Abstract:

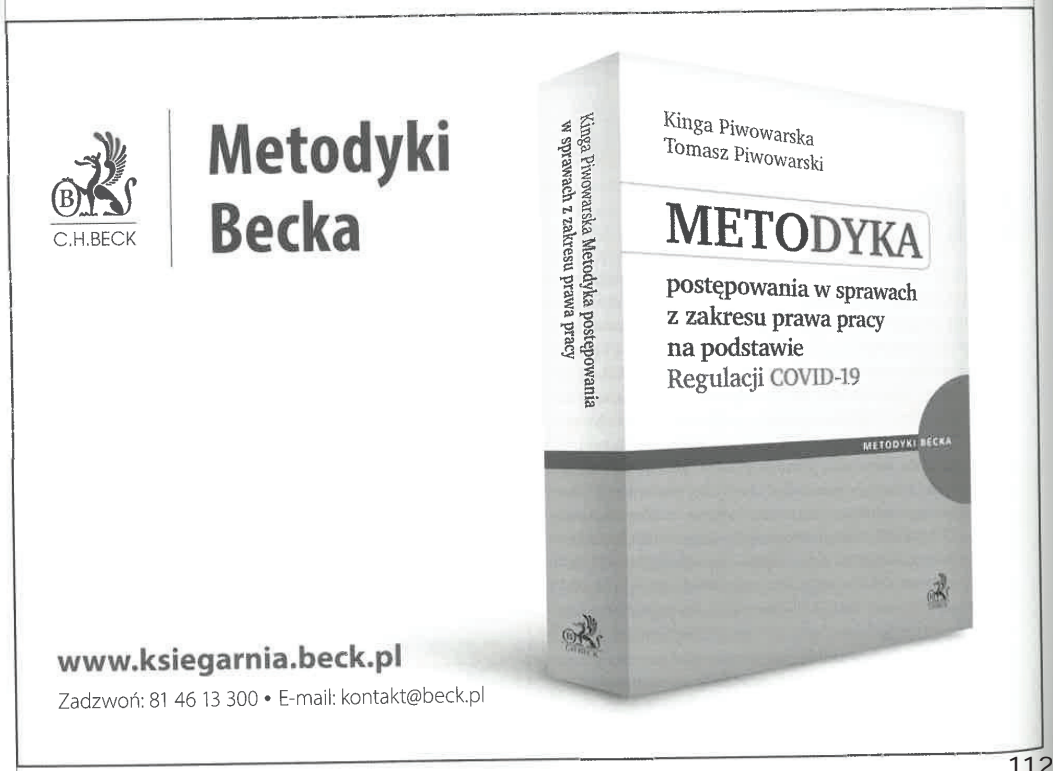
Wpływ nowych technologii na kształtowanie warunków pracy
Wstępna analiza możliwości wykorzystania rozwoju technologicznego w stosunku pracy, ukazuje już *prima facie* potrzebę głębokiej rewizji tego ostatniego. Rewizji szczególnie pod kątem dopasowania regulacji do zmieniającej się wokół nas rzeczywistości. Wskazane regulacje Kodeksu pracy były tworzone w innych realiach i niewątpliwie w pewnych sytuacjach hamują rozwój prawa pracy w tym sensie, że prawo pracy powinno nauczyć się korzystać z rozwoju technologicznego, a nie tylko z konieczności rozwój takowy tolerować. A kategoria „ułatwiania" nie jest synonimem kategorii „pogarszania sytuacji" i nie stoi na przeszkodzie realizacji wielu funkcji prawa pracy, w tym przede wszystkim funkcji ochronnej.

Słowa kluczowe: prawo pracy a nowe technologie, stosunek pracy a nowe technologie, definicja stosunku pracy, praca zdalna, miejsce pracy, kierownictwo w stosunku pracy

How new technologies affect employment conditions
The preliminary analysis of the possibilities to utilise technological development in an employment relationship reveals *prima facie* the need for a profound revision of the latter, in particular from the viewpoint of adjusting regulations to the ever changing reality that surrounds us. The indicated Labour Code regulations were devised in a different realities and in certain situations undoubtedly hamper the development of labour law in the sense that it should learn how to utilise technological development rather than only tolerate such development out of necessity. The category of „facilitating" is not a synonym to „worsening the situation" and does not obstruct realisation of many functions of labour law, primarily the protective function.

Key words: labour law an new technologies, employment relationship and new technologies, definition of an employment relationship, remote working, workplace, management in an employment relationship

Reklama



Connected cars – wybrane problemy i wyzwania regulacyjne

Agata Szeliga[1]
Marta Kupczak-Strzelecka[2]
Maria Rudzińska[3]

Pojazdy połączone i autonomiczne stają się coraz popularniejsze. Zapewniają dostęp do nowych funkcjonalności, ale wytwarzają duże ilości danych. W maju 2020 r. zakończone zostały konsultacje projektu Wytycznych nr 1/2020 z 28.1.2020 r. dotyczących przetwarzania danych osobowych w kontekście połączonych samochodów i aplikacji związanych z poruszaniem[4] Europejskiej Rady Ochrony Danych[5]. Wytyczne budzą wiele wątpliwości, np. odnośnie traktowania połączonego pojazdu jako urządzenia końcowego i wymogu zgody na przechowywanie i dostęp do zawartych w nim danych. Nowego podejścia wymaga też informowanie o przetwarzaniu danych. Na te kwestie nakłada się także implementacja Europejskiego kodeksu łączności elektronicznej[6]. Projekt Prawa komunikacji elektronicznej[7] porusza kwestię komunikacji *machine to machine* (M2M) wykorzystywanej w takich pojazdach. Dostawcy usług transmisji danych wykorzystywanej na potrzeby M2M będą objęci nowymi regulacjami tylko, jeśli ich usługi będą publicznie dostępne. Usługi świadczone dedykowanym odbiorcom nie zostaną objęte nowym reżimem.

Pojazdy autonomiczne i *connected cars*

1. Pojazdy autonomiczne

Koncepcja pojazdu autonomicznego zakłada możliwość poruszania się pojazdem bez udziału osoby nim kierującej. Klasyfikacja autonomiczności pojazdów, sporządzona przez *National Highway Traffic Safety Administration* (NHTSA)[8], zakłada **pięć poziomów autonomiczności**[9], które przedstawiają się następująco:

- **Poziom 0** – pełna odpowiedzialność kierowcy za prowadzenie pojazdu wraz z jego pełną obsługą;
- **Poziom 1** – zautomatyzowanie pewnych układów przy jednoczesnej obsłudze wszystkich układów przez kierowcę; układy mogą być wspomagane lub samoczynnie aktywowane (np. układy ABS, EPS);
- **Poziom 2** – kierowca nie musi obsługiwać zautomatyzowanych układów, takich jak automatyczne utrzymywanie pojazdu w pasie ruchu itp.;
- **Poziom 3** – przejęcie przez system kontroli nad sterowaniem pojazdem w określonych okolicznościach – kierowca pozostaje zobligowany do interwencji w sytuacjach tego wymagających;
- **Poziom 4** – przejęcie przez system pełnej kontroli nad sterowaniem pojazdu. Kierowca nie musi kontrolować sytuacji ani interweniować[10].

Jak wskazano powyżej, skala zaczyna się od braku jakichkolwiek autonomicznych układów czy systemów, a kończy na sytuacji, w której system przejmuje kontrolę nad kierowaniem pojazdu w każdej sytuacji, w każdych warunkach i na każdej drodze.

2. Pojazdy połączone *Connected cars*

Zdolność pojazdów do komunikowania się będzie mieć kluczowe znaczenie dla włączenia pojazdów zautomatyzowanych do ogólnego systemu transportu. Jednak pojazdów autonomicznych nie należy mylić z połączonymi samochodami (*connected cars*). Kluczową cechą pojazdów autonomicznych jest ich **niezależność**, przejawiająca się tym, że przynajmniej niektóre aspekty ich funkcji kontrolnych o istotnym znaczeniu dla bezpieczeństwa działają bez bezpośredniego udziału kierowcy. Natomiast w przypadku połączonych samochodów, ich podstawowym założeniem jest komunikacja między człowiekiem, samochodem i otoczeniem (*connectivity*). Chociaż niektóre systemy występujące w samochodach mogą zapewniać zarówno funkcje charakterystyczne dla pojazdów autonomicznych, jak i samochodów połączonych, mogą one również istnieć oddzielnie[11].

