39. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności

25-29 września 2017 r., Hongkong

Rezolucja w sprawie ochrony danych w automatycznych pojazdach połączonych

39. Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności:

Uznając, że automatyczne pojazdy połączone mogą stwarzać znaczne korzyści dla użytkowników ze względu na ich dużą łatwość użytkowania lub wygodę oraz dla społeczeństwa w ogóle, pozwalając na polepszenie ruchu drogowego i bezpieczeństwa kierowców i pasażerów pojazdów, jak również innych użytkowników dróg i pieszych;

Podkreślając szybki rozwój technologiczny automatycznych pojazdów połączonych pozwalających na rozwój i wprowadzenie na rynek nowych i innowacyjnych produktów, urządzeń lub usług telematycznych, które w większości przypadków zbierają i przetwarzają dane osobowe dzięki różnym czujnikom, które są w nich zainstalowane, co może prowadzić do nowych wyzwań dla podstawowych praw ochrony danych osobowych i prywatności użytkowników, w szczególności w różnych kontekstach, gdzie pojazdy mogą być używane przez wiele osób;

Biorąc pod uwagę Deklarację wypracowaną podczas spotkania ministrów transportu grupy G7 i Komisarza UE ds. transportu, które miało miejsce w Cagliari we Włoszech w dniach 21-22 czerwca 2017 r.[1], która stwierdza konieczność stosowania się do istotnych obowiązujących wytycznych dotyczących cyberbezpieczeństwa i ochrony danych osobowych i zaleca wszystkim podmiotom, aby oceniły, jak te dane mogą być wykorzystane do stworzenia usług i aplikacji, które polepszyłyby bezpieczeństwo i warunki ruchu drogowego, równocześnie respektując interesy konsumentów w zakresie cyberbezpieczeństwa i ochrony prywatności;

Zważywszy na deklarację wypracowaną podczas spotkania ministrów odpowiedzialnych za gospodarkę cyfrową grupy G20 w Dusseldorfie, w Niemczech, w dniach 6 - 7 kwietnia 2017 r., dotyczącą cyfryzacji w świecie wzajemnych powiązań[2], która stwierdza konieczność wzmocnienia zaufania w gospodarce cyfrowej, respektując jednocześnie ramy prawne ochrony danych i prywatności oraz zwiększające bezpieczeństwo wykorzystywania technologii informacyjno-komunikacyjnych, jak również przejrzystość i ochronę konsumentów;

Zaniepokojeni możliwym brakiem mechanizmów dotyczących informacji, wyboru dla użytkowników, kontroli nad danymi i ważnej zgody, które pozwoliłyby właścicielom, kierowcom i pasażerom pojazdów, innym użytkownikom dróg i pieszym kontrolować dostęp do danych pojazdów i do danych dotyczących prowadzenia pojazdów, jak również ich wykorzystania;

[1] http://www.g7italy.it/sites/default/files/documents/Final Declaration_0.pdf.
[2] https://www.bmwi.de/Redaktion/DE/Downloads/G/g20-digital-economy-ministerial-declaration-english-version.pdf?_blob=publicationFile&v=12

Obserwując rozwój różnych technologii współpracujących inteligentnych systemów transportowych, gdzie pojazdy przekazują swoje dane pozycyjne i kinematyczne, przekazując w sposób ciągły informacje do innych pojazdów (v2V), do infrastruktury transportowej (v2i) lub do innych podmiotów trzecich (v2x), aby stworzyć ogólny obraz sytuacji ruchu ulicznego w celu zapewnienia bezpieczeństwa i płynności ruchu drogowego;

Zaniepokojeni faktem, że nieograniczone i powszechne rozpowszechnianie danych przez pojazdy w kontekście komunikacji v2v, v2i i v2x może pociągać za sobą niezgodne z prawem przetwarzanie i nieuprawniony dostęp do danych osobowych kierowców, pasażerów i innych osób przez osoby trzecie oraz ich dalsze przetwarzanie;

Podkreślając jednakże, że technologie współpracujących inteligentnych systemów transportowych powinny być opracowywane w sposób pozwalający na identyfikowalność i uwierzytelnienie pojazdów, biorąc przy tym należycie pod uwagę zasady ochrony prywatności w fazie projektowania (*privacy by design*) oraz zasady domyślnej ochrony prywatności (*privacy by default*);

Uznając, że twórcy różnych technologii współpracujących inteligentnych systemów transportowych są świadomi ryzyka dotyczącego ochrony prywatności powodowanego przez te technologie i podjęli znaczne wysiłki na rzecz zminimalizowania tego ryzyka poprzez zmniejszenie ilości danych osobowych i uniemożliwienie identyfikacji osób, których dane dotyczą;

Podkreślając, że szerokie pozyskiwanie danych przekazywanych przez system pojazdów połączonych, obejmujący współpracujący inteligentny system transportowy, może nie tylko pociągać za sobą zgromadzenie profili przemieszczania się osób, ale także wytworzyć dużą ilość danych dotyczących oceny zachowań dotyczących prowadzenia pojazdu, które mogą stanowić ważne informacje dla pewnych podmiotów, np. firm ubezpieczeń komunikacyjnych, producentów samochodów, firm reklamowych i organów ds. egzekwowania prawa i przepisów ruchu drogowego, w szczególności gdy dane będą spersonalizowane, np. poprzez używanie identyfikatorów pojazdów transmisyjnych;

Wspominając rozwiązania wskazujące dobre praktyki, które są stosowane do celów nadawczych telewizji płatnych i komunikacji radiowo-cyfrowej policji, aby ograniczyć dostęp do rozpowszechnianych informacji tylko do uprawnionych odbiorców;

Zauważając, że Rzecznicy Ochrony Danych Osobowych i Prywatności dostarczają konkretnych wskazówek odnośnie do zasad ochrony prywatności mających zastosowanie do przetwarzania danych lub rozwiązań dotyczących automatycznych pojazdów połączonych;

Podkreślając, ze Światowe Forum do spraw ujednolicenia rozporządzeń dotyczących pojazdów zawarło wytyczne dotyczące cyberbezpieczeństwa i ochrony danych w swojej ujednoliconej rezolucji dotyczącej produkcji pojazdów (R.E.3)[3], jak w załączniku 6;

[3] https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29resolutions/ECE-TRANS-WP.29-78r5e.pdf

Potwierdzając wymogi określone w części 1 sekcji 4 wyżej wskazanych wytycznych dotyczących cyberbezpieczeństwa i ochrony danych, które obejmują uwzględnienie pojęć *privacy by design* oraz *privacy by default;*

Potwierdzając rezolucję w sprawie ochrony prywatności w fazie projektowania[4] przyjętą podczas 32. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności w 2010 r. w Jerozolimie, rezolucję w sprawie profilowania[5] przyjętą podczas 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności w 2013 r. w Warszawie, jak również rezolucję w sprawie Big Data przyjętą podczas 36. Międzynarodowej Konferencji w Fort Balaclava na Mauritiusie[6];

39. Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności wzywa wszystkie właściwe strony, a w szczególności:

- **organizacje normalizacyjne,**
- **organy władzy publicznej,**
- **producentów pojazdów i wytwórców wyposażenia,**
- **dostawców usług transportu osób i wynajmu samochodów,**
- **dostawców usług opartych na danych, takich jak usługi rozpoznawania mowy, nawigacji, zdalnej obsługi lub telematyczne usługi ubezpieczeń komunikacyjnych,**

do pełnego przestrzegania praw użytkowników do ochrony ich danych osobowych i prywatności oraz do brania ich pod uwagę na wszystkich etapach tworzenia i rozwoju nowych urządzeń lub usług.

Zatem wzywa się wyżej wymienione strony do:

1. zapewnienia osobom, których dane dotyczą, kompleksowych informacji na temat tego, jakie dane są gromadzone i przetwarzane podczas wykorzystywania pojazdów połączonych, do jakich celów i przez kogo,
2. zastosowania środków anonimizacji lub gdy to niemożliwe – pseudonimizacji, aby zredukować do minimum ilość danych osobowych,
3. przechowywania danych osobowych nie dłużej niż jest to konieczne do zgodnego z prawem celu, w jakim są one przetwarzane, do dalszych zgodnych celów, lub zgodnie z prawem lub zgodą, oraz do usunięcia ich po tym czasie,
4. dostarczania środków technicznych do usunięcia danych osobowych, gdy pojazd ma być sprzedany lub zwrócony właścicielowi,
5. zapewnienia szczegółowej i łatwej w zastosowaniu kontroli prywatności dla użytkowników pojazdów, aby osoby te mogły, gdy to właściwe, wyrazić zgodę lub wstrzymać dostęp do różnych kategorii danych znajdujących się w pojazdach,
6. zapewnienia środków technicznych pozwalających użytkownikom pojazdów na ograniczenie zbierania danych,

[4] https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf
[5] https://icdppc.org/wp-content/uploads/2015/02/Profiling-resolution2.pdf
[6] https://icdppc.org/wp-content/uploads/2015/2/resolution-on-Big-Data.pdf

7. zapewnienia bezpiecznych urządzeń do przechowywania danych, które zapewnią użytkownikom pojazdów całkowitą kontrolę dostępu do danych zbieranych przez ich pojazdy,
8. zapewnienia środków technicznych dla zapewnienia elementów bezpieczeństwa komunikacji online , które będą chronić przed cyberatakami i uniemożliwiać dostęp do danych osobowych, jak również ich przejęcie,
9. opracowania i wprowadzenia w życie technologii dla współpracujących inteligentnych systemów transportowych w sposoby, które :
    a. zapobiegają nieuprawnionemu dostępowi do danych osobowych pozyskanych przez pojazdy (v2v), infrastrukturę transportową (v2i) lub inne podmioty trzecie (v2x) i przejęciu tych danych,
    b. pozwalają użytkownikom pojazdów na zapobieganie wymianie danych pozycyjnych i kinematycznych, kontynuując jednak otrzymywanie powiadomień dotyczących ostrzeżeń na drogach,
    c. chronią przed nielegalnym śledzeniem i lokalizacją kierowców,
    d. zapewniają, aby mechanizmy bezpiecznej komunikacji v2v, v2i i v2x podczas procesu uwierzytelniania nie stanowiły dodatkowego ryzyka dla ochrony danych osobowych i prywatności,
    e. ograniczają ryzyko śledzenia pojazdów i identyfikacji kierowców.
10. respektowania zasad *privacy by default* i *privacy by design*, poprzez zapewnienie środków technicznych i organizacyjnych oraz procedur do zapewnienia poszanowania prywatności osoby, której dane dotyczą, zarówno przy ustalaniu sposobów przetwarzania, jak i przy przetwarzaniu danych,
11. opracowania technologii i struktur ochrony prywatności, które odpowiednio przetwarzają dane osobowe w pojazdach,
12. zagwarantowania, aby samouczące się algorytmy potrzebne dla automatycznych pojazdów połączonych były przejrzyste pod względem ich funkcjonalności i były poddawane uprzedniej ocenie przez niezależny organ w celu ograniczenia ryzyka dyskryminacyjnych decyzji zautomatyzowanych,
13. zapewnienia użytkownikom pojazdów sposobów prowadzenia pojazdów przyjaznych dla ochrony prywatności, z ustawieniami domyślnymi,
14. przeprowadzania oceny skutków dla ochrony danych dla nowego, innowacyjnego lub niosącego duże ryzyko tworzenia lub wdrażania tych technologii,
15. wspierania poszanowania ochrony danych osobowych użytkowników pojazdów poprzez odpowiedzialne przetwarzanie tych danych, przy należytym wzięciu pod uwagę szkód, jakie przetwarzanie i wykorzystywanie danych może spowodować dla użytkowników pojazdów,
16. prowadzenia dialogu z rzecznikami ochrony danych i prywatności w celu wypracowania narzędzi służących do zapewniania zgodności, które mają towarzyszyć przetwarzaniu związanemu z pojazdami połączonymi i zapewnić pewność prawną w tej dziedzinie.

Federalna Komisja Handlu USA wstrzymuje się od głosu w sprawie niniejszej Rezolucji.