten powinien obejmować co najmniej ryzyko dla bezpieczeństwa wykryte we wszystkich urządzeniach dostarczonych użytkownikowi końcowemu przez dostawcę w ramach abonamentu, takich jak na przykład routery i urządzenia mobilne, oraz obejmować pouczenie na temat zagrożeń związanych ze zmianą ustawień dokonanych w ramach ochrony prywatności zgodnie z zasadą uwzględnienia ochrony prywatności już w fazie projektowania.

    Grupa Robocza zaleca rozszerzenie zakresu stosowania, aby uwzględnić dostawców oprogramowania umożliwiającego łączność elektroniczną (por. motyw 8) oraz być może również nową kategorię: dostawców technologii kluczowej dla zapewnienia łączności niebędących dostawcami usług (np. dostawców technologii szyfrowania). W przypadku ostatniego rozszerzenia należy zwrócić uwagę, by obowiązek ten nie pokrywał się z obowiązkami w zakresie zgłaszania naruszenia bezpieczeństwa przewidzianymi w innych instrumentach, takich jak dyrektywa w sprawie bezpieczeństwa sieci i informacji[21] i inne instrumenty prawne dotyczące dostawców certyfikatów. Ponieważ ostatnia kategoria dostawców technologii co do zasady nie pozostaje w bezpośrednim kontakcie z użytkownikami końcowymi, należy również doprecyzować, w jaki sposób mogą oni wypełniać spoczywający na nich obowiązek informacyjny przewidziany w tym przepisie.

36. Grupa Robocza z zadowoleniem przyjmuje przepisy art. 2 i 13, które będą miały zastosowanie do usług łączności interpersonalnej wykorzystującej numery. Nie jest jednak prima facie oczywiste, dlaczego **podobny poziom ochrony prywatności nie powinien być również zapewniony równoważnym funkcjonalnie usługom połączeń OTT.**

[21] 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, http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.POL

37. Grupa Robocza jest również zaniepokojona **brakiem jednoznaczności w odniesieniu do każdorazowej zgody na wyszukiwanie zwrotne w spisach numerów.** W art. 15 ust. 2 proponowanego rozporządzenia zobowiązano dostawców do uzyskania zgody użytkowników końcowych przed aktywowaniem funkcji wyszukiwania w odniesieniu do ich danych (zob. również motyw 31). Grupa Robocza z zadowoleniem przyjmuje harmonizację wymogu uzyskania zgody na umieszczenie w spisie numerów, lecz ubolewa nad brakiem szczegółowości w odniesieniu do różnych rodzajów wyszukiwań. Dyrektywa o prywatności i łączności elektronicznej w obecnym brzmieniu uprawnia państwa członkowskie do wprowadzenia wymogu uzyskania osobnej zgody na wyszukiwanie zwrotne na podstawie art. 12 ust. 3. Artykuł ten stanowi, co następuje: „państwa członkowskie mogą wymagać, aby dla jakiegokolwiek celu publicznego spisu abonentów innego niż przeszukiwanie danych do kontaktu osób, na podstawie podania ich nazwiska oraz, w miarę potrzeb, minimalnej ilości innych danych identyfikacyjnych, wymagana była dodatkowa zgoda abonentów". Na mocy tego przepisu w wielu państwach członkowskich wymagana jest osobna zgoda na funkcje wyszukiwania zwrotnego, biorąc pod uwagę różne poziomy identyfikowalności, a zatem inwazyjności obydwu funkcji.

38. Z bardziej formalnego punktu widzenia **poziom kar pieniężnych nie jest ujednolicony w odniesieniu do wszystkich naruszeń rozporządzenia.** Na mocy proponowanego rozporządzenia państwa członkowskie określają zasady nakładania kar za naruszenia art. 23 ust. 4, art. 23 ust. 6 i art. 24 proponowanego rozporządzenia. Bardziej konsekwentne byłoby uwzględnienie tej kwestii również w samym rozporządzeniu w sprawie prywatności i łączności elektronicznej.

39. Ponadto **proponowane rozporządzenie opiera się na definicjach, które mogą się stać „ruchomymi celami".** W przypadku szeregu kluczowych koncepcji proponowane rozporządzenie odnosi się do innego instrumentu prawnego, który obecnie znajduje się w formie projektu: proponowanego Europejskiego kodeksu łączności elektronicznej (zob. na przykład art. 4 ust. 1 lit. b)). Dwa istotne przykłady ilustrujące ten problem obejmują definicję „użytkownika końcowego", która uwzględnia obecnie osoby fizyczne i prawne, oraz definicje „usługi łączności elektronicznej" i „usługi łączności interpersonalnej" odzwierciedlone w art. 4 ust. 1 lit. b) proponowanego rozporządzenia, przy czym ostatnią definicję w dalszym stopniu doprecyzowano w art. 4 ust. 2 w celu uwzględnienia rodzajów usług wyłączonych expressis verbis w Europejskim kodeksie łączności elektronicznej[22]. Niniejsza opinia opiera się na definicjach w ich obecnym brzmieniu, jednak całkiem prawdopodobna jest zmiana proponowanego Europejskiego kodeksu łączności

[22] Przykładowo art. 4 ust. 2 proponowanego rozporządzenia stanowi, że usługa łączności interpersonalnej „obejmuje usługi, które umożliwiają komunikację interpersonalną i interaktywną chociażby w ramach pomniejszej funkcji wspomagającej, która jest nieodłącznie powiązana z inną usługą", natomiast art. 2 pkt 5 Europejskiego kodeksu łączności elektronicznej expressis verbis wyklucza tego rodzaju usługi z zakresu tej definicji. (W art. 2 pkt 4 Europejskiego kodeksu łączności elektronicznej włączono „usługę łączności interpersonalnej" do szerszej kategorii „usługi łączności elektronicznej".)

elektronicznej lub jego kluczowych pojęć. Miałoby to bezpośrednie skutki również dla rozporządzenia w sprawie prywatności i łączności elektronicznej. W idealnym scenariuszu wszystkie terminy zaczerpnięte z Europejskiego kodeksu łączności elektronicznej należałoby niezależnie zdefiniować w rozporządzeniu w sprawie prywatności i łączności elektronicznej; lub – jako minimum – proponowane rozporządzenie powinno zawierać wyjaśnienie, w przypadku gdy istnieją jakiekolwiek terminy, których definicje różnią się od definicji zawartych w Europejskim kodeksie łączności elektronicznej (np. wskazane powyżej włączenie „usług pomocniczych" do definicji „usługi łączności interpersonalnej"). W braku takiej możliwości Grupa Robocza chciałaby jednak zasugerować wszystkim stronom uczestniczącym w procesie legislacyjnym zapewnienie, by dyskusję oraz głosowanie zarówno nad proponowanym rozporządzeniem, jak i Europejskim kodeksem łączności elektronicznej, przeprowadzono jednocześnie, aby umożliwić zainteresowanym stronom poprawną ocenę zakresu stosowania oraz skutków nowych instrumentów.

## 5. SUGESTIE DOTYCZĄCE DOPRECYZOWANIA W CELU ZAGWARANTOWANIA PEWNOŚCI PRAWA

Oprócz kwestii omówionych powyżej Grupa Robocza pragnie również podkreślić, że korzystne byłoby doprecyzowanie niektórych przepisów proponowanego rozporządzenia. Tego rodzaju wyjaśnienia uznaje się za konieczne, aby zwiększyć pewność prawa dla wszystkich zainteresowanych stron odnośnie do jednolitości wykładni i stosowania rozporządzenia w sprawie prywatności i łączności elektronicznej w całej UE.

*DOPRECYZOWANIE ZAKRESU STOSOWANIA*

40. Jeżeli chodzi o zakres stosowania proponowanego rozporządzenia, Grupa Robocza sugeruje następujące wyjaśnienia:

    a. **Termin „użytkownik końcowy" powinien obejmować wszystkich indywidualnych użytkowników.** W art. 2 pkt 14 Europejskiego kodeksu łączności elektronicznej zdefiniowano „użytkownika końcowego" jako użytkownika, który nie udostępnia publicznych sieci łączności ani publicznie dostępnych usług łączności elektronicznej. Należy doprecyzować, że osoby fizyczne wnoszące wkład w sieci – na przykład sieci kratowe (ang. *mesh network)* za pośrednictwem swojego routera bezprzewodowego – nie są wyłączone z zakresu ochrony proponowanego rozporządzenia.
    b. **Należy doprecyzować, że terytorialny zakres stosowania obejmuje wszystkich użytkowników końcowych w Unii.** Art. 3 ust. 1 lit. a) stanowi, że proponowane rozporządzenie ma zastosowanie do świadczenia usług łączności elektronicznej na rzecz użytkowników końcowych „w Unii", natomiast art. 3 ust. 1 lit. c) stanowi, że ma ono zastosowanie do ochrony informacji związanych z urządzeniem końcowym użytkowników końcowych „znajdujących się w Unii" (dodano podkreślenie). Brzmienie to różni się w poszczególnych tłumaczeniach. Niemieckie tłumaczenie nie zawiera tego rozróżnienia w przeciwieństwie do innych tłumaczeń, takich jak tłumaczenie francuskie, hiszpańskie i niderlandzkie. Z motywu 9 expressis verbis wynika,

że zamierzony terytorialny zakres stosowania jest szeroki, niezależnie od tego, czy usługi są świadczone spoza Unii, czy też przetwarzanie odbywa się w Unii. Sugeruje się zatem usunięcie terminu „znajdujące się" zawartego w art. 3 ust. 1 lit. c), aby podkreślić ten szeroki zakres stosowania.

c. **Wydaje się, że proponowane rozporządzenie chroni poufne komunikaty wyłącznie podczas ich *przesyłania*, a nie podczas *przechowywania*.** Zgodnie z obecnym podejściem zastosowanym w proponowanym rozporządzeniu należy się skoncentrować na ochronie przesyłu komunikatów. Zob. na przykład motyw 15, który stanowi, że zakaz przechwytywania danych pochodzących z łączności powinien obowiązywać podczas ich przekazywania, tj. do czasu otrzymania treści łączności elektronicznej przez docelowego odbiorcę. Zakres tej ochrony opiera się na koncepcyjnych ramach łączności, które są przestarzałe. Większość danych pochodzących z łączności nadal jest przechowywana przez dostawców usług, nawet po ich otrzymaniu. Należy zapewnić ochronę poufności tych danych. Ponadto komunikacja między abonentami tych samych usług opartych na chmurze (na przykład dostawcami aplikacji webmail) będzie się często wiązała z bardzo niewielkim zakresem przekazywania: wysłanie wiadomości e-mail wiązałoby się przede wszystkim z odzwierciedleniem tego faktu w bazie danych dostawcy, a nie z faktyczną wymianą komunikatów pomiędzy dwoma stronami. Argument, że kwestia ta jest już objęta zakresem stosowania RODO, jest nieprzekonujący: całościowym celem proponowanego rozporządzenia jest ochrona całej poufnej komunikacji niezależnie od związanych z nią środków technicznych. Istnieje możliwość, że jest to zwykła omyłka pisarska, ponieważ zakaz przewidziany w art. 5 odnosi się do „przechowywania" i „przetwarzania".

d. **Wszystkie publiczne hotspoty zapewniające dostęp do internetu bezprzewodowego powinny być objęte tym zakresem stosowania.** Ponieważ korzystanie z bezprzewodowych hotspotów jest powszechne, całkowicie logiczne jest, że nie powinny istnieć żadne wątpliwości co do ochrony poufności komunikacji przekazywanej za pośrednictwem takich hotspotów. Dokonana w rozporządzeniu próba wyjaśnienia tej kwestii jest jednak nieudana, ponieważ zakres stosowania rozszerzono wyłącznie na sieci udostępniane „nieokreślonej grupie użytkowników końcowych" (motyw 13). Należy zdefiniować terminy „nieokreślona grupa użytkowników końcowych" oraz „zamknięta grupa użytkowników końcowych". W szczególności należy doprecyzować, że bezpieczne sieci bezprzewodowe (tj. zabezpieczone hasłem) również są objęte zakresem stosowania w przypadku podania tego hasła teoretycznie nieokreślonej grupie użytkowników, których tożsamości nie można z góry ustalić (np. klientom kawiarni, odwiedzającym port lotniczy). Podstawowa zasada w tym kontekście stanowi, że zgodnie z poprzednią opinią Grupy Roboczej dotyczącą przeglądu dyrektywy o prywatności i łączności elektronicznej „jedynie usługi świadczone w sytuacji urzędowej lub sytuacji zatrudnienia wyłącznie do celów zawodowych lub urzędowych lub do celów komunikacji technicznej między podmiotami niepublicznymi lub podmiotami publicznymi wyłącznie w celu kontroli pracy lub procesów biznesowych, jak również korzystanie z usług

wyłącznie do celów wewnętrznych można wyłączyć z zakresu instrumentu na rzecz prywatności i łączności elektronicznej" (s. 8).

e. **Dane zgromadzone podczas świadczenia usług cyfrowej transmisji powinny być objęte zakresem stosowania proponowanego rozporządzenia.** Biorąc pod uwagę wrażliwy charakter czynności przeglądania, ponieważ ujawnia ona osobiste zainteresowania i cechy charakterystyczne przeglądających, w rozporządzeniu w sprawie prywatności i łączności elektronicznej należy wskazać (na przykład w jednym z motywów), że wyłączenie usług przekazywania „treści przekazywanych przy wykorzystaniu sieci [...] łączności elektronicznej" z zakresu definicji „usługi łączności elektronicznej" nie oznacza, że dostawcy usług oferujący zarówno usługi łączności elektronicznej, jak i usługi w zakresie treści, nie są objęci zakresem stosowania przepisów rozporządzenia w sprawie prywatności i łączności elektronicznej, które jest ukierunkowane na dostawców usług łączności elektronicznej. Jest to szczególnie istotne, ponieważ świadczenie usług przekazywania „treści przekazywanych przy wykorzystaniu sieci [...] łączności elektronicznej" jest wyłączone z zakresu definicji „usługi łączności elektronicznej" zgodnie z proponowanym Europejskim kodeksem łączności elektronicznej (art. 2 pkt 4).

f. **Dane pochodzące z łączności co do zasady stanowią dane osobowe.** W motywie 4 zauważono, że dane pochodzące z łączności mogą zawierać dane osobowe. Większość danych pochodzących z łączności stanowi jednak dane osobowe[23], przy czym w znacznej mierze mają one raczej osobisty i wrażliwy charakter, a zatem brzmienie tego motywu należy zmienić w taki sposób, by wskazywał on, że dane te co do zasady stanowią dane osobowe.

g. **Poufna komunikacja obejmuje wiadomości wysyłane w ramach platformy.** W motywie 1 wyjaśniono, że zasada poufności obowiązuje „w stosunku do obecnych i przyszłych środków komunikacji". Motyw zawiera również wykaz przykładów tego rodzaju środków, w tym „wiadomości przesyłane przez media społecznościowe". Celem prawodawcy było prawdopodobnie uwzględnienie prywatnych wiadomości wymienianych między użytkownikami portalu społecznościowego (np. Facebooka lub Twittera) lub wiadomości umieszczanych na osi czasu dostępnych dla ograniczonej liczby osób, jednak brzmienie tego motywu nie jest wystarczająco jednoznaczne.

h. **W jaki sposób rozporządzenie w sprawie prywatności i łączności elektronicznej ma zastosowanie do interakcji maszyna-maszyna.** Jak wskazano w pkt 9, Grupa Robocza z zadowoleniem przyjmuje rozszerzenie ochrony na interakcję maszyna-maszyna. Wspomniano o tym jednak jedynie w motywie 12, a nie w odpowiadającym artykule. Ochrona ta jest pożądana, gdyż tego rodzaju komunikacja często obejmuje informacje chronione na

[23] Zobacz na przykład wyrok TSUE z dnia 6 listopada 2003 r. w sprawie C-101/01, pkt 24 (w odniesieniu do numeru telefonu), wyrok TSUE z dnia 19 października 2016 r. w sprawie C-582/14 (Breyer), pkt 49 (w odniesieniu do dynamicznych adresów IP) oraz wyrok TSUE z dnia 8 kwietnia 2014 r. w sprawach C-239/12 i C-594/12 (Digital Rights Ireland), pkt 26–27 (w odniesieniu do wrażliwości metadanych).

podstawie praw dotyczących prywatności. Z drugiej strony należy wyłączyć wąską kategorię łączności maszyna-maszyna sensu stricto, jeżeli nie ma ona żadnego wpływu na prywatność ani poufność komunikacji, tak jak na przykład w przypadkach, w których tego rodzaju komunikacja odbywa się w ramach wykonywania protokołu transmisji między elementami sieci (np. serwerami, przełącznikami) w celu wzajemnej informacji o stanie działania. Szczególnym kontekstem, w którym stosowanie rozporządzenia w sprawie prywatności i łączności elektronicznej wymaga wyjaśnienia, są inteligentne systemy transportowe. Przewiduje się, że pojazdy będą stale przesyłały dane zawierające niepowtarzalny identyfikator za pośrednictwem radia. W braku dodatkowej ochrony danych pochodzących z łączności zapewnionej w rozporządzeniu w sprawie prywatności i łączności elektronicznej mogłoby to doprowadzić do stałego śledzenia nawyków w zakresie kierowania pojazdem, tras podróży i prędkości kierowców. Art. 2 pkt 1 Europejskiego kodeksu łączności elektronicznej zawiera jednak nową rozszerzoną definicję sieci łączności elektronicznej. Obejmują one systemy transmisyjne nieposiadające mechanizmu scentralizowanej administracji umożliwiające przekazywanie sygnałów za pomocą radia. Motyw 14 rozporządzenia w sprawie prywatności i łączności elektronicznej stanowi, że tego rodzaju dane stanowią dane pochodzące z łączności elektronicznej. Zgodnie z art. 5 proponowanego rozporządzenia wszelkiego rodzaju przechwytywanie, monitorowanie lub przechowywanie tego rodzaju danych pochodzących z łączności jest zakazane, o ile nie ma zastosowania jeden z wyjątków. Istnieje jednak zainteresowanie przetwarzaniem tych danych umożliwiających przedmiotom, takim jak samochody i urządzenia bezzałogowe, przekazywanie wzajemnych ostrzeżeń o ich otoczeniu lub o innych zagrożeniach. Pytanie brzmi, jaki wyjątek miałby zastosowanie w tym przypadku. Wyrażenie zgody przez użytkowników końcowych nie jest możliwym do zastosowania wyjątkiem, ponieważ może zaistnieć konieczność posiadania ciągłej możliwości przetwarzania tych danych. Dostawcy powinni zatem mieć możliwość stosowania szczególnego wyjątku umożliwiającego przedmiotom, takim jak samochody i urządzenia bezzałogowe, przekazywanie wzajemnych ostrzeżeń o ich otoczeniu lub o innych zagrożeniach.

*DOPRECYZOWANIE POJĘCIA ZGODY I KWESTII JEJ STOSOWANIA*

41. Jeżeli chodzi o pojęcie zgody i zastosowanie zgody w obecnym brzmieniu proponowanego rozporządzeniu, Grupa Robocza sugeruje następujące wyjaśnienia:
    a. **W jaki sposób należy stosować pojęcie zgody w kontekście osób prawnych.** W motywie 3 stwierdzono, że rozporządzenie powinno zapewniać, aby przepisy RODO miały zastosowanie również do użytkowników końcowych będących osobami prawnymi. Dotyczy to również definicji zgody zawartej w RODO (zob. również motyw 18). Jak stwierdzono w uwadze 13, Grupa Robocza z zadowoleniem przyjmuje wyraźne objęcie osób prawnych zakresem stosowania rozporządzenia. Praktyczne stosowanie

tej zasady budzi jednak wątpliwości. Zgodnie z definicją zgody zawartą w RODO musi być ona „świadoma", a okazanie woli osób, których dane dotyczą, musi przybrać formę „oświadczenia lub wyraźnego działania potwierdzającego" (art. 4 pkt 11 RODO). Należy doprecyzować, kiedy osobę prawną można faktycznie uznać za „świadomą" oraz kiedy następuje złożenie tego rodzaju oświadczenia woli przez osobę prawną.

b. W tym kontekście warto zauważyć, że pracodawca nie może w większości wypadków wyrazić zgody w imieniu swoich pracowników, ponieważ jeżeli pracodawca żąda od pracowników wyrażenia zgody, a – biorąc pod uwagę brak równowagi sił – niewyrażenie zgody przez pracownika prowadzi do rzeczywistej lub potencjalnej istotnej szkody, tego rodzaju zgoda jest dotknięta wadą nieważności, ponieważ nie została wyrażona dobrowolnie[24]. Jeżeli chodzi o **przedsiębiorstwa zapewniające urządzenia lub sprzęt osobom fizycznym, proponowane rozporządzenie nie zawiera (odpowiedniego) wyjątku** od zakazu ingerencji. Jednym z przykładów ilustrujących ten problem jest sytuacja, w której pracodawca ma zamiar zaktualizować telefon zapewniony przez przedsiębiorstwo. Drugi przykład obejmuje sytuację, w której pracodawca oferuje pracownikom samochody objęte leasingiem, a do celów administracyjnych zezwala osobie trzeciej na gromadzenie danych dotyczących lokalizacji za pośrednictwem jednostki pokładowej samochodu. W obydwu przypadkach pracodawca posiada interes w ingerencji w te urządzenia.

   Tego rodzaju ingerencji nie można uznać za konieczną do świadczenia usługi społeczeństwa informacyjnego (art. 8 ust. 1 lit. c) lub konieczną w celu pomiaru odbiorców w sieci web (art. 8 ust. 1 lit. d)). Rozwiązaniem tego problemu mogłoby być ustanowienie nowego wyjątku w celu uwzględnienia sytuacji, w której (i) pracodawca zapewnia określony sprzęt w kontekście stosunku pracy; (ii) pracownik jest użytkownikiem tego sprzętu; oraz (iii) ingerencja jest absolutnie niezbędna w celu korzystania ze sprzętu przez pracownika (co wiąże się ze stosowaniem zasad proporcjonalności i pomocniczości w odniesieniu do gromadzenia danych). Możliwość ingerencji przez pracodawcę w urządzenie użytkownika końcowego powinna być bezwzględnie uzależniona od spełnienia tych przesłanek.

c. **Poprawa kontroli w celu zatrzymania automatycznego przekierowywania połączeń.** W art. 14 przewidziano istotną kontrolę w odniesieniu do użytkowników końcowych, aby zatrzymać automatyczne przekierowywanie połączeń przez osobę trzecią. Ochronę tę można w dalszy sposób wzmocnić, wymagając również w pierwszej kolejności wyrażenia zgody przez użytkownika końcowego na rozpoczęcie przekierowywania połączeń.

*DOPRECYZOWANIE KWESTII DANYCH DOTYCZĄCYCH LOKALIZACJI I INNYCH METADANYCH*

[24] Zob. opinia 15/2011 w sprawie definicji zgody (WP 187), opinia 8/2001 w sprawie przetwarzania danych osobowych w związku z zatrudnieniem (WP 48) oraz nowa opinia w sprawie przetwarzania danych w miejscu pracy (przyjęta równocześnie z niniejszą opinią).

42. Grupa Robocza sugeruje doprecyzowanie następujących kwestii w odniesieniu do danych dotyczących lokalizacji i innych metadanych:
    a. Należy doprecyzować znaczenie **„danych dotyczących lokalizacji generowanych w inny sposób niż w okolicznościach związanych z przypadkiem łączności" w motywie 17.** Nie jest jasne, czy odnosi się to do danych dotyczących lokalizacji zebranych np. za pośrednictwem aplikacji, która korzysta z danych pochodzących z funkcji GPS zainstalowanej w urządzeniach inteligentnych lub generuje dane dotyczące lokalizacji w oparciu o pobliskie routery WiFi, lub dane dotyczące lokalizacji zebrane przez asystentów wbudowanej nawigacji, lub inne sposoby generowania danych dotyczących lokalizacji. Taki brak jasności powoduje niepewność prawną co do zakresu obowiązku. W każdym razie dane dotyczące lokalizacji urządzenia końcowego należącego do osoby fizycznej są danymi osobowymi, dlatego przetwarzanie tych danych podlega obowiązkom określonym w RODO.
    b. Należy wyjaśnić, że **najbardziej uzasadnione przetwarzanie danych dotyczących lokalizacji i innych metadanych <u>nie</u> wymaga niepowtarzalnego identyfikatora**. W motywie 17 wspomina się o mapach aktywności jako przykładzie komercyjnego wykorzystania metadanych z zakresu łączności elektronicznej przez dostawców usług łączności elektronicznej. Do stworzenia podstawowej mapy aktywności nie są potrzebne żadne niepowtarzalne identyfikatory, wystarczy jedynie kalkulacja statystyczna. Inny przykład wspomniany w motywie, tj. wykorzystanie istniejącej infrastruktury i presji na nią, także można policzyć za pomocą określonych punktów pomiarowych np. poprzez utworzenie zagregowanych statystyk dotyczących wykorzystania wież kontroli ruchu do wskazania nacisku w danej lokalizacji w określonym czasie, bez konieczności poznania również tożsamości osób podłączonych do internetu.

       Ponadto w motywie jako przykład wskazuje się wyświetlanie ruchu drogowego w danym kierunku w określonym czasie, w przypadku którego konieczny będzie niepowtarzalny identyfikator wiążący pozycje osób w pewnych interwałach czasowych. W związku z tym przykładem wydaje się, że motyw uzasadnia dalsze przetwarzanie tych danych w celu wsparcia analiz „dużego zbioru danych". Jedynym warunkiem przewidzianym w proponowanym rozporządzeniu w odniesieniu do tego rodzaju przetwarzania jest obowiązek przeprowadzenia oceny skutków w zakresie ochrony danych, jeżeli przetwarzanie „z dużym prawdopodobieństwem może skutkować dużym zagrożeniem dla praw i wolności osób fizycznych". Warunek ten jest niewystarczający. Jest również sprzeczny z obowiązkiem określonym w art. 6, z którego wynika, że ten rodzaj przetwarzania danych może odbywać się wyłącznie za zgodą użytkowników i tylko wtedy, gdy dane nie mogą być zanonimizowane tj. pozbawione niepowtarzalnych identyfikatorów. Użytkownicy często nie mogą odmówić dostawcom usług łączności elektronicznej gromadzenia ich danych geolokalizacyjnych, jeżeli takie gromadzenie jest konieczne ze względów technicznych do przekazywania użytkownikowi komunikatów lub jeżeli takie przetwarzanie

jest konieczne do świadczenia wymaganej usługi (np. nawigacyjnej). We wcześniejszej opinii Grupa Robocza stwierdziła, że takie dane dotyczące lokalizacji, pochodzące z urządzeń inteligentnych są wrażliwymi danymi osobistymi oraz że korzyści wynikające z analizy tych danych nie przeważają nad prawami użytkowników do ochrony poufności ich metadanych pochodzących z łączności ani nie przeważają nad ich ogólnymi prawami do ochrony danych w ramach RODO. W związku z powyższym w motywie należy przynajmniej określić, że w przypadku dalszego przetwarzania danych dotyczących lokalizacji lub innych metadanych dostawcy muszą przestrzegać obowiązków wymienionych w art. 25 RODO. Wymaga to podjęcia co najmniej następujących środków:

(i) stosowanie tymczasowych pseudonimów;

(ii) usunięcie każdej tabeli wyszukiwania wstecznego między tymi pseudonimami i oryginalnymi danymi identyfikacyjnymi;

(iii) agregacja do poziomu, na którym indywidualni użytkownicy nie mogą już być identyfikowani na podstawie ich tras oraz;

(iv) usunięcie wartości oddalonych, w odniesieniu do których identyfikacja byłaby nadal możliwa (wszystkie te środki muszą być stosowane łącznie).

Ponadto na mocy rozporządzenia w sprawie prywatności i łączności elektronicznej strony uczestniczące w przetwarzaniu danych dotyczących lokalizacji i innych metadanych muszą być zobowiązane do udostępniania publicznie stosowanych przez siebie metod anonimizacji i dalszej agregacji, bez uszczerbku dla tajemnicy chronionej prawnie. Umożliwiłoby to organom nadzorczym i społeczeństwu łatwe sprawdzenie, czy wybrana metoda jest odpowiednia.

*DOPRECYZOWANIE KWESTII NIEZAMÓWIONYCH KOMUNIKATÓW*

43. Grupa Robocza sugeruje wyjaśnienie następujących kwestii dotyczących niezamówionych komunikatów:
    a. **sformułowanie zakazu prowadzenia marketingu bezpośredniego bez zgody.** W art. 16 ust. 1 proponowanego rozporządzenia stwierdza się obecnie, że usługi łączności elektronicznej „mogą" być wykorzystywane do wysyłania komunikatów marketingu bezpośredniego (za zgodą), ale nie zawiera wyraźnego zakazu dotyczącego wysyłania (przekierowywania lub przedstawiania) komunikatów marketingu bezpośredniego bez zgody. Różni się to od podejścia określonego w pozostałych przepisach, w których najpierw sformułowano zakaz, a następnie wprowadzono pewne szczególne wyjątki. Obecne brzmienie sugeruje łagodniejsze podejście (które prawdopodobnie nie jest zamierzone). Grupa Robocza proponuje nieco zmienione brzmienie obecnego art. 13 ust. 1 dyrektywy o prywatności i łączności elektronicznej: „korzystanie przez osoby fizyczne lub prawne z usług łączności elektronicznej, w tym połączeń głosowych, automatycznych systemów wywoływania i łączności, w tym półautomatycznych systemów, które łączą odbiorcę połączenia z osobą fizyczną, faksów i poczty elektronicznej lub inne sposoby korzystania z usług

łączności elektronicznej do celów przedstawienia użytkownikom końcowym komunikatów marketingu bezpośredniego mogą być dozwolone jedynie wobec użytkowników końcowych, którzy uprzednio wyrazili na to zgodę";

b. **zakres przepisów dotyczących komunikatów marketingowych i połączeń z istniejącymi kontaktami.** Artykuł 16 ust. 2 stanowi, że jeżeli dana osoba otrzymuje od istniejącego klienta elektroniczne dane kontaktowe dotyczące poczty elektronicznej, może wykorzystywać te dane do celów marketingu bezpośredniego własnych podobnych produktów lub usług jedynie wówczas, gdy klienci mają jasną możliwość wyrażenia – bezpłatnie i w łatwy sposób – sprzeciwu w czasie gromadzenia danych i w odniesieniu do każdej wiadomości. Ogranicza się to obecnie do kontaktów komercyjnych uzyskanych „w kontekście sprzedaży produktu lub usługi" i do dalszego marketingu komercyjnego własnych podobnych produktów lub usług. Z uwagi na fakt, że przepisy dotyczące marketingu bezpośredniego odnoszą się w równym stopniu do niekomercyjnych działań promocyjnych (np. prowadzonych przez organizacje charytatywne lub partie polityczne), przepis ten należy zmienić, aby miał również zastosowanie do organizacji niekomercyjnych, umożliwiając im kontaktowanie się z poprzednimi zwolennikami podczas promowania własnych podobnych celów lub ideałów, a to samo prawo do wyrażenia sprzeciwu powinno mieć zastosowanie do połączeń wykonywanych w ramach marketingu bezpośredniego. Ponadto należy określić termin ważności „kontaktów z bieżącymi klientami" w ramach łączności elektronicznej w celach komercyjnych, charytatywnych lub politycznych, a ten sam termin powinien mieć również zastosowanie do połączeń wykonywanych w ramach marketingu bezpośredniego. Jeżeli państwa członkowskie wybrały system sprzeciwiania się wobec połączeń głosowych w ramach marketingu, istnienie relacji „kontakt z bieżącym klientem" ma pierwszeństwo przed rejestrem „nieoddzwaniania". W takich okolicznościach użytkownicy końcowi nie posiadają skutecznej możliwości zapobiegania uciążliwym połączeniom nawiązywanym przez przedsiębiorstwa lub organizacje, z którymi wcześniej się kontaktowali, a obecnie nie chcą już współpracować. Dlatego, co do zasady, w rozporządzeniu należy określić ważność warunku „bieżący klient" np. przez rok lub dwa lata, w odniesieniu do uzasadnionych oczekiwań danych użytkowników końcowych;

c. **stosowanie przepisów dotyczących marketingu bezpośredniego wobec osób prawnych**. Art. 16 ust. 5 proponowanego rozporządzenia stanowi, że państwa członkowskie zapewniają dostateczną ochronę uzasadnionego interesu użytkowników końcowych, którzy są osobami prawnymi, co do niezamawianych komunikatów. W art. 13 ust. 5 obecnej dyrektywy o prywatności i łączności elektronicznej opisuje się uzasadnione interesy abonentów innych niż osoby fizyczne. Nie są jasne konsekwencje tej zmiany w brzmieniu. Należy wyjaśnić w motywach, że zmiana ta nie odzwierciedla zamiaru zapewnienia niższego poziomu ochrony. W związku z tym zakaz prowadzenia marketingu bezpośredniego bez zgody dotyczy „użytkowników końcowych będących osobami fizycznymi, którzy wyrazili na to zgodę" (podkreślenie dodane). Należy doprecyzować, że obejmuje to osoby fizyczne

*pracujące dla* osób prawnych. Z drugiej strony zgoda nie byłaby wymagana w przypadku kontaktu z osobami prawnymi za pośrednictwem ogólnych danych kontaktowych, jakie podali do wiadomości publicznej w tym właśnie celu (np. „info@companyname.eu”);

d. **stosowanie przepisów dotyczących marketingu bezpośredniego wobec osób występujących jako przedstawiciele (polityczni):** Zgodnie z opracowanym art. 16 niektóre komunikaty wysłane do wybranych przedstawicieli mogą nie zawierać wzmianki o kwestiach lub interesach komercyjnych. Należy wyjaśnić, że rozporządzenie nie zapobiega wysyłaniu takich komunikatów.

*DOPRECYZOWANIE KWESTII STOSOWANIA INSTRUMENTÓW W ZAKRESIE PRAW PODSTAWOWYCH*

44. Należy doprecyzować **zakres stosowania karty i Konwencji o ochronie praw człowieka i podstawowych wolności (EKPC) w odniesieniu do krajowych przepisów dotyczących zatrzymywania danych**. Motyw 26 stanowi, że wszystkie środki stosowane przez państwa członkowskie w celu zabezpieczenia interesów publicznych, takie jak zgodne z prawem środki przechwytywania danych, muszą być zgodne z kartą (oraz EKPC). Jest to pożądane, ponieważ jest to zgodne z tokiem rozumowania przedstawionym w orzeczeniu w sprawie Tele2/Watson, zgodnie z którym wszelkie krajowe wyjątki od prawa Unii w zakresie ochrony przetwarzania danych podlegają karcie (zaś naruszenia na mocy przepisów krajowych można wnieść do Trybunału Sprawiedliwości UE). W art. 11 proponowanego rozporządzenia zauważa się jednak tylko, że ograniczenia zakresu stosowania art. 5–8 proponowanego rozporządzenia odbywają się z poszanowaniem istoty podstawowych praw i wolności oraz gdy środek jest konieczny i proporcjonalny. W tym miejscu należy również zamieścić wyraźne odniesienie do karty i EKPC.

45. **Poufność komunikacji jest również chroniona na mocy art. 8 EKPC.** W pkt 1.1 uzasadnienia i w motywie 1 wyjaśniono, że proponowane rozporządzenie wdraża art. 7 karty. Zostało to powtórzone w motywie 19. Podstawowe prawo do poufnej komunikacji jest jednak chronione nie tylko tym przepisem, ale również art. 8 EKPC. Umieszczenie wyraźnego odniesienia w artykule proponowanego rozporządzenia stanowiłoby dodatkowe potwierdzenie, że właściwe orzecznictwo Europejskiego Trybunału Praw Człowieka także zostanie uwzględnione podczas oceny (ostatecznej wersji) rozporządzenia. Odniesienie takie zostało znalazło się już w motywach 20 (dotyczącym urządzeń końcowych) i 26 (dotyczącym zgodnego z prawem przechwytywania) i dodatkowo zostało poparte uwagami przedstawionymi w pkt 2.1 uzasadnienia (dotyczącym związku między kartą a EKPC w kontekście osób prawnych), ale nie znajduje się w żadnym z odnośnych artykułów, jak np. art. 11 ust. 1.

*INNE WYJAŚNIENIA*

46. Należy doprecyzować, że **obowiązki wynikające z RODO, takie jak te dotyczące systemu naruszenia ochrony danych i oceny skutków dla ochrony danych, mają nadal zastosowanie**, gdy strony przetwarzają dane osobowe w kontekście danych pochodzących z łączności elektronicznej. Jak wspomniano w motywie 5, proponowane rozporządzenie jest *lex specialis* względem RODO, a przetwarzanie danych pochodzących z łączności elektronicznej powinno być dozwolone jedynie zgodnie z proponowanym rozporządzeniem; można mieć wątpliwości, czy niektóre zobowiązania wynikające z RODO mają również zastosowanie w kontekście proponowanego rozporządzenia. Dotyczy to w szczególności sytuacji, gdy proponowane rozporządzenie można interpretować w taki sposób, aby wykonać określony obowiązek, w przypadku gdy RODO również go obejmuje. Wśród przykładów można wymienić:
    (i) proponowane rozporządzenie zobowiązuje do powiadomienia o „wykrytym" ryzyku w zakresie bezpieczeństwa (art. 17) (zob. również uwaga 35), jednak RODO obejmuje system powiadamiania o naruszeniach ochrony danych (art. 33 i 34);
    (ii) w proponowanym rozporządzeniu wspomina się, że w pewnych okolicznościach obowiązkowe jest przeprowadzenie oceny skutków dla ochrony danych i odbycie konsultacji z organem nadzorczym zgodnie z RODO (motyw 17 i 19 oraz art. 6 ust. 3 lit. b)), podczas gdy w RODO określono już, kiedy należy przeprowadzić ocenę skutków dla ochrony danych i kiedy wymagane są konsultacje (art. 35 i 36) oraz;
    (iii) nie sprecyzowano, czy jeżeli spełnia się niezbędne warunki wyjątku od zakazu przetwarzania danych na mocy art. 5 proponowanego rozporządzenia, nadal należy przestrzegać wszystkich istotnych obowiązków zgodnie z RODO, jeżeli chodzi o przetwarzanie danych osobowych, a wszelkie inne rodzaje przetwarzania w ramach RODO są zabronione. Należy doprecyzować, że test zgodności określony w art. 6 ust. 4 RODO nie ma zatem zastosowania;
    (iv) w proponowanym rozporządzeniu w sprawie prywatności i łączności elektronicznej nie przewiduje się mechanizmu certyfikacji podobnego do art. 42 i 43 RODO. W związku z tym, że zakres art. 42 RODO ogranicza się ściśle do ustanowienia mechanizmów certyfikacji ochrony danych oraz do wprowadzenia znaków jakości i oznaczeń w dziedzinie ochrony danych w celu wykazania zgodności z RODO, należy rozważyć, czy nie wskazane byłoby wprowadzenie porównywalnego przepisu, który umożliwiłby certyfikację operacji przetwarzania, norm, produktów lub usług pod względem ich zgodności z rozporządzeniem w sprawie prywatności i łączności elektronicznej.

    W celu zapewnienia, aby ten brak jasności nie został wykorzystany jako argument za obniżeniem poziomu ochrony na mocy proponowanego rozporządzenia, należy jasno stwierdzić, że we wszystkich tych przypadkach administratorzy danych muszą przestrzegać RODO.

47. Ponadto należy wyjaśnić, że **wymóg wycofania zgody ma również zastosowanie w kontekście ingerencji w urządzenia końcowe**. W art. 8 ust. 1 lit. b) proponowanego rozporządzenia przewiduje się możliwość ingerencji za zgodą użytkownika końcowego w jego urządzenie końcowe. W art. 9 ust. 3 wymaga się,

aby użytkownicy końcowi mieli możliwość wycofania swojej zgody w dowolnej chwili, ale dotyczy to wyłącznie zgody na analizę metadanych i treści. Należy doprecyzować, że obowiązek ten rozciąga się na ingerencję w urządzenia końcowe.

48. Kolejna powiązana kwestia – należy doprecyzować, że **przypomnienie o możliwości cofnięcia zgody dotyczy również zgody uzyskanej za pośrednictwem ustawień przeglądarki**. W art. 9 ust. 3 wymaga się, aby użytkownikom końcowym okresowo, co 6 miesięcy, przypominano o możliwości wycofania swojej zgody w dowolnej chwili. Chociaż Grupa Robocza uważa, że ogólne ustawienia przeglądarki i innego oprogramowania, w tym systemów operacyjnych, aplikacji i interfejsów oprogramowania dla urządzeń podłączonych do internetu rzeczy (tj. nie w oparciu o szczegółowe kontrole), nie mogą być ważnym środkiem wyrażenia zgody, ponieważ ogólne ustawienia nie są odpowiednie do udzielenia konkretnej zgody na konkretne scenariusze (zob. uwaga 24), ustawienia domyślne powinny być przyjazne dla użytkownika (zob. uwaga 19). *Jeżeli* pozostaje to w treści proponowanego rozporządzenia, ustawienia muszą być na tyle szczegółowe, aby umożliwić kontrolę wszystkich rodzajów przetwarzania danych, na które użytkownik wyraża zgodę, oraz objęcie wszystkich funkcji urządzenia, które mogą prowadzić do przetwarzania danych. Ponadto użytkownikowi końcowemu należy przynajmniej okresowo (co 6 miesięcy) przypominać o możliwości zmiany tych ustawień.

49. Z zadowoleniem przyjmuje się fakt, że proponowane rozporządzenie wymaga, aby oprogramowanie już wprowadzone na rynek informowało użytkownika końcowego o ustawieniach prywatności (art. 10). **Nie jest jednak jasne, w jaki sposób można to skutecznie zastosować do dotychczasowych produktów** i innych produktów, które nie są już obsługiwane. Ponadto należy dokładniej wyjaśnić, w jaki sposób obowiązek ten będzie miał zastosowanie do oprogramowania typu open source, które jest opracowywane w sposób otwarty i zdecentralizowany.

50. Należy doprecyzować, że **oferowanie możliwości blokowania plików cookie (osób trzecich) zgodnie z art. 10 proponowanego rozporządzenia ma pierwszeństwo przed wyjątkiem dotyczącym pomiaru odbiorców w sieci web** zgodnie z art. 8 ust. 1 lit. d). Lub innymi słowy: mimo że strona internetowa może wykorzystywać analizy pomiarów odbiorców w sieci web zgodnie z art. 8 ust. 1 lit. d), użytkownicy nadal powinni mieć prawo do blokowania tych technologii śledzenia w swojej przeglądarce.

51. **Należy doprecyzować definicję (pół)automatycznych systemów wywoływania i łączności.** Definicja tego terminu w art. 4 ust. 3 lit. h) proponowanego rozporządzenia zawiera odniesienie do terminu w drugiej części zdania („w tym wywołań dokonywanych z użyciem zautomatyzowanych systemów wywoływania i łączności, które łączą osobę wywoływaną z inną osobą"). Sugeruje się skreślenie tego ostatniego zdania z definicji i zmianę definicji w art. 4 ust. 3 lit. g), aby uwzględnić połączenia wykonywane za pomocą półautomatycznych systemów łączności, takich jak np. automatyczne dialery, które łączą osobę wywoływaną z inną osobą.

52. **Należy doprecyzować informacje stanowiące „część abonamentu na usługę”**. W motywie 14 wspomina się, że metadane pochodzące z łączności elektronicznej „mogą zawierać informacje stanowiące część abonamentu na usługę, gdy takie informacje są przetwarzane na potrzeby przesyłania, dystrybuowania lub wymiany treści łączności elektronicznej”. Nie jest jasne, jaki jest cel tego sformułowania.

53. Należy wyjaśnić **zastosowanie mechanizmów spójności i współpracy.** W motywie 38 zauważa się, że proponowane rozporządzenie opiera się na mechanizmie spójności określonym w RODO. Ponadto art. 18 ust. 1 stanowi, że stosuje się odpowiednio rozdziały VI i VII RODO. W art. 19 zauważono, że Europejska Rada Ochrony Danych wykonuje zadania określone w art. 70 RODO. Chociaż zastosowanie tych przepisów jest stosunkowo jasne, nie można wykluczyć wystąpienia problemów związanych z interpretacją w odniesieniu do kluczowych pojęć dotyczących mechanizmów spójności i współpracy zgodnie z RODO. Na przykład mechanizm wiodącego organu nadzorczego ma zastosowanie w tych przypadkach, w których prowadzone jest „transgraniczne przetwarzanie” (art. 56 ust. 1 RODO): nie jest pewne, w jaki sposób ma on zastosowanie w przypadku ingerencji w urządzenia końcowe lub analizy treści lub metadanych zgodnie z proponowanym rozporządzeniem. Wskazane jest zatem wyjaśnienie zastosowania tych kluczowych pojęć w motywie i podkreślenie, że wszelkie pozostałe kwestie dotyczące zastosowania tych rozdziałów RODO w kontekście proponowanego rozporządzenia zostaną rozwiązane poprzez interpretację przepisów zawartych w tych rozdziałach zgodnie z intencją prawodawcy. Ponadto wskazane jest doprecyzowanie, że art. 70 stosuje się odpowiednio do Europejskiej Rady Ochrony Danych w kontekście proponowanego rozporządzenia (obecnie brak tego zapisu w motywie).

*** * ***