3. Zastosowanie komunikacji *machine to machine* w połączonych samochodach

Dla funkcjonowania połączonych samochodów niezwykle ważny jest rozwój i zastosowanie w praktyce **komunikacji *machine to machine* („M2M")**, zwanej często zamiennie „Internetem rzeczy" (IoT). Komunikacja *machine to machine* jest technolo-

[1] Autorka jest radcą prawnym i partnerem w kancelarii Sołtysiński Kawecki & Szlęzak.

[2] Autorka jest radcą prawnym i Senior Counsel w kancelarii Sołtysiński Kawecki & Szlęzak.

[3] Autorka (*researcher*) jest młodszym prawnikiem w kancelarii Sołtysiński Kawecki & Szlęzak.

[4] Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related application, version 1.0, dostępny na: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf; dalej jako: Wytyczne.

[5] Dalej jako: EROD.

[6] Dyrektywa Parlamentu Europejskiego i Rady 2018/1972 z 11.12.2018 r. ustanawiająca Europejski kodeks łączności elektronicznej, Dz.Urz. L Nr 321 z 17.12.2018 r., s. 36 ze zm.; dalej jako: EKŁE.

[7] Projekt nowego Prawa komunikacji elektronicznej z 29.7.2020 r., dostępny na: https://legislacja.gov.pl/docs//2/12336501/12703257/12703258/dokument457029.pdf; dalej jako: projekt PrKomEl.

[8] Na potrzeby niniejszego artykułu wykorzystano klasyfikację NHTSA, pomijając przy tym drugą najczęściej stosowaną w publikacjach klasyfikację opracowaną przez *Society of Automotive Engineers*, która przedstawia problematykę etapów autonomiczności w sposób bardziej szczegółowy.

[9] *National Highway Traffic Safety Administration*, Preliminary Statement of Policy Concerning Automated Vehicles, dostępne (w języku angielskim) na: https://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf.

[10] Zob. *T. Neumann*, Perspektywy wykorzystania pojazdów autonomicznych w transporcie drogowym w Polsce, „Autobusy – Technika, Eksploatacja, Systemy Transportowe" Nr 12/2018, s. 788.

[11] *European Data Protection Supervisor*, TechDispatch #3: Connected Cars, dostępne (w języku angielskim) na: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-3-connected-cars_en.

gią automatycznego przesyłania danych z jednego do drugiego terminala, przy czym terminalami tymi są określone urządzenia, w tym samochody, komunikujące się ze sobą za pomocą różnorodnych technologii transmisyjnych (jak sieci satelitarne, lokalne, a także komórkowe)[12]. Ma przy tym bardzo szerokie zastosowanie, w szczególności jeżeli chodzi o systemy transportowe (np. w zakresie monitorowania przemieszczających się pojazdów czy ich stanu technicznego), ale także w szeroko pojętej branży motoryzacyjnej. Przewiduje się, że nastąpi silny rozwój usług M2M w połączonych pojazdach wraz z rozwojem technologii, usług i sieci 5G[13]. Jak zakłada Komisja Europejska, 5G umożliwi obiektom „w ruchu" nieprzerwane połączenie z Internetem zarówno w miastach, jak i w korytarzach międzymiastowych. Sieć 5G będzie w niezakłócony sposób współistniała z już stosowanymi technologiami uzupełniającymi, służącymi przykładowo do łączności krótkiego zasięgu pojazd-pojazd i pojazd-infrastruktura[14]. Jak podaje Komisja Europejska[15], aby wspierać usługi związane z bezpieczeństwem wymagające bardzo dużego skrócenia opóźnień, różni producenci pojazdów zobowiązali się do montażu dodatkowych urządzeń łączności krótkiego zasięgu (opartych na Wi-Fi) w pojazdach od 2019 r., a zarządcy dróg rozpoczęli również działania poprzedzające wdrożenie infrastruktury łączności wzdłuż dróg, umożliwiającej bezpośrednią interakcję pomiędzy pojazdami lub pomiędzy pojazdami a infrastrukturą drogową.

Komunikacja M2M w samochodach wiąże się z szeregiem zagadnień prawnych i regulacyjnych, w tym z zakresu danych osobowych i prawa telekomunikacyjnego. Wybrane z nich zostaną omówione poniżej.

Connected cars a przetwarzanie danych osobowych

1. Wprowadzenie

Nowoczesne samochody już teraz mogą generować ogromne ilości danych, w tym dotyczących sposobu jazdy, telemetrii, eksploatacji samochodu, warunków pogodowych lub drogowych, a nawet danych o zdrowiu kierowców (w przypadku systemów monitorujących stan kierowcy i ostrzegających przed zmęczeniem) lub o ich cechach biometrycznych (np. w przypadku niektórych funkcji sterowanych głosem lub informacji związanych ze stylem jazdy, np. używaniem hamulca[16]).

Szacunki dotyczące ilości danych generowanych przez połączone samochody są bardzo różne, począwszy od 25 GB na godzinę[17], poprzez 1 TB danych dziennie, po nawet 32 TB dziennie[18]. Niezależnie od tych sporów, są to niewątpliwie ogromne ilości danych. Dane te mogą pozostawać w samochodzie, być przesyłane do producenta, a z założenia – mają być wymieniane z innymi użytkownikami dróg lub z infrastrukturą drogową (np. ostrzegając zbliżające się samochody o sobie lub odpowiednio modyfikując ustawienia świateł, aby zapewnić ich efektywny i bezkolizyjny przejazd). Do przekazywania danych może dochodzić w szczególności za pomocą instalowanych w samochodach urządzeń zapewniających transmisję danych przy wykorzystaniu sieci komórkowych (np. modemy LTE czy 5G), ale też urządzeń własnych kierowcy lub pasażera (np. smartfonów), które dzięki połączeniu z Internetem zapewniają łączność systemów samochodowych z zewnętrznymi systemami podmiotów trzecich, czy też za pomocą innych czujników instalowanych w samochodach.

W dniu 4.5.2020 r. zakończone zostały prowadzone przez EROD konsultacje publiczne Wytycznych nr 1/2020. Wytyczne wzbudziły spore zainteresowanie – wpłynęło bowiem ponad 60 stanowisk od szerokiego grona zainteresowanych: przedstawicieli Państw Członkowskich, osób prywatnych, producentów samochodów, stowarzyszeń branżowych, organizacji konsumenckich, klubów motoryzacyjnych i firm telekomunikacyjnych, zarówno z Unii Europejskiej, ale też z Chin i Stanów Zjednoczonych[19]. Warto podkreślić, że Wytyczne nie są pierwszą próbą uregulowania kwestii związanych z przetwarzaniem danych osobowych w połączonych i autonomicznych samochodach. W październiku 2017 r. francuski organ ochrony danych osobowych – *Commission National Informatique & Libertés* (CNIL) wydał Pakiet Zgodności: Połączone Samochody i Dane Osobowe[20]. Natomiast w styczniu 2016 r. niemieckie organy ochrony danych osobowych wydały, wspólnie ze stowarzyszeniem branży samochodowej VDA, swoje rekomendacje dotyczące tej kwestii.

[12] *M. Gajewska*, Komunikacja M2M w zastosowaniach transportowych, „Prace Naukowe Politechniki Warszawskiej" Nr 113/2016, s. 171.

[13] Ministerstwo Cyfryzacji, Strategia 5G dla Polski, dostępna na: https://www.gov.pl/documents/31305/436699/Strategia+5G+dla+Polski.pdf/0cd08029-2074-be13-21c8-fc1cf09629b0.

[14] *Komisja Europejska*, Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 14.9.2016 r.; COM(2016) 587: Łączność dla konkurencyjnego jednolitego rynku cyfrowego: w kierunku europejskiego społeczeństwa gigabitowego, s. 7, dostępny na: https://ec.europa.eu/transparency/regdoc/rep/1/2016/PL/1-2016-587-PL-F1-1.PDF.

[15] *Komisja Europejska*, Komunikat Komisji Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Droga do zautomatyzowanej mobilności: strategia UE na rzecz mobilności w przyszłości z 17.5.2018 r.; COM(2018) 283, s. 15, dostępny na: https://eur-lex.europa.europa.eu/resource.html?uri=cellar:0e8b694e-59b5-11e8-ab41-01aa75ed71a1.0010.02/DOC_1&format=PDF.

[16] Z przeprowadzanych badań wynika że możliwa jest 100% identyfikacja każdego z 15 kierowców na bazie krótkich danych testowych (8 min, 15 min, 1 godzina) i wielu sensorów samochodowych; przy czym 87% poprawna identyfikacja zachodzi już w przypadku użycia jednego sensora (pedał hamulca) i w pierwszych 15 minutach normalnej jazdy odnotowanej w bazie, *M. Enev, A. Tukakuwa, K. Koscher, T. Kohno*, Automated Driver Fingerprinting, dostępne na: www.autosec.org/pubs/fingerprint.pdf.

[17] *European Data Protection Supervisor*, TechDispatch #3: Connected Cars, *op. cit.*

[18] *Ch. Mellor*, Data storage estimates for intelligent vehicles vary widely, 17.1.2020 r., Blocks & Files, dostępne (w języku angielskim) na: https://blocksandfiles.com/2020/01/17/connected-car-data-storage-estimates-vary-widely/.

[19] Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, dostępny na: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en.

[20] *Commission Nationale de l'Informatique et des Libertés*, Compliance Package: Connected Vehicles and Personal Data, dostępne (w języku angielskim) na: https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.

2. Dane generowane przez samochód a dane osobowe

Wśród danych generowanych przez samochody niewątpliwie występują **dane osobowe**, czyli informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), gdzie osobą fizyczną możliwą do zidentyfikowania jest osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej [art. 4 pkt 1) RODO[21]]. W motywie (26) RODO można znaleźć dodatkowe kryteria, które należy brać pod uwagę przy ocenie, czy dana osoba fizyczna jest możliwa do zidentyfikowania, tj. wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny.

W praktyce pojawia się jednak szereg wątpliwości, jakie dane wytwarzane w połączonych samochodach należy uznać za dane osobowe, a także kto będzie ich administratorem.

W pkt 3 Wytycznych EROD przyjęła, że większość danych wytwarzanych przez połączone samochody będzie stanowić dane osobowe, gdyż będą one dotyczyły kierowców lub pasażerów, i to nawet jeśli nie będą wprost powiązane z nazwiskiem, ale z technicznymi aspektami i funkcjonalnościami samochodu. Jako przykłady danych osobowych EROD wskazała ogólnie na dane o stylu jazdy, pokonywanych odległościach, dane eksploatacyjne dotyczące zużycia części samochodowych lub dane gromadzone przez kamery samochodowe, które mogą obejmować zachowanie kierowcy oraz informacje o innych osobach znajdujących się w lub poza pojazdem, a które w powiązaniu z innymi danymi mogą umożliwiać ich identyfikację.

Podejście EROD wzbudziło kontrowersje, zwłaszcza wśród producentów samochodów. W praktyce posiadają oni nazwisko i inne dane identyfikacyjne pierwszego indywidualnego nabywcy samochodu, a informacje o kolejnych właścicielach – w przypadkach, gdy zarejestrują oni swoje pojazdy u producentów lub importerów. Producenci nie mają zwykle informacji, kto będzie faktycznym użytkownikiem samochodu, natomiast mogą mieć informacje o stylu jazdy takiej osoby, czy jej wizerunek z kamer samochodowych. Producenci nie muszą też uzyskiwać dostępu do wszystkich danych generowanych w samochodzie (np. jeżeli nie są przesyłane do producenta). W rezultacie, jeżeli techniczna możliwość powiązania danych znajdujących się w samochodzie oznaczałaby, że zachodzi uzasadnione prawdopodobieństwo identyfikacji takiej osoby przez producenta, musiałby on takie dane zawsze traktować jako dane osobowe. Rodzi się jednak pytanie, czy faktycznie sama techniczna możliwość powiązania danych powinna skutkować uznaniem, że takie dane zostaną przez producenta wykorzystane w celu identyfikacji, zwłaszcza biorąc pod uwagę koszt i czas potrzebny do takiego działania, jak również zobowiązania producenta. Warto byłoby rozważyć wskazówki, jaki nakład kosztów czy czasu pozwalałby uznać, że nie jest prawdopodobne wykorzystanie tych informacji do identyfikacji określonej osoby.

Wątpliwości budzi również sama kwalifikacja danych wskazanych przez EROD jako danych osobowych. Jak wskazałyśmy powyżej, z przeprowadzonych badań wynika, że np. sposób hamowania wraz z innymi wskaźnikami pozwala na jednoznaczną identyfikację osoby biorącej udział w testach już po krótkim czasie. Natomiast niektórym danym, np. samej informacji o przebiegu samochodu (bez danych o lokalizacji), wersji zainstalowanego oprogramowania, zagregowanych danych dotyczących prędkości czy zużycia paliwa, pewnym informacjom eksploatacyjnym (np. o temperaturze silnika, ciśnieniu oleju, emisji spalin) trudno jednak przypisać charakter danych osobowych, gdyż nie umożliwiają one identyfikacji określonej osoby fizycznej.

3. Sposób wykorzystania danych

Wytyczne mają znaleźć zastosowanie do danych osobowych związanych z korzystaniem z połączonych samochodów w celach niezawodowych przez osoby, których dane dotyczą i mają obejmować zarówno dane osobowe przetwarzane wewnątrz samochodu, wymieniane między samochodem a urządzeniami podłączonymi do niego (np. smartfonami, tabletami), jak i zbierane w samochodzie i eksportowane do zewnętrznych podmiotów (np. producentów samochodów, ubezpieczycieli, warsztatów samochodowych, zarządców infrastruktury) do dalszego przetwarzania.

Wytyczne idą zatem dalej niż dotychczas przyjmowane stanowisko. Do przetwarzania danych nieopuszczających samochodu nie stosowano bowiem do tej pory przepisów o ochronie danych osobowych, zakładając, że w większości przypadków używania samochodów do celów prywatnych, takie korzystanie będzie wiązało się z przetwarzaniem danych w ramach czynności o czysto osobistym charakterze, do którego RODO nie znajduje zastosowania [art. 4 ust. 2 lit. c) RODO]. Co więcej, w swoim Pakiecie Zgodności dla Połączonych Samochodów, CNIL uznał, że przepisy dotyczące ochrony danych osobowych nie powinny znaleźć zastosowania również w przypadku przekazywania danych poza samochód, o ile dane nie są przekazywane dostawcom usług, ale pozostają bądź w sieciach pod pełną kontrolą użytkownika (np. sieci Wi-Fi lub Bluetooth), bądź w publicznie dostępnych sieciach telekomunikacyjnych (np. GSM), w zakresie, w jakim operator tych sieci dostarcza tylko usługi komunikacji elektronicznej (np. umożliwia połączenie między aplikacją zainstalowaną przez użytkownika na jego telefonie a komputerem samochodu, bez przekazywania danych z samochodu lub telefonu do podmiotu udostępniającego aplikację czy producenta samochodu)[22].

[21] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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, Dz.Urz. L Nr 119 z 4.5.2016 r., s. 1 i n. ze zm.; dalej jako: RODO.

[22] *Commission Nationale de l'Informatique et des Libertés*, Compliance Package: Connected Vehicles and Personal Data, *op. cit.*, scenariusz nr 1 IN-IN, s. 19.

Warto podkreślić, że dane są generowane przez różne systemy samochodowe przynajmniej od kilkudziesięciu lat, a wiele z nich może być uważane za dane osobowe. **Przyjęcie interpretacji proponowanej w Wytycznych, aby stosować przepisy RODO do danych osobowych, które nie opuszczają samochodu używanego do celów prywatnych, wydaje się być nieuzasadnione w świetle art. 4 ust. 2 lit. c) RODO.** Dane te są używane bowiem przez kierowców, czy pasażerów w związku z eksploatacją przez nich samochodu, a zatem w celach osobistych. Ponadto, trudno znaleźć racjonalne uzasadnienie dla innego traktowania takich danych w samochodach połączonych i „niepołączonych". Często bowiem te dane będą praktycznie takie same.

4. Podstawy przetwarzania danych osobowych. Przetwarzanie w innych celach

Największe kontrowersje w projekcie Wytycznych budzą jednak podstawy przetwarzania danych pochodzących z połączonych samochodów i możliwość dalszego ich przetwarzania w innych celach.

Zdaniem EROD, połączony samochód, tak jak smartfon, komputer czy smart TV, stanowi **urządzenie końcowe** zdefiniowane w art. 1 dyrektywy 2008/63/WE z 20.6.2008 r. w sprawie konkurencji na rynkach końcowych urządzeń telekomunikacyjnych[23], tzn. jest:

1) urządzeniem bezpośrednio lub pośrednio podłączonym do interfejsu publicznej sieci telekomunikacyjnej w celu przesyłania, przetwarzania lub odbierania informacji; w obydwu przypadkach (połączenia bezpośredniego lub pośredniego), połączenie może być dokonane za pomocą przewodu, światłowodu lub elektromagnetycznie; połączenie jest pośrednie, jeżeli urządzenie jest umieszczone między końcowym urządzeniem telekomunikacyjnym a interfejsem sieci lub
2) urządzeniem naziemnych stacji satelitarnych.

W rezultacie, EROD zajęła stanowisko, że do połączonych samochodów należy stosować art. 5 ust. 3 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z 12.7.2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), tzw. dyrektywy *ePrivacy*[24]. Zgodnie z tym przepisem, przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym abonenta lub użytkownika jest dozwolone wyłącznie pod warunkiem wyrażenia przez nich zgody po otrzymaniu jasnych i wyczerpujących informacji. W zakresie przechowywania i uzyskiwania dostępu do danych osobowych w urządzeniu końcowym, art. 5 ust. 3 dyrektywy *ePrivacy* ma pierwszeństwo w opinii EROD nad art. 6 RODO, który jednak znajdzie zastosowanie do dalszego przetwarzania danych pobranych w wyniku uzyskania dostępu do urządzenia końcowego.

Samo porównanie samochodu do smartfona już budzi kontrowersje, ale należy istotnie zastanowić się, czy słusznie EROD uznaje połączony samochód za urządzenie końcowe. W naszej ocenie jest to błędna kwalifikacja. Po pierwsze, do interfejsu publicznej sieci telekomunikacyjnej może być co najwyżej połączone jedno z urządzeń wbudowanych w samochodzie (np. modem 5G lub LTE). Samochód jako taki jest stworzony z wielu różnych systemów elektronicznych i mechanicznych, które nie muszą być bezpośrednio połączone z urządzeniem łączącym się z siecią telekomunikacyjną. Celem samochodu i tych systemów nie jest przesyłanie, przetwarzanie czy odbieranie informacji, ale poruszanie się. Funkcja transmisji danych jest zatem funkcją dodatkową, zwiększającą komfort i bezpieczeństwo jego użytkowania, ale nie funkcją podstawową. Stosując analogicznie wykładnię EROD, za urządzenie końcowe należałby również uznać statki, czy samoloty, co jednak do tej pory nie miało miejsca. Dodatkowo warto podkreślić, nie każdy użytkownik połączonego samochodu będzie automatycznie użytkownikiem urządzenia końcowego w rozumieniu dyrektywy *ePrivacy*. Tym ostatnim jest bowiem osoba fizyczna korzystająca z publicznie dostępnych usług łączności elektronicznej. Tymczasem usługi komunikacji między połączonymi samochodami nie muszą być wcale publicznie dostępne – mogą być oferowane nie tylko ogółowi użytkowników, ale tylko np. użytkownikom określonej aplikacji czy marki samochodów.

Należy również pamiętać, że **zgoda** może być podstawą przetwarzania wyłącznie, jeśli została udzielona w sposób skuteczny. W tym celu musi ona być m.in. dobrowolna, konkretna i świadoma. Powinna być wyrażona odrębnie od umowy, w jasny i zrozumiały sposób, a także może być w każdym czasie odwołana (art. 7 RODO). Biorąc pod uwagę ilość danych już generowanych w samochodach i różne cele ich przetwarzania, spełnienie tych wymogów będzie ogromnie trudne i będzie zapewne wymagało przygotowania wielu różnych wzorów zgód, biorących pod uwagę również poziom zrozumienia poszczególnych użytkowników. Dodatkowych nakładów będzie wymagało zarządzanie takimi zgodami, ich zakresami oraz oświadczeniami o ich odwołaniu. Z perspektywy użytkownika, proces pozyskiwania takich zgód może być uważany za uciążliwy i niejasny.

Warto podkreślić, że CNIL w opublikowanym przez siebie Pakiecie Zgodności dotyczącym połączonych samochodów nie traktował samochodu jako urządzenia końcowego i nie ograniczał podstaw przetwarzania do zgody użytkownika. W modelach zakładających przekazywanie danych poza samochód (w scenariuszu nr 2: *in-out* lub w scenariuszu nr 3: *in-out-in*), jako podstawę komercyjnego przetwarzania danych wskazywał wykonanie umowy lub podjęcie działań na żądanie osoby, której dane dotyczą przed jej zawarciem, a jako podstawę realizacji funkcji *eCall* – wykonanie obowiązku prawnego[25].

W naszej ocenie, **nie powinno się wykluczyć z góry możliwości przetwarzania danych również na podstawie uzasadnionego prawnie interesu użytkowników samochodów, producentów lub dostawców usług, zwłaszcza w przypadku rozwiązań zwiększających bezpieczeństwo**. Wątpliwości budzi również wymóg spełnienia przesłanek z art. 6 RODO dla dalszego przetwarzania danych pobranych za zgodą użytkownika. Mogą wystąpić tutaj dwa podstawowe warianty. Takie dalsze przetwarzanie może być dokonywane w celu, w którym przyznany został dostęp do danych lub w którym były przechowywane (wariant pierwszy), albo w innym celu (wariant drugi).

[23] Dz.Urz. L Nr 131 z 27.5.1998 r., s. 73 ze zm.

[24] Dz.Urz. L Nr 201 z 31.7.2002 r., s. 37 ze zm.; dalej jako: dyrektywa *ePrivacy*.

[25] *Commission Nationale de l'Informatique et des Libertés*, Compliance Package: Connected Vehicles and Personal Data, *op. cit.*, s. 23 i n.

W pierwszym wariancie, stanowisko EROD oznacza, że przetwarzanie danych w jednym, tym samym celu wymaga dwóch podstaw prawnych: z art. 5 ust. 3 dyrektywy *ePrivacy* i z art. 6 RODO. W praktyce mogłyby to być różne podstawy, np. jeżeli kierowca zawarł umowę ubezpieczenia w modelu „płać jak jeździsz" (*pay-as-you-drive*), podstawą przechowania danych dotyczących jego jazdy i ich udostępnienia ubezpieczycielowi musiałaby być, zgodnie z art. 5 ust. 3 dyrektywy *ePrivacy*, zgoda tego użytkownika, natomiast podstawą do dalszej ich analizy przez ubezpieczyciela w celu ustalenia wysokości składki lub podstaw odpowiedzialności – wykonanie umowy lub działania podjęte na żądanie osoby fizycznej przed jej zawarciem [art. 6 ust. 1 lit. b) RODO]. Takie rozdzielenie podstaw przetwarzania wydaje się całkowicie sztuczne, zwłaszcza, że odwołanie zgody uniemożliwiałoby w praktyce wykonanie umowy ubezpieczenia, czyli osiągnięcie faktycznego celu przetwarzania.

W drugim wariancie, dane zebrane przez producenta samochodu w ramach działań serwisowych mogłyby być potencjalnie wykorzystane w innym celu, np. do poprawy jakości lub optymalizacji obsługi. W opinii EROD nie jest to jednak możliwe bez uzyskania kolejnej zgody osoby, której dane dotyczą, gdyż zastosowanie testu zgodności przewidzianego w art. 6 ust. 4 RODO obniżałoby standard ochrony wymagany na gruncie art. 5 ust. 3 dyrektywy *ePrivacy*. Takie podejście jest konsekwencją pierwotnego stanowiska EROD dotyczącego wymogu przetwarzania danych osobowych tylko na podstawie zgody. W naszej ocenie, wymaga ono jednak weryfikacji i w przypadku dopuszczenia innych podstaw przetwarzania, zastosowanie testu zgodności powinno być również akceptowalne.

Podsumowując, opieranie przetwarzania wyłącznie na zgodzie użytkownika samochodu nie tylko rodziłoby problemy prawne związane z przetwarzaniem danych w tych samych lub innych celach, ale z założenia zniechęcałoby do udzielania takich zgód, ograniczając zakres przetwarzanych danych, co może mieć niekorzystny wpływ na rozwój funkcji związanych z bezpieczeństwem pojazdów.

5. Transparentność

Zgodnie z jedną z podstawowych zasad przetwarzania danych, powinno ono być prowadzone w sposób przejrzysty dla osoby, której dane dotyczą [art. 5 ust. 1 lit. a) RODO]. Oznacza to w szczególności, że **osoba której dane dotyczą, powinna otrzymać informacje, o których mowa w art. 13 lub 14 RODO**. Sama Komisja Europejska zwraca uwagę, że **polityki prywatności wyświetlane w samochodach** potrafią liczyć nawet 15 stron[26]. Prowadzi to często do akceptacji tych warunków bez faktycznego zapoznania się z nimi przez użytkowników. Problem ten nie dotyczy wyłącznie producentów samochodów, czy dostawców aplikacji wykorzystywanych przez połączone samochody, ale wszelkich rozwiązań IT wykorzystujących dane osobowe.

O ile postulat wprowadzenia jednolitych oznaczeń, które mogłyby być stosowane w przypadku przekazywania określonych danych przez samochody połączone należy uznać za słuszny, to niektóre ze sposobów jego wykonania zaproponowane przez EROD mogą rozpraszać kierowców i wpływać negatywnie na bezpieczeństwo (np. proponowane przez EROD w pkt 86 Wytycznych, informowanie o przekazywaniu danych lokalizacyjnych oświetleniem w kabinie lub sygnałem). W przypadku niektórych funkcjonalności, np. dotyczących ostrzegania przed kolizją w trudnych warunkach (np. we mgle) funkcja lokalizacji może być włączona przez dłuższy czas – stałe emitowanie takiego sygnału nie będzie więc wpływało korzystnie na bezpieczeństwo użytkowników. Wielu użytkowników zapewne wyłączyłoby taką funkcję.

6. Przechowywanie danych

W Wytycznych EROD rekomenduje, aby dane osobowe były przechowywane w samochodzie, idealnie na specjalnej bezpiecznej platformie, odseparowanej od krytycznych funkcjonalności samochodu. Takie rozwiązanie, zdaniem EROD, pozwoli uniknąć wykorzystania usług chmurowych i związanych z nimi ryzyk.

Wprowadzenie odrębnej platformy do przechowywania danych, oddzielonej od pozostałych systemów, może ułatwić dostęp osób trzecich do danych, takich jak niezależne warsztaty samochodowe, które w chwili obecnej napotykają na problemy w dostępie do danych w związku z ograniczeniami nakładanymi przez producentów. Z drugiej strony, biorąc pod uwagę ilość danych generowanych przez samochody połączone, jak również konieczność przekazywania niektórych z tych danych na zewnątrz (np. do innych samochodów czy infrastruktury) **rekomendacje odnośnie lokalnego przechowywania i wątpliwości odnośnie przechowywania danych w chmurze nie są zrozumiałe**. Jak pokazała pandemia COVID-19, **usługi chmurowe**, z uwagi na ich zalety, są koniecznością nowoczesnych firm i mogą być świadczone w sposób bezpieczny. Usługi chmurowe mogą być też świadczone w oparciu o różne modele, w tym chmury prywatnej (producenta samochodów lub dostawcy usług), środowiskowej lub hybrydowej, w których ryzyka naruszenia bezpieczeństwa mogą być dodatkowo ograniczone, np. przez odpowiednią kwalifikację informacji, szyfrowanie czy przechowywanie w chmurze publicznej informacji mniej sensytywnych.

Wreszcie, brak stałej aktualizacji systemów informatycznych zwiększa ryzyko nieuprawnionego dostępu czy wystąpienia innych incydentów bezpieczeństwa. Na to ryzyko zwraca się uwagę też w Wytycznych, w których EROD sam wskazuje w pkt 57, że dane przechowywane w samochodzie mogą nie być zabezpieczone w wystarczający sposób przed nieupoważnionym dostępem. W chwili obecnej większość producentów nie zapewnia automatycznej i zdalnej aktualizacji oprogramowania samochodowego, a więc ryzyka związane z jej brakiem są jak najbardziej realne. Trudno wobec tego znaleźć uzasadnienie dla rekomendacji o lokalnym przechowywaniu danych i unikaniu usług chmurowych.

Connected cars a prawo telekomunikacyjne

1. Wprowadzenie

Jak wskazano powyżej, w celu zapewnienia komunikacji M2M w połączonych pojazdach, a w przyszłości także w pojazdach całkowicie autonomicznych, stosowane są różne technologie, wykorzystywane często łącznie. Najbardziej powszechne to bezprzewodowe sieci komórkowe, sieci Wi-Fi oraz system GPS. W wymiarze prawnym oznacza to, że podmioty zapew-

[26] *European Data Protection Supervisor*, TechDispatch #3: Connected Cars, *op. cit.*, rozdział „Lack of transparency".

niające komunikację M2M pomiędzy samochodami mogą mieć do czynienia z działalnością regulowaną jaką jest działalność telekomunikacyjna.

W komunikacie pt. „Łączność dla konkurencyjnego jednolitego rynku cyfrowego: w kierunku europejskiego społeczeństwa gigabitowego"[27] Komisja Europejska podkreśliła znaczenie dostępu do Internetu dla jednolitego rynku cyfrowego i potrzebę rozmieszczenia sieci służących cyfrowej przyszłości Europy. W tym celu, w komunikacie przedstawiono wizję europejskiego „społeczeństwa gigabitowego", w którym dostępność i wykorzystanie sieci o bardzo dużej przepustowości umożliwia powszechne korzystanie z produktów, usług i aplikacji w ramach jednolitego rynku cyfrowego. Realizacja tej wizji wymaga osiągnięcia do 2025 r. trzech celów strategicznych:

1) zapewnienia gigabitowego dostępu do Internetu w miejscach stanowiących siłę napędową rozwoju społeczno-gospodarczego, aby w ten sposób wspierać wzrost i zatrudnienie w Europie;
2) zapewnienia na wszystkich obszarach miejskich oraz na wszystkich głównych szlakach komunikacyjnych zasięgu sieci 5G, aby w ten sposób wspierać konkurencyjność Europy;
3) zapewnienia we wszystkich gospodarstwach domowych w Europie dostępu do Internetu o przepustowości co najmniej 100 Mb/s, aby w ten sposób wspierać spójność Europy.

Rząd Polski, w ramach przyjętej przez Radę Ministrów w dniu 10.3.2020 r. aktualizacji Narodowego Planu Szerokopasmowego, zobowiązał się do realizacji tych celów w ciągu najbliższych 5 lat. Duży nacisk w chwili obecnej kładzie się szczególnie na sieci 5G, które traktowane są jako jeden z najważniejszych czynników warunkujących postęp ekonomiczny i techniczny, a także przezwyciężania kryzysu wywołanego pandemią. Umożliwią one realizację innowacyjnych projektów, takich jak inteligentne systemy transportowe, przekształcając dotychczasowe modele biznesowe i wprowadzając nowe. Przewiduje się, że sieci 5G całkowicie zmienią sposoby interakcji pomiędzy urządzeniami mobilnymi i otaczającym użytkowników końcowych środowiskiem[28].

2. Sieci komórkowe

Komunikacja *machine to machine* oparta na sieciach komórkowych wymaga transmisji danych za pomocą tych sieci. Świadczenie usług transmisji danych w mobilnych sieciach telekomunikacyjnych stanowi regulowaną działalność telekomunikacyjną w świetle obecnie obowiązujących przepisów. Zgodnie z art. 1 ust. 1 pkt 1 ustawy z 16.7.2004 r. – Prawo telekomunikacyjne[29], **działalnością telekomunikacyjną** jest działalność polegająca na świadczeniu usług telekomunikacyjnych, dostarczaniu sieci telekomunikacyjnych lub świadczeniu usług towarzyszących. Zatem świadczenie usług telekomunikacyjnych stanowi odrębny rodzaj działalności telekomunikacyjnej obok dostarczania sieci telekomunikacyjnych i obok świadczenia usług towarzyszących. PrTelekom nie zawiera (nawet przykładowego) katalogu usług telekomunikacyjnych, w tym nie wyróżnia usług komunikacji M2M. Zamiast tego zawiera ogólną definicję usługi telekomunikacyjnej.

Usługa telekomunikacyjna w rozumieniu art. 2 pkt 48 PrTelekom to usługa polegająca głównie na przekazywaniu sygnałów w sieci telekomunikacyjnej. Niewątpliwe transmisja danych w sieci komórkowej w celu skomunikowania samochodów polega właśnie na przekazywaniu sygnałów w sieci telekomunikacyjnej, a więc stanowi usługę telekomunikacyjną. Definicja usługi telekomunikacyjnej jest na tyle szeroka, że nie ogranicza się tylko do przekazu sygnałów telekomunikacyjnych pomiędzy użytkownikami – osobami fizycznymi, może zatem obejmować też komunikację M2M. Zatem w chwili obecnej na gruncie obowiązującego PrTelekom, świadczenie usług M2M w oparciu o transmisję danych w sieciach komórkowych może stanowić regulowaną działalność telekomunikacyjną obwarowaną szeregiem obowiązków.

Nieco inne podejście proponuje polski ustawodawca w **projekcie PrKomEl**, stanowiącego implementację EKŁE. Nowością jest przede wszystkim **bezpośrednie odwołanie się do usług M2M**. O ile jednak projekt PrKomEl nie definiuje wprost usług M2M, to wprowadza – jako jeden z rodzajów usług komunikacji elektronicznej – **„usługi transmisyjne stosowane na potrzeby świadczenia usług komunikacji maszyna–maszyna"**[30]. Stanowi to odzwierciedlenie regulacji zawartej w art. 2 pkt 4c EKŁE. *Ratio legis* regulacji unijnej i podążającego za nim projektu PrKomEl jest, aby w przypadku usług transmisji danych na potrzeby realizacji komunikacji M2M, ich dostawcy zwolnieni byli z niektórych obowiązków wobec abonentów, w szczególności konsumentów, takich jak obowiązek informacyjny przed zawarciem umowy czy nieprzekraczanie maksymalnego okresu obowiązywania umowy. Zdaniem ustawodawcy unijnego, usługi transmisji danych na potrzeby realizacji komunikacji M2M nie są typowymi usługami abonenckimi. Zasadne jest zatem, aby dostawcy tych usług nie byli związani przepisami, których celem jest wyłącznie ochrona interesów abonentów[31]. Dodatkowo jednak **w preambule EKŁE, zdefiniowana została sama usługa komunikacji M2M**. Mianowicie, zgodnie z EKŁE, usługi M2M to usługi obejmujące automatyczne przesyłanie danych i informacji między urządzeniami lub aplikacjami opartymi na oprogramowaniu z ograniczonym udziałem człowieka lub bez jego udziału[32]. Definicji tej próżno doszukiwać się w projekcie PrKomEl, które w dalszej części posługuje się jeszcze nieco innym terminem, tj. „usługi transmisji danych używane do świadczenia usług komunikacji maszyna–maszyna", który to termin pomija kwestie transmisji informacji (towarzyszących transmisji danych) w usługach M2M.

Niemniej na gruncie projektu PrKomEl warto zwrócić uwagę na **rozróżnienie usług**, stanowiące pewne *novum*. Mianowicie, to nie sama usługa komunikacji M2M jest przedmiotem regulacji zawartej w projekcie PrKomEl (i EŁKE), ale właśnie usługa transmisyjna (transmisja danych) wykorzystywana na potrzeby świadczenia usług komunikacji maszyna–maszyna. Oznacza to, że pomimo, iż projekt PrKomEl nie definiuje samej usługi M2M, to wyraźnie rozgranicza pomiędzy samą usługą M2M

[27] Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 14.9.2016 r.; *op. cit.*

[28] Uzasadnienie do projektu PrKomEl, s. 2, dostępne na: https://legislacja.gov.pl/projekt/12336501.

[29] T. jedn.: Dz.U. z 2019 r. poz. 2460 ze zm.; dalej jako: PrTelekom.

[30] Art. 2 pkt 76 lit. c) projektu PrKomEl.

[31] Uzasadnienie do projektu PrKomEl, *op. cit.*, s. 112.

[32] Motyw (249) preambuły EKŁE.

(która nie jest przedmiotem nowej regulacji) od transmisji (danych) służącej realizacji usługi M2M. W konsekwencji oznacza to, że możliwy jest taki model działalności, w którym inny podmiot świadczy usługę M2M, a inny – usługę transmisji danych po to, aby usługa M2M mogła być zrealizowana. W obrocie gospodarczym, najczęściej tym drugim podmiotem dostarczającym transmisję danych będzie właśnie wpisany do rejestru przedsiębiorca telekomunikacyjny (operator lub dostawca usług telekomunikacyjnych) świadczący profesjonalnie usługi transmisji danych w sieciach komórkowych, nie tylko na potrzeby realizacji usług M2M.

Takie ujęcie problematyki usług M2M (wynikające z przepisów EŁKE) pozwoli na uniknięcie przez przedsiębiorców realizujących *stricte* usługę M2M konieczności poddania się reżimowi wynikającemu z prowadzenia działalności regulowanej. Ma to w szczególności znaczenie dla branży motoryzacyjnej, gdzie sama usługa M2M może być realizowana przez producenta pojazdu albo przez podmiot trzeci (dostawcę oprogramowania), zaś transmisja danych może zostać dostarczona przez operatora telekomunikacyjnego. Słusznie wskazuje Prezes UKE, że „operator (telekomunikacyjny – przyp. *A.S.*, *M.K-S*, *M.R.*) nie zawsze jest dostawcą kompleksowej usługi. Może mieć miejsce sytuacja, w której inny podmiot zakupi u operatora karty SIM przeznaczone do wykorzystania w modelu M2M, a następnie wyposaży je w swoje oprogramowanie, co nada im określone funkcjonalności"[33].

W niektórych modelach biznesowych podmiot realizujący usługę komunikacji M2M, np. producent pojazdu, będzie chciał jednak refakturować koszty zużytej na jej potrzeby transmisji danych dostarczonej przez operatora telekomunikacyjnego. Projekt PrKomEl utrzymuje w takiej sytuacji zasadę, zgodnie z którą sprzedaż we własnym imieniu i na własny rachunek usługi telekomunikacyjnej wykonanej przez innego dostawcę usług stanowi świadczenie usług telekomunikacyjnych, a więc regulowaną działalność gospodarczą[34].

Projekt PrKomEl powtarza też, co do zasady, **obowiązki ciążące na podmiotach wykonujących działalność telekomunikacyjną** z obowiązującego PrTelekom. Zatem także ci przedsiębiorcy, dla których działalność telekomunikacyjna (komunikacji elektronicznej) będzie stanowiła tylko dodatkową, akcesoryjną działalność w stosunku do podstawowej działalności gospodarczej, w dalszym ciągu będą podlegać uprzedniemu wpisowi do rejestru przedsiębiorców telekomunikacyjnych; obowiązkowi corocznego raportowania rodzaju i zakresu prowadzonej działalności telekomunikacyjnej; obowiązkowi dokonywania corocznej inwentaryzacji infrastruktury i usług; obowiązkom w zakresie bezpieczeństwa cybernetycznego, obronności i bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, itd.

Niewywiązanie się z któregokolwiek z powyższych obowiązków ustawowych podlega karze pieniężnej w wysokości do 3% przychodu uzyskanego przez dany podmiot w poprzednim roku kalendarzowym. Niezależnie od kar finansowych nakładanych na przedsiębiorców telekomunikacyjnych, Prezes UKE może nałożyć na osobę zarządzającą danym przedsiębiorstwem telekomunikacyjnym karę pieniężną w wysokości do 300% jej miesięcznego wynagrodzenia. Warto w tym miejscu zgłosić więc postulat *de lege ferenda*, że przedsiębiorcy, dla których działalność telekomunikacyjna będzie stanowiła tylko dodatkową, akcesoryjną działalność w stosunku do podstawowej działalności gospodarczej, powinni zostać zwolnieni z obowiązków regulacyjnych, ewentualnie obowiązki takie powinny zostać ograniczone do niezbędnego minimum, np. wpisu do rejestru prowadzonego przez Prezesa UKE.

W tym miejscu warto jednak wskazać na kolejną nowość. Mianowicie, na gruncie projektu PrKomEl nowym i zdecydowanie korzystnym dla wielu przedsiębiorców rozwiązaniem jest zawężenie definicji regulowanej działalności telekomunikacyjnej jedynie do usług telekomunikacyjnych publicznie dostępnych[35]. Przez usługę telekomunikacyjną publicznie dostępną projekt PrKomEl, tak jak obecne PrTelekom, rozumie usługę dostępną dla ogółu użytkowników[36]. Oznacza to, że w przypadku usług transmisyjnych na potrzeby komunikacji M2M niebędących usługami dostępnymi dla ogółu użytkowników, podmioty prowadzące działalność gospodarczą w takim zakresie nie zostaną objęte nowymi przepisami, czyli w konsekwencji nie będą podlegać obowiązkom regulacyjnym.

Ma to szczególnie doniosłe znaczenie w przypadku usług transmisji danych na potrzeby komunikacji M2M. Jak wspomniano powyżej, producenci samochodów lub podmioty dostarczające rozwiązania softwarowe do komunikacji M2M w połączonych pojazdach mogą refakturować usługi transmisyjne świadczone przez operatorów telekomunikacyjnych, co oznacza regulowaną działalność telekomunikacyjną ze wszystkimi powyżej wskazanymi konsekwencjami. Tymczasem w przypadku komunikacji M2M w połączonych pojazdach, najczęściej będzie tak, że będzie ona dostępna tylko dla ograniczonego kręgu odbiorców[37], np. dla posiadaczy określonego modelu samochodu. W konsekwencji, także usługa transmisyjna na potrzeby M2M nie będzie dostępna dla ogółu, ale właśnie dla posiadaczy takich pojazdów. Niepubliczny charakter usługi transmisyjnej na potrzeby komunikacji M2M umożliwi niestosowanie przepisów projektu PrKomEl do producentów samochodów (czy dostawców oprogramowania) dla pojazdów połączonych, jeśli zdecydują się oni na refakturowanie usługi transmisyjnej.

3. Sieci WiFi

Sieci Wi-Fi są powszechnie wykorzystywane do zapewnienia bezprzewodowego dostępu do Internetu, najczęściej w sposób nieodpłatny i przez podmioty, których podstawowym zakresem działalności jest inna działalność niż telekomunikacyjna (uniwersytety, galerie handlowe, hotele, restauracje, samorządy lokalne). W powyżej wspomnianym komunikacie Komisji Europejskiej pt. „Łączność dla konkurencyjnego jednolitego rynku cyfrowego: w kierunku europejskiego społeczeństwa gigabitowego" zaproponowano szereg inicjatyw, w tym inicjatywę „Wi-Fi dla Europy", która ma sprzyjać powszechnej dostępności połączeń Wi-Fi dla obywateli w całej UE. Celem jest ożywie-

[33] *Urząd Komunikacji Elektronicznej*, Raport UKE z października 2016 r.: Nasycenie usługami M2M oraz sposób ich wykorzystania w Polsce, s. 3, dostępny na: https://www.telepolis.pl/grafika/newsy/2016-10/internet_rzeczy_-_analiza.pdf.

[34] Art. 2 pkt 69 projektu PrKomEl.

[35] Art. 1 pkt 1 projektu PrKomEl.

[36] Art. 2 pkt 49 projektu PrKomEl.

[37] Ciekawym zagadnieniem w komunikacji M2M jest, czy w ogóle można mówić, iż jej użytkownikami są osoby fizyczne, skoro jest to komunikacja pomiędzy maszynami na podstawie rozwiązań softwarowych. Dopiero jej wynik w postaci informacji może być przekazywany do użytkownika.

nie europejskiej gospodarki cyfrowej i zwiększenie konkurencyjności, zachęcenie społeczeństw do aktywnego uczestnictwa w jednolitym rynku cyfrowym oraz sprostanie coraz większym potrzebom w zakresie łączności.

Transmisja danych za pomocą sieci Wi-Fi jest także wykorzystywana do zapewnienia komunikacji M2M w połączonych pojazdach. Obecne PrTelekom nie reguluje w szczególny sposób sytuacji prawnej sieci Wi-Fi, stąd świadczenie usługi dostępu do Internetu poprzez sieci Wi-Fi stanowi, co do zasady, regulowaną działalność telekomunikacyjną. PrTelekom nie wyłącza bowiem formalnie z zakresu regulowanej działalności telekomunikacyjnej usług, które są świadczone nieodpłatnie i tylko określonemu gronu użytkowników np. gościom restauracji.

Z aprobatą należy więc przyjąć art. 5 ust. 3 projektu PrKomEl, który w ślad za EKŁE, przewiduje, że nie stanowi działalności telekomunikacyjnej umożliwianie korzystania z publicznej sieci telekomunikacyjnej za pośrednictwem lokalnej sieci radiowej, jeżeli jest to działalność dodatkowa w stosunku do wykonywanej przez podmiot działalności głównej. Umożliwienie korzystania z sieci publicznej za pomocą sieci Wi-Fi należy rozumieć jako obejmujące nie tylko usługę dostępu do Internetu, ale także transmisję danych za pomocą sieci Wi-Fi, np. na potrzeby komunikacji M2M w połączonych samochodach. Warunkiem jest jednak, aby była to działalność dodatkowa w stosunku do wykonywanej przez podmiot działalności głównej. Nie ma natomiast potrzeby, aby była to usługa bezpłatna. Aczkolwiek w praktyce mogą powstać wątpliwości, kiedy udostępnianie usług za pośrednictwem sieci Wi-Fi stanowić będzie działalność dodatkową w stosunku do działalności głównej, projektowany zapis należy uznać za idący w dobrym kierunku. W istocie sankcjonuje on bowiem dotychczasową praktykę w tym zakresie.

4. GPS

Trzecim rodzajem technologii wykorzystywanej do zapewnienia komunikacji M2M w połączonych pojazdach jest system GPS. ***Global Positioning System*** – **GPS** to system nawigacji satelitarnej stworzony, utrzymywany i zarządzany przez rząd Stanów Zjednoczonych. Korzystać z jego usług może w zasadzie każdy – wystarczy tylko posiadać odpowiedni odbiornik GPS. Takie odbiorniki są produkowane przez niezależne firmy komercyjne. System GPS jest darmowy i taki ma pozostać zgodnie z polityką Stanów Zjednoczonych[38].

System GPS jest szeroko wykorzystywany do zapewnienia usług lokalizacji pojazdów i ich nawigacji. Jak słusznie podnosi się w doktrynie, ustalenie lokalizacji środków transportu może być wynikiem działań dostawcy usług telekomunikacyjnych, a może być także wynikiem zastosowania funkcji urządzenia końcowego użytkownika wyposażonego w lokalizator korzystający z sygnałów satelitarnych, np. GPS[39]. Zatem w zakresie, w jakim komunikacja M2M w pojazdach połączonych odbywać się będzie z wykorzystaniem systemu GPS, nie będzie ona stanowić regulowanej działalności telekomunikacyjnej.

[38] Zob. https://www.gps.gov/.

[39] *S. Piątek*, Prawo telekomunikacyjne. Komentarz, Warszawa 2019, kom. do art. 2 PrTelekom, s. 114–115.

Wyzwania

1. Brak definicji i spójnej regulacji dla połączonych samochodów i samochodów autonomicznych

Obecnie, regulacje dotyczące samochodów połączonych i autonomicznych są opracowywane rozdzielnie. Podstawową cechą wyróżniającą samochodów połączonych jest ich komunikacja ze światem zewnętrznym[40], natomiast samochodów autonomicznych – możliwość poruszania się samochodu bez kierowcy lub z jego ograniczonym zaangażowaniem. W Wytycznych, EROD nie odnosi się w ogóle do samochodów autonomicznych. Takie rozdzielenie regulacji wydaje się całkowicie niezrozumiałe i nie sprzyja tworzeniu spójnych standardów ochrony danych osobowych. O ile możliwe jest tworzenie samochodów połączonych, które nie są autonomiczne, to już odwrotna sytuacja będzie w praktyce niewykonalna. Co więcej, z uwagi na ograniczony wpływ kierowcy na jazdę samochodów autonomicznych, zakres danych osobowych dotyczących zwłaszcza stylu jazdy, powinien w ich przypadku ulec znacznemu ograniczeniu. Zwiększyć może się natomiast zakres danych pozyskiwanych z zewnątrz, w tym o innych użytkownikach ruchu. Danych tych w praktyce nie będzie można przetwarzać na podstawie zgody osób, których dane dotyczą. Wskazane byłoby zatem uwzględnienie regulacji dotyczącej samochodów autonomicznych w tworzonych rekomendacjach dotyczących przetwarzania danych osobowych.

2. Zdobycie zaufania użytkowników samochodów – obowiązek przejrzystego i rzetelnego informowania o przetwarzaniu danych

Z konsultacji publicznych przeprowadzonych w 2017 r. przez *Federation International de L'Automobile – Region I* wynika, że konsumenci chcą wiedzieć, jakie dane są przez nich udostępniane, gdy korzystają z samochodu. Większość z nich (90%) uważało, że dane generowane przez samochód powinny pozostać własnością jego właściciela lub użytkownika, a przetwarzanie powinno być oparte na zgodzie[41]. Konsultacje te doprowadziły do zawiązania inicjatywy *„my car my data"*, która ma zabezpieczać interesy kierowców i właścicieli samochodów połączonych. Stanowisko EROD dotyczące podstaw przetwarzania danych z samochodów połączonych niewątpliwie brało pod uwagę stanowisko konsumentów europejskich. Bez rzetelnej informacji o przetwarzaniu danych trudno będzie zmienić i ich stanowisko, i stanowisko regulatorów. Nie sprzyja temu obecny sposób realizowania obowiązku informacyjnego lub wymagań dotyczących zgody, który budzi coraz większe wątpliwości odnośnie swojej skuteczności. Naszym zdaniem, należałoby rozważyć zmianę podejścia do wykonywania obowiązku informacyjnego. Tytułem przykładu, odpowiednie ustawienia wraz z przedstawieniem konsekwencji mogłyby być przedstawiane przy lub po

[40] *Commission Nationale de l'Informatique et des Libertés*, Compliance Package: Connected Vehicles and Personal Data, *op. cit.*, s. 4.

[41] *Federation Internationale de L'Automobile Region I – Europe*, The Middle East and Africa, What Europeans think about connected cars, dostępne (w języku angielskim) na: http://mycarmydata.eu/docs/FIA_survey_2016.pdf.

zawarciu umowy sprzedaży samochodu, a przed jego dostarczeniem. Osoba fizyczna sprzedająca samochód używany powinna mieć możliwość szybkiego usunięcia albo w przypadku danych eksploatacyjnych, które mogą być przydatne innym użytkownikom – anonimizacji danych osobowych. Aplikacja samochodowa powinna również pozwalać na dokonanie świadomych ustaleń w zakresie danych przez kolejnych użytkowników.

3. Podstawy prawne przetwarzania danych

Trudno zgodzić się z argumentacją EROD, że samochód połączony jest telekomunikacyjnym urządzeniem końcowym i w rezultacie, z zastosowaniem wymogu zgody w celu przechowywania i uzyskiwania dostępu do generowanych w nim danych osobowych. Zgoda nie powinna być jedyną podstawą przetwarzania takich danych i należałoby wypracować scenariusze, w których dane mogą być przetwarzane na innych podstawach prawnych (np. w celu wykonania umowy) lub do innych celów, po przeprowadzeniu testu z art. 6 ust. 4 RODO.

4. Komunikacja M2M w pojazdach autonomicznych i połączonych

Na gruncie obecnego brzmienia projektu PrKomEl same usługi komunikacji M2M nie będą podlegać regulacji. Jednak wykorzystywana na potrzeby ich realizacji usługa transmisji danych w sieciach komórkowych pozostanie w dalszym ciągu regulowaną usługą telekomunikacyjną. Istnieją argumenty przemawiające za tym, aby producent samochodów nie był kwalifikowany jako przedsiębiorca telekomunikacyjny na gruncie projektu PrKomEl, nawet jeśli będzie świadczył kompleksową usługę obejmującą zarówno komunikację M2M, jak i usługę transmisyjną, z uwagi na ograniczony krąg odbiorców tych usług do użytkowników produkowanych przez niego samochodów. Stąd ważne jest, aby projekt PrKomEl utrzymał planowaną zasadę, że jego zakresem będą objęte jedynie publicznie dostępne usługi telekomunikacyjne. Jest to milowy krok w porównaniu z obecnym PrTelekom. M

Abstract:

Connected cars **– wybrane problemy i wyzwania regulacyjne**

Pojazdy połączone i autonomiczne stają się coraz popularniejsze. Zapewniają dostęp do nowych funkcjonalności, ale wytwarzają duże ilości danych. W maju 2020 r. zakończone zostały konsultacje projektu Wytycznych EROD dotyczących przetwarzania danych osobowych w samochodach połączonych. Wytyczne budzą wiele wątpliwości, np. odnośnie traktowania połączonego pojazdu jako urządzenia końcowego i wymogu zgody na przechowywanie i dostęp do zawartych w nim danych. Nowego podejścia wymaga też informowanie o przetwarzaniu danych. Na te kwestie nakłada się też implementacja Europejskiego kodeksu łączności elektronicznej. Projekt Prawa komunikacji elektronicznej porusza kwestie komunikacji *machine to machine* (M2M) wykorzystywanej w takich pojazdach. Dostawcy usług transmisji danych wykorzystywanej na potrzeby M2M będą objęci nowymi regulacjami tylko, jeśli ich usługi będą publicznie dostępne. Usługi świadczone dedykowanym odbiorcom nie zostaną objęte nowym reżimem.

Słowa kluczowe: połączone samochody, *connected cars*, dane osobowe, RODO, prawo telekomunikacyjne, Prawo komunikacji elektronicznej, 5G, pojazdy autonomiczne, *machine-to-machine*, M2M, Internet rzeczy, IoT

Connected cars – selected regulatory problems and challenges

Connected and autonomous cars are becoming increasingly popular. They provide access to new functionalities, but also generate large amounts of data. Consultations on the draft EDPB Guidelines for the processing of personal data in connected cars were completed in May 2020. The Guidelines raise doubts e.g. regarding treatment of the connected car as an end device and the requirement of granting consent for the storage of and access to the collected data. The approach to notifying data processing also needs to be verified. In addition, the implementation of the European Electronic Communications Code is approaching. The draft of Electronic Communications Act addresses the issues of machine to machine („M2M") communication used in such vehicles. Providers of data transmission services used for M2M will be subject to the new regulations only if their services are publicly available. Services provided to dedicated users will not be subject to the new regime.

Key words: connected cars, data protection, GDPR, telecommunications law, 5G, electronic communications law, autonomous vehicles, machine-to-machine, M2M, Internet of Things, IoT