



„SMARTFONY NA KÓŁKACH” INTELIGENTNE SAMOCHODY Z CHINY A CYBERBEZPIECZEŃSTWO EUROPY

Paulina Uznańska

WARSZAWA
GRUDZIEŃ 2025

„SMARTFONY NA KÓŁKACH”

INTELIGENTNE SAMOCHODY Z CHIN A CYBERBEZPIECZEŃSTWO EUROPY

Paulina Uznańska

© Copyright by Ośrodek Studiów Wschodnich im. Marka Karpia

REDAKCJA MERYTORYCZNA

Jakub Jakóbowski

REDAKCJA

Katarzyna Kazimierska

WSPÓŁPRACA

Szymon Sztyk, Matylda Skibińska

OPRACOWANIE GRAFICZNE

OSW

INFOGRAFIKA

Urszula Gumińska-Kurek

SKŁAD

Wojciech Mańkowski

ZDJĘCIE NA OKŁADCE

Shutterstock AI / Shutterstock.com



Ośrodek Studiów Wschodnich im. Marka Karpia
ul. Koszykowa 6a, 00-564 Warszawa
tel.: (+48) 22 525 80 00, info@osw.waw.pl

www.osw.waw.pl

ISBN 978-83-68327-46-5

Spis treści

TEZY | 5

WSTĘP | 8

I. INTELIGENTNE SAMOCHODY: PERSPEKTYWA CHRL | 9

1. Chińskie oceny zagrożeń dla cyberbezpieczeństwa | **10**
2. Metody regulacji i kontroli | **12**

II. DANE GROMADZONE PRZEZ INTELIGENTNE SAMOCHODY | 16

1. Dane wrażliwe | **16**
2. Dane osobowe | **18**

III. CYBERBEZPIECZEŃSTWO INTELIGENTNYCH SAMOCHODÓW | 21

IV. IMPLIKACJE DLA EUROPY I REKOMENDACJE DZIAŁAŃ | 23

1. Wnioski dla Europy płynące z chińskich regulacji | **24**
2. Stan obecny i rekomendowane kierunki działania UE | **25**

TEZY

- Na polskim i europejskim rynku pojawia się coraz więcej inteligentnych samochodów (智能网联汽车; Intelligent & Connected Vehicles; ICV), czyli aut wyposażonych w technologie łączności, które umożliwiają skanowanie otoczenia, geolokalizację, komunikację z infrastrukturą i zdalne usługi w czasie rzeczywistym. Pojazdy te mają możliwość ekspansywnego zbierania danych (m.in. geoprzestrzennych i osobowych). Choć technologie te starają się dziś rozwijać i wdrażać wszystkie koncerny samochodowe, to obecnie globalnym liderem w tym obszarze staje się Chińska Republika Ludowa (ChRL). Udział chińskich aut osobowych w sprzedaży w Polsce osiągnął ok. 7% po pierwszych dziewięciu miesiącach 2025 r., a w samym październiku przekroczył 10%. Zaawansowane technologicznie pojazdy będą stopniowo coraz bardziej dominować w ofercie kierowanej do Europy, w tym do Polski.
- Chińskie organy państwowe wskazują na inteligentne samochody jako fundamentalne zagrożenie dla bezpieczeństwa państwa. Akcentują przy tym ryzyko wycieku tajemnic państwowych, zbierania danych o infrastrukturze krytycznej i instalacjach wojskowych oraz transferu za granicę wrażliwych informacji o funkcjonowaniu gospodarki i społeczeństwa. Do głównych ryzyk zalicza się: zwiększoną podatność na cyberataki (przykładowo zdalne przejęcie samochodów lub zakłócenie działania ich czujników mogłoby doprowadzić do katastrof w ruchu lądowym), zbieranie przez pojazdy wrażliwych danych o otoczeniu samochodu (np. dotyczących infrastruktury krytycznej), a także z wnętrza auta (np. rozmów czy danych biometrycznych kierowcy i pasażerów). Chińscy regulatorzy wskazują również na ryzyko wycieku za granicę wiedzy pochodzącej z analizy zbiorów danych z milionów samochodów, umożliwiającej np. określenie natężenia ruchu wokół jednostek wojskowych, szacowanie poziomu aktywności gospodarczej, czy wynikającej z masowego skanowania i rozpoznawania twarzy przechodniów.
- Odpowiedzią ChRL na te wyzwania jest kompleksowy system regulacji, obejmujący m.in. zakaz przesyłania za granicę danych uznawanych za ważne dla bezpieczeństwa państwa oraz wrażliwych danych osobowych gromadzonych przez pojazdy poruszające się po chińskich drogach. Sugerowane jest też instalowanie w inteligentnych samochodach trybu umożliwiającego wyłączenie gromadzenia informacji z otoczenia pojazdu. W przypadku producentów zagranicznych Pekin uzależnia także możliwość poruszania

się pojazdu w niektórych obszarach Chin od przejścia zaawansowanego procesu certyfikacji. Przykładowo inteligentne samochody amerykańskiej marki Tesla funkcjonujące na chińskim rynku podlegały do niedawna nieoficjalnym ograniczeniom dotyczącym poruszania się i parkowania, m.in. w pobliżu budynków rządowych, na lotniskach i autostradach oraz w miejscach, w których planowano wydarzenia z udziałem kluczowych przedstawicieli KPCh, w tym Xi Jinpinga. Produkowane w Szanghaju od 2019 r. auta Tesli przeszły proces certyfikacji w 2024 r. – po serii chińskich testów bezpieczeństwa danych. Działania te są elementem szerszej strategii państwa, w ramach której Chiny ustanawiają narzędzia regulacyjne mające zagwarantować, że inteligentne pojazdy będą wykorzystywane na terenie kraju zgodnie z interesem państwowym definiowanym przez KPCh. Równolegle Pekin zabiega o pogłębioną integrację technologii inteligentnych samochodów z technologiami o potencjalnym zastosowaniu militarnym, m.in. z systemem satelitarnym BeiDou.

- Wprowadzie w istniejących regulacjach ChRL podchodzi do kwestii inteligentnych samochodów defensywnie, niemniej w przyszłości może wykorzystać ich potencjał, aby podjąć działania ofensywne. Wskazują na to pośrednio logika i poziom rozbudowania regulacji wewnętrznych dotyczących tych pojazdów, zaawansowane zdolności ofensywne Chin w cyberprzestrzeni, rozwinięty ekosystem wywiadowczy, a także niektóre dokumenty strategiczne (np. zalecenie państwowe w sprawie łączenia technologii cywilnych i wojskowych w rozwoju inteligentnych samochodów). Rodzi to potrzebę wnikliwych działań sprawdzających inteligentne pojazdy pod kątem m.in. skanowania infrastruktury krytycznej przez liczne sensory, zbierania informacji wrażliwych, cyberataków. Ma to szczególne znaczenie w związku z nieformalnym sojuszem Chiny–Rosja i ryzykiem ewentualnego przekazywania Federacji Rosyjskiej danych gromadzonych obecnie przez inteligentne auta poruszające się po europejskich drogach. Takie pojazdy, niezależnie od kraju pochodzenia producenta, są również podatne na cyberataki, a ze względu na możliwości zdalnego sterowania – także na wykorzystanie do aktów dywersji.
- Obecnie nie istnieją kompleksowe przepisy unijne, które kształtowałyby ramy prawne funkcjonowania inteligentnych samochodów. Jest to technologia przełomowa, która wymaga szczegółowych i możliwych do wyegzekwowania ram regulacyjnych, zapobiegających m.in. automatycznemu transferowi danych wrażliwych za granicę oraz ograniczających ryzyko cyberataków. Rozwiązania chińskie mogą stanowić punkt wyjścia do

zrozumienia ryzyk związanych z tą technologią, a pośrednio też tworzenia środowiska regulacyjnego dla ich ograniczania. Wzorowanie się na chińskich dokumentach jako zbiorze dobrych praktyk dałoby istotny argument w komunikowaniu władzom ChRL ewentualnej decyzji o wprowadzeniu ściślejszych regulacji dotyczących chińskich inteligentnych aut. Ponadto zaostrzone regulacje, np. nakazujące przechowywanie danych w Polsce czy Europie i użycie lokalnych rozwiązań IT, mogłyby stać się skutecznym narzędziem polityki przemysłowej, zmuszającym chińskie firmy do lokalizacji wartości dodanej zaawansowanych usług w UE.

WSTĘP

Wzrost popularności chińskich aut rozbudził w Europie dyskusje na temat wiążących się z tym zagrożeń dla cyberbezpieczeństwa, wynikających m.in. z wykorzystania rozlicznych sensorów do aktywności szpiegowskiej czy potencjalnego użycia autonomicznych samochodów do aktów sabotażu. Częstym punktem odniesienia w tych dyskusjach są regulacje i analizy ryzyka wprowadzane w innych państwach, m.in. Stanach Zjednoczonych, Wielkiej Brytanii czy Izraelu. Tymczasem **to sama ChRL posiada jeden z najbardziej rozbudowanych systemów regulacji i standaryzacji dla inteligentnych pojazdów**. Chińskie instytucje państwowe **wskazują na szereg wynikających z tego zagrożeń dla cyberbezpieczeństwa i w asertywny sposób kontrolują poruszające się po chińskich drogach samochody zagranicznych producentów, jak Tesla**. Niniejszy raport ma przybliżyć tamtejszy ekosystem regulacyjny, dając zarówno wgląd w podejście chińskich władz do inteligentnych aut, jak i wartościowy punkt wyjścia do wdrażania podobnych regulacji w Europie.

Celem jest ukazanie, w jaki sposób Chiny definiują technologię inteligentnych samochodów – zarówno jako **źródło strategicznych szans**, jak i obszar potencjalnych **zagrożeń dla bezpieczeństwa państwa**. Analiza obejmuje przegląd wybranych **ram regulacyjnych tworzonych przez organy ChRL** w celu zarządzania tymi ryzykami. Badanie opiera się na **dokumentach chińskojęzycznych (mandaryńskich) publikowanych przez instytucje centralne i lokalne** – w tym ministerstwa, organy regulacyjne, jednostki standaryzacyjne oraz administracje miejskie. Obejmuje zarówno akty prawnie wiążące, jak i projekty regulacji i norm, które wskazują na kierunek rozwoju przyszłych polityk. Raport nie ma charakteru kompleksowego i może nie uwzględniać niektórych dokumentów wydanych przez chińskie instytucje, co wynika m.in. z silnie zamkniętego charakteru tamtejszego internetu. Wszystkie wykorzystane materiały pochodzą ze źródeł otwartych.

I. INTELIGENTNE SAMOCHODY: PERSPEKTYWA CHRL

W Chinach branża motoryzacyjna uznawana jest za strategiczny filar przyszłości technologicznej państwa. Inteligentne samochody znajdują się w centrum zainteresowania władz ChRL od 2015 r. – pojawiają się już we flagowej strategii przemysłowej ChRL „Made in China 2025” jako ważny kierunek modernizacji chińskiego przemysłu motoryzacyjnego¹. Wzrost sektora inteligentnego transportu stanowi również jedno z założeń rozwojowych wpisanych w XIV pięcioletni plan ChRL na lata 2021–2025².

Organy państwowe ChRL wskazują na strategiczne znaczenie tej branży:

*Rozwój inteligentnych samochodów sprzyja podnoszeniu podstawowych zdolności przemysłowych, przełamywaniu kluczowych barier technologicznych, **wzmacnianiu zdolności do przewodzenia nowej rewolucji technologicznej i przemysłowej** oraz kształtowaniu nowych przewag konkurencyjnych przemysłu³.*

Inteligentne samochody to dla Chin nie tylko przyszłość motoryzacji, lecz także element budowy potęgi militarnej. Technologia ta w optyce chińskiej nie należy wyłącznie do sektora cywilnego, ale ma też służyć **wzmacnianiu potencjału wojskowego ChRL**. Wpisuje się to w promowaną przez Xi Jinpinga politykę przenikania się sektora wojskowego i cywilnego (军民融合) – polegającą na eliminowaniu barier między sektorem badań cywilnych a przemysłem obronnym i ukierunkowaną na stworzenie najbardziej zaawansowanej technologicznie armii świata. Z perspektywy ChRL szczególne znaczenie ma system satelitarny BeiDou, który z jednej strony zapewnia precyzyjne usługi nawigacji w inteligentnych samochodach, z drugiej zaś jest strategicznie ważny dla operacji wojskowych.

¹ Plan „Made in China 2025” (中国制造2025), Rada Państwowa ChRL, 19.05.2015, gov.cn, wersja anglojęzyczna: *Notice of the State Council on the Publication of “Made in China 2025”*, CSET, 10.03.2022, cset.georgetown.edu.

² XIV pięcioletni plan rozwoju gospodarczego i społecznego Chińskiej Republiki Ludowej oraz cele długoterminowe na rok 2035 (中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要), Rada Państwowa ChRL, 13.03.2021, gov.cn, wersja anglojęzyczna: *Outline of the People’s Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035*, CSET, 13.05.2021, cset.georgetown.edu.

³ *Strategia rozwoju innowacji w dziedzinie inteligentnych pojazdów* (智能汽车创新发展战略), 24.02.2020, ndrc.gov.cn.

Według międzyresortowego zespołu do spraw strategii rozwoju innowacji w dziedzinie inteligentnych pojazdów w ChRL:

*Należy prowadzić wojskowo-cywilne inicjatywy badawcze i przyspieszyć wdrażanie systemu nawigacji satelitarnej BeiDou oraz systemu obserwacji Ziemi o wysokiej rozdzielczości **w dziedzinach związanych z inteligentnymi pojazdami***⁴.

Jak wskazuje Ministerstwo Przemysłu i Technologii ChRL:

*Konieczne jest wspieranie budowy **systemu nawigacji satelitarnej BeiDou**, stacji bazowych i innych obiektów infrastruktury, **zwiększanie skali stosowania wysokoprecyzyjnych usług czasowo-przestrzennych dla pojazdów** oraz zaspokojenie zapotrzebowania na wysokoprecyzyjne usługi nawigacji.*

*Należy **wspierać tworzenie mechanizmu współdzielenia danych map podstawowych dla inteligentnych pojazdów oraz danych teledetekcyjnych z satelitów***⁵.

Z chińskich dokumentów państwowych wynika, że inteligentne samochody mają służyć:

- budowie potencjału technologicznego;
- rozwijaniu cywilno-wojskowych inicjatyw badawczych;
- wspieraniu systemu nawigacji satelitarnej BeiDou.

1. Chińskie oceny zagrożeń dla cyberbezpieczeństwa

Rozwój inteligentnych pojazdów w Chinach idzie w parze z obawami o bezpieczeństwo narodowe. W dokumentach państwowych zagrożenia te definiuje się następująco: 1) pojazdy inteligentne zwiększają podatność na cyberataki (na przykład zdalne przejęcie kontroli nad nimi lub zakłócenie działania ich czujników może prowadzić do poważnych wypadków drogowych), 2) samochody te gromadzą wrażliwe dane zarówno z otoczenia, jak i z wnętrza (np. dane dotyczące infrastruktury krytycznej; dane biometryczne kierowcy i pasażerów), co zwiększa podatność na analizę wywiadowczą.

⁴ Ibidem.

⁵ *Plan działania na rzecz rozwoju przemysłu (inteligentnych) pojazdów połączonych z internetem* (车联网(智能网联汽车)产业发展行动计划), Ministerstwo Przemysłu i Technologii Informatycznych ChRL, 25.12.2018, gov.cn.

Według Państwowej Komisji Standaryzacyjnej ChRL:

*Inteligentne pojazdy, jako środki transportu wykorzystywane w życiu codziennym, mają naturalną przewagę w pozyskiwaniu i gromadzeniu danych geoprzestrzennych z rozległych obszarów, przez długi czas i na wielu poziomach. Ogromne ilości zgromadzonych danych mogą być wykorzystywane do **analizy wywiadowczej, oceny infrastruktury wojskowej i cywilnej oraz analizy wzorców działań w sferze obronnej i gospodarczej**. Stwarzają tym samym potencjalne **zagrożenie dla bezpieczeństwa państwa**.*

Wskazuje się również na istotne ryzyka wycieku tajemnic państwowych:

Dane geoprzestrzenne o wysokiej dokładności [gromadzone przez inteligentne samochody] (...) obejmują informacje przestrzenne, chmury punktów i obrazy. Na mocy przepisów dotyczących tajemnic państwowych w zakresie zarządzania informacjami i pomiarami geograficznymi należą one do kategorii „trójwymiarowych modeli, chmur punktów, zdjęć skośnych, zdjęć rzeczywistych, nawigacyjnych map elektronicznych itp. o poziomej dokładności wyższej lub równej 10 metrów (poza strefami wojskowymi) lub względnej dokładności pomiaru wysokości obiektów lepszej lub równej 5%, których ciągły zasięg pokrywa obszar większy niż 25 km²”. Dane te stanowią **tajemnicę państwową**.

[Inteligentne samochody] generują problemy związane z **nielegalnym pozyskiwaniem, przechowywaniem i przekazywaniem (za granicę) danych geoprzestrzennych**, co może łatwo doprowadzić do ujawnienia **tajemnic państwowych**.

Wśród zagrożeń wymienia się też cyberataki i zdalne przejęcie kontroli nad pojazdami – wskazuje się na nie w wymaganiach miasta Shenzhen, będącego obszarem pilotażowym dla wdrażania samochodów autonomicznych i regulacji prawnych dotyczących ich funkcjonowania w ChRL:

Wraz z rozwojem poziomu inteligencji i sieciowego połączenia pojazdów zyskujemy większą kontrolę nad samochodami, co przynosi liczne udogodnienia w życiu codziennym. Równocześnie jednak coraz bardziej uwidaczniają się zagrożenia, takie jak **cyberataki, wycieki informacji, a nawet możliwość zdalnego przejęcia kontroli nad inteligentnymi pojazdami**⁶.

⁶ Wymagania dotyczące bezpieczeństwa danych dla inteligentnych pojazdów połączonych (智能网联汽车数据安全要求), rząd miasta Shenzhen, 22.08.2023, sz.gov.cn.

Technologie inteligentnych samochodów producentów zagranicznych zostały wprost wskazane jako zagrożenie dla bezpieczeństwa narodowego:

*Szerokie wykorzystanie i promocja **pojazdów oraz marek zagranicznych producentów na terenie kraju** stwarzają **potencjalne i niemożliwe do oszacowania zagrożenia dla bezpieczeństwa informacji geoprzestrzennych oraz bezpieczeństwa narodowego Chin**⁷.*

Rozwój inteligentnych samochodów jest przez ChRL postrzegany jako źródło istotnych zagrożeń dla bezpieczeństwa państwa, obejmujących:

- podatność pojazdów na cyberataki;
- ryzyko zdalnego przejęcia kontroli nad pojazdami;
- zbieranie wrażliwych danych z otoczenia samochodu (np. dotyczących infrastruktury krytycznej);
- gromadzenie wrażliwych danych z wnętrza pojazdu (np. nagrywanie rozmów oraz zbieranie danych biometrycznych kierowcy i pasażerów).

Szczegółne zagrożenie stanowią pojazdy zagranicznych producentów.

2. Metody regulacji i kontroli

W obliczu rewolucji technologicznej w motoryzacji Chiny stawiają na ścisłą kontrolę inteligentnych samochodów. Jej fundamentem są dwie ustawy: o cyberbezpieczeństwie (z 2017 r.) i o bezpieczeństwie danych (z 2021 r.). Nakładają one na producentów liczne obowiązki, m.in.: przechowywania kluczowych danych wyłącznie w Chinach (ich transfer za granicę wymaga zgody Państwowej Administracji ds. Cyberprzestrzeni); wdrożenia systemów zarządzania bezpieczeństwem; kategoryzowania danych według znaczenia, w tym dla państwa, oraz dokonywania ocen ryzyka i raportowania do regulatorów.

Jak stwierdzają chińskie organy państwowe, **inteligentne samochody są na tyle przełomową technologią, że wymagają ciągłej aktualizacji ram regulacyjnych:**

⁷ Podstawowe wymagania dotyczące testów bezpieczeństwa systemu czujników wykorzystujących dane przestrzenno-czasowe inteligentnych i połączonych pojazdów (智能网联汽车时空数据传感系统安全检测基本要求), Państwowa Komisja Standaryzacyjna ChRL, 2023, std.samr.gov.cn.

*Inteligentne pojazdy – symbole nowej fali rewolucji technologicznej i transformacji przemysłowej – rozwijają się w szybkim tempie. Imponujące postępy w technologii motoryzacyjnej uwiadcniają **opóźnienia w zakresie przepisów, regulacji oraz standardów technicznych dotyczących cyberbezpieczeństwa i ochrony danych inteligentnych pojazdów.***

*Aby zapewnić **bezpieczeństwo państwa**, w tym **bezpieczeństwo danych geoprzestrzennych**, należy pilnie opracować odpowiednie przepisy i standardy [dotyczące inteligentnych pojazdów], a także **wzmocnić nadzór i zarządzanie tym sektorem**⁸.*

Wspomniane ustawy stanowią fundament uzupełniany stopniowo regulacjami administracyjnymi oraz standardami technicznymi, które państwo może szybko aktualizować wraz z rozwojem technologii inteligentnych samochodów. Proces tworzenia nowych ram nadzorują Ministerstwo Przemysłu i Technologii Informatycznych oraz Państwowa Komisja Standaryzacyjna ChRL. W ich ramach działa Państwowa Komisja Techniczna ds. Standaryzacji Mobilności oraz jej Podkomisja TC114/SC34 ds. Pojazdów Inteligentnych i Połączonych z Siecią (全国汽车标准化技术委员会智能网联汽车分技术委员会编号TC114/SC34). W pracach podkomisji uczestniczy 72 ekspertów, głównie przedstawiciele sektora motoryzacyjnego.

Ważną rolę odgrywają również władze lokalne, które opracowują regionalne, nieobowiązkowe standardy techniczne dla przedsiębiorstw. W tym zakresie wyróżnia się m.in. miasto Shenzhen – jeden z kluczowych ośrodków innowacji w Chinach, którego władze stworzyły szereg lokalnych norm dotyczących inteligentnych aut. Część z nich obejmuje zagadnienia kluczowe z perspektywy bezpieczeństwa państwa, takie jak ochrona danych i cyberbezpieczeństwo.

Powyższe regulacje uzupełnia dodatkowy system testów i certyfikacji dla producentów pojazdów inteligentnych. Działania te prowadzone są od 2024 r. przez Chińskie Stowarzyszenie Producentów Samochodów (中国汽车工业协会) oraz Państwowe Centrum Koordynacji Zespołów Technicznych ds. Reagowania na Sytuacje Kryzysowe w Sieci Komputerowej ChRL (国家计算机网络应急技术处理协调中心). W testach ocenia się:

- a. **skuteczność anonimizacji danych o twarzach** (zdjęć kierowców, pasażerów) oraz **danych dotyczących otoczenia pojazdu** (np. zdjęć twarzy przechodniów, tablic rejestracyjnych innych samochodów); system pojazdu musi

⁸ Ibidem.

wykrywać co najmniej 90% twarzy i tablic rejestracyjnych w danych (zdjęciach i nagraniach wideo) oraz poddawać je anonimizacji;

- b. **przetwarzanie danych z kabiny wewnątrz pojazdu:** dane osobowe zebrane z kabiny pojazdu mogą być przekazywane podmiotom zewnętrznym wyłącznie za zgodą osoby, której dotyczą; zabrania się przesyłania danych osobowych bezpośrednio za granicę;
- c. **domyślne niegromadzenie danych z kabiny pojazdu:** zbieranie danych w kabinie pojazdu powinno wymagać uprzedniej konfiguracji przez kierowcę;
- d. **powiadamianie o przetwarzaniu danych osobowych:** powiadomienie musi określać kategorie przetwarzanych danych osobowych oraz uzasadniać konieczność przetwarzania każdej z nich (w tym cel, sposób wykorzystania i metody przetwarzania); informacja powinna wskazywać okres i miejsce przechowywania zgromadzonych danych osobowych;
- e. **precyzyjność i adekwatność danych gromadzonych przez pojazd:** zakres i jakość danych zbieranych przez pojazd powinny być adekwatne do realizowanych funkcji. Przykładowo, jeśli funkcja wymaga jedynie wykrycia przeszkody, kamery pojazdu nie powinny nagrywać obrazu w jakości pozwalającej identyfikować twarze przechodniów poruszających się w okolicy samochodu. Jest to najnowszy rodzaj testu, dodany do pozostałych czterech w sierpniu 2025 r.⁹

Samochody marki Tesla były w Chinach nieformalnie wykluczane z poruszania się w pobliżu wrażliwych obiektów, takich jak:

- budynki rządowe;
- obiekty wojskowe;
- lotniska;
- autostrady;
- miejsca planowanych wydarzeń z udziałem kluczowych przedstawicieli KPCh, w tym Xi Jinpinga.

⁹ [Komunikat dotyczący wyników testów pięciu wymogów bezpieczeństwa przetwarzania danych samochodowych, III tura](#) (关于汽车数据处理5项安全要求检测情况的通报 (第三批), Chińskie Stowarzyszenie Producentów Samochodów, 18.08.2025, caam.org.cn).

Produkująca swe auta w Szanghaju od 2019 r. Tesla jest pierwszym zagranicznym (amerykańskim) przedsiębiorstwem motoryzacyjnym, które uzyskało certyfikację bezpieczeństwa danych chińskich władz. Pozytywną ocenę wydano w kwietniu 2024 r. i dotyczyła ona dwóch modeli marki: Tesli Model 3 i Tesli Model Y. Oficjalnie udział w testach bezpieczeństwa danych jest dobrowolny i otwarty zarówno dla producentów krajowych, jak i zagranicznych. Przed uzyskaniem certyfikacji samochody Tesli podlegały jednak nieformalnym ograniczeniom dotyczącym poruszania się i parkowania w pobliżu miejsc newralgicznych z punktu widzenia bezpieczeństwa państwa, jak instytucje rządowe, obiekty wojskowe, lotniska, autostrady, a także takich, w których planowano wydarzenia z udziałem kluczowych przedstawicieli KPCh, w tym Xi Jinpinga. Restrykcje te obowiązywały pomimo uruchomienia przez Teslę już w 2021 r. w Szanghaju centrum danych w celu dostosowania się do przepisów dotyczących lokalnego przechowywania danych generowanych w Chinach. Tesla poinformowała, że uzyskanie certyfikacji bezpieczeństwa ma umożliwić jej samochodom szerszy dostęp do wspomnianych miejsc. Ważność tych certyfikatów wygaśnie jednak po dwóch latach.

Do przedsiębiorstw chińskich, które otrzymały dotychczas certyfikację na wybrane modele, należą m.in.: BYD, Li Auto, Lotus, Hozon New Energy, NIO, Chongqing Changan, SAIC, Chery, Geely, Great Wall, XPeng i FAW-Volkswagen. Niektórzy producenci, m.in. BYD, XPeng i Geely, są już obecni na polskim rynku.

Chiny budują rygorystyczny system regulacji inteligentnych samochodów, obejmujący:

- certyfikację bezpieczeństwa danych;
- standardy techniczne – państwowe i lokalne;
- regulacje administracyjne;
- kluczowe ustawy: o cyberbezpieczeństwie, o bezpieczeństwie danych oraz o ochronie danych osobowych.

II. DANE GROMADZONE PRZEZ INTELIGENTNE SAMOCHODY

Inteligentne samochody – dzięki radarom, czujnikom, kamerom o wysokiej rozdzielczości, precyzyjnym mapom oraz globalnym satelitarnym systemom nawigacyjnym (GNSS) – mogą obserwować, rejestrować i analizować dane zarówno z otoczenia, jak i z wnętrza pojazdu. W chińskich dokumentach państwowych opisano typy tych danych oraz sposoby zarządzania nimi.

1. Dane wrażliwe

Dane wrażliwe zdefiniowano jako **dane mające newralgiczne znaczenie dla bezpieczeństwa państwa**. Należą do nich:

- a. dane dotyczące **informacji geoprzestrzennych, przepływu osób i pojazdów we wrażliwych obszarach**, takich jak **strefy zarządzania wojskowego, jednostki przemysłu obronnego i naukowego oraz organy partyjne i rządowe na szczeblu powiatu i wyższym**;
- b. dane dotyczące **natężenia ruchu pojazdów, logistyki i innych aspektów funkcjonowania gospodarki**;
- c. dane dotyczące funkcjonowania **sieci ładowania pojazdów elektrycznych**;
- d. dane wideo i zdjęcia z kamer zewnętrznych pojazdów zawierające **informacje o twarzach osób i numerach rejestracyjnych pojazdów**;
- e. dane osobowe dotyczące **ponad 100 tys. osób**;
- f. inne dane określone przez krajowe organy ds. informacji i komunikacji, a także przez odpowiednie organy państwowe, takie jak Państwowa Komisja Rozwoju i Reform, Ministerstwo Przemysłu i Technologii Informacyjnych, Ministerstwo Bezpieczeństwa Publicznego oraz Ministerstwo Transportu, mające newralgiczne znaczenie dla bezpieczeństwa narodowego, interesu publicznego lub praw i interesów osób¹⁰.

¹⁰ *Postanowienia dotyczące zarządzania bezpieczeństwem danych samochodowych (wersja próbna)* (汽车数据安全管理若干规定(试行)), Państwowa Administracja ds. Cyberprzestrzeni ChRL, Państwowa Komisja Rozwoju i Reform ChRL, Ministerstwo Przemysłu i Technologii Informacyjnych ChRL, Ministerstwo Bezpieczeństwa Publicznego ChRL, Ministerstwo Transportu ChRL, 16.08.2021, gov.cn.

Dodatkowo dane wrażliwe zbierane przez inteligentne pojazdy klasyfikowane są wedle kilku typów:

dane najwyższej wagi, których wyciek stanowiłby poważne zagrożenie dla bezpieczeństwa państwa (typ S3)	np. mapy obszarów wrażliwych, natężenie ruchu wokół stref wojskowych i instytucji rządowych, zbiory danych obejmujące powyżej 100 tys. osób, część danych dotyczących działania sieci ładowania samochodów, dane dotyczące ruchu drogowego, np. jego natężenia czy przepływu osób
dane wysokiej wagi (typ S2)	np. dane o przepływach logistycznych, nagrania zewnętrzne zawierające zdjęcia twarzy oraz tablic rejestracyjnych, część danych o pracy sieci ładowania pojazdów elektrycznych, dane decyzyjne systemów AD, dane dotyczące stanu pojazdu (np. stanu zasilania i ładowania, trybu sterowania i napędu, aktualnego biegu, stanu hamulców, świateł, wycieraczek i pasów bezpieczeństwa pojazdu, aktualnego poziomu paliwa i naładowania akumulatora itp.)
dane niskiej wagi (typ S1)	np. numery VIN, logi operacyjne kierowcy, zagregowane dane o zachowaniach kierowcy
dane najniższej wagi (typ S0)	wymiary pojazdu, dane techniczne, dane o warunkach naturalnych (np. pogodzie)

Źródło: *Wymagania dotyczące bezpieczeństwa danych dla inteligentnych pojazdów połączonych* (智能网联汽车数据安全技术要求), op. cit.

Chińskie przepisy ustanawiają **zasady zarządzania danymi wrażliwymi**:

- a. **przechowywanie w kraju:** dane wrażliwe gromadzone przez inteligentne samochody w ChRL powinny być przechowywane na terytorium kraju. Należy przeprowadzać testy mające na celu weryfikację, czy dane te nie są przekazywane poza granice Chin. Jeśli aktywność biznesowa wymaga przekazania danych wrażliwych wygenerowanych podczas działalności w ChRL za granicę, administrator danych może tego dokonać wyłącznie po uzyskaniu oceny bezpieczeństwa od Państwowej Administracji ds. Cyberprzestrzeni ChRL;
- b. **minimalizowanie ilości zbieranych informacji:** zakres i rozdzielczość kamer, radarów i innych czujników muszą odpowiadać wymaganiom świadczonych usług;

- c. **kontrola dostępu:** wykorzystanie danych wrażliwych wymaga wdrożenia zabezpieczeń uniemożliwiających nieuprawniony dostęp;
- d. **nieodwracalne usuwanie:** po usunięciu dane wrażliwe muszą być nie-
możliwe do odzyskania¹¹;
- e. **możliwość wyłączenia:** „tryb samolotowy” w inteligentnych pojazdach.

Rozwiązaniem proponowanym przez organy standaryzacyjne ChRL jest instalowanie w inteligentnych samochodach trybu zatrzymującego gromadzenie danych z zewnątrz pojazdu (poprzez wyłączenie czujników, kamer samochodowych, radarów itp.), który można uruchomić jednym kliknięciem. Pojazd znajdujący się w tym ustawieniu nie ma możliwości gromadzenia danych dotyczących m.in. dróg, budynków, ukształtowania terenu, tablic rejestracyjnych i uczestników ruchu drogowego. Włączenie trybu zatrzymania gromadzenia danych z otoczenia pojazdu ma być obowiązkowo widoczne na zewnątrz samochodu, m.in. dla służb zarządzających wrażliwymi obszarami¹².

2. Dane osobowe

Inteligentne samochody, wyposażone w **kamery, czujniki podczerwieni, skanery linii papilarnych i mikrofony**, są w stanie rejestrować każdy ruch i głos kierowcy, pasażerów oraz osób znajdujących się w otoczeniu pojazdu. Zgodnie z art. 4 chińskiej Ustawy o ochronie danych osobowych informacje te należą do danych osobowych¹³. W chińskich dokumentach standaryzacyjnych szczególną wagę przywiązuje się do:

- a. **wrażliwych danych osobowych**, czyli informacji o trasach przejazdów, nagrań audio, wideo, zdjęć oraz danych biometrycznych;
- b. **danych pochodzących z kabiny inteligentnych aut**, czyli zebranych wewnątrz samochodu za pomocą kamer, czujników podczerwieni,

¹¹ *Ibidem*; Wymagania dotyczące bezpieczeństwa danych dla inteligentnych pojazdów połączonych (智能网联汽车数据安全技术要求), op. cit.

¹² *Przewodnik po standardowych praktykach w zakresie cyberbezpieczeństwa. Wytyczne standaryzacyjne dotyczące praktyk cyberbezpieczeństwa: blokowanie gromadzenia danych spoza pojazdu jednym kliknięciem* (网络安全标准实践指南 – 一键停止收集车外数据指引), Krajowy Komitet Techniczny 260 ds. Cyberbezpieczeństwa, Chińska Administracja Standaryzacyjna, czerwiec 2024, tc260.org.cn.

¹³ *Ustawa o ochronie danych osobowych Chińskiej Republiki Ludowej* (中华人民共和国个人信息保护法), Państwowa Administracja ds. Cyberprzestrzeni ChRL, 20.08.2021, cac.gov.cn.

skanerów linii papilarnych oraz mikrofonów – mogą one obejmować dane osobowe oraz informacje powstałe w wyniku ich przetwarzania¹⁴.

Dokumenty chińskich organów wskazują, że inteligentne pojazdy mogą ekspansywnie zbierać wrażliwe dane osobowe. Zalicza się do nich:

- a. dane identyfikacyjne: dowód osobisty, prawo jazdy;
- b. dane biometryczne: dane genetyczne, odciski palców, wzór głosu, wzór dłoni, kształt małżowiny usznej, dane o tęczęwce i inne umożliwiające identyfikację lub określenie unikalnych cech osoby fizycznej;
- c. informacje o majątku osobistym: numer konta bankowego, informacje o depozytach (w tym wysokość środków, historia płatności), nieruchomościach, historii i zdolności kredytowej, przepływach pieniężnych, posiadaniu walut wirtualnych;
- d. informacje dotyczące komunikacji osobistej: rejestry i treści komunikacji;
- e. informacje o kontaktach: książka adresowa, lista znajomych, lista grup;
- f. informacje o aktywności online: historia przeglądania stron internetowych;
- g. informacje o lokalizacji użytkownika: ścieżka przemieszczania się, informacje o miejscu pobytu i zakwaterowaniu, współrzędne geograficzne;
- h. inne informacje: dane dźwiękowe, nagrania i zdjęcia osób¹⁵.

Zasady przetwarzania danych osobowych wdrażane w ChRL obejmują:

- a. **przechowywanie na terenie kraju:** podmioty przetwarzające dane zebrane przez samochody mają obowiązek przechowywania danych osobowych gromadzonych przez inteligentne samochody w ChRL na terytorium kraju. W przypadku konieczności przekazania danych za granicę administrator danych powinien zawnieść o ocenę bezpieczeństwa transferu danych do Państwowej Administracji ds. Cyberprzestrzeni ChRL;

¹⁴ Wymagania dotyczące bezpieczeństwa danych dla inteligentnych pojazdów połączonych (智能网联汽车数据安全要求), op. cit.

¹⁵ Ibidem.

- b. **domyślne ograniczenia:** o ile kierowca nie zmieni ustawień, pojazdy nie powinny gromadzić danych osobowych ani przekazywać ich poza pojazd;
- c. **zgoda użytkownika:** przetwarzanie danych osobowych wymaga zgody właściciela lub kierowcy auta. Przed rozpoczęciem zbierania danych przez pojazd użytkownik musi otrzymać zrozumiałe informacje m.in. o rodzaju gromadzonych danych, celu i sposobie przetwarzania, miejscu i okresie przechowywania, a także o danych kontaktowych administratora. Użytkownik ma prawo w dowolnym momencie cofnąć zgodę na przetwarzanie danych. System pojazdu powinien umożliwiać łatwe wycofanie zgody, a producenci są zobowiązani do zapewnienia odpowiednich rozwiązań. W sytuacjach awaryjnych, np. zagrożenia życia i zdrowia, oraz w celu zapewnienia bezpieczeństwa ruchu drogowego dane mogą być przetwarzane bez zgody właściciela/kierowcy;
- d. **anonimizację:** dane wizualne zawierające zdjęcia twarzy i tablic rejestracyjnych muszą zostać zanonimizowane przed przekazaniem ich na zewnątrz pojazdu. Proces anonimizacji podlega rygorystycznym testom: wykrywalność obiektów podlegających anonimizacji (tj. twarzy, tablic rejestracyjnych) musi wynosić co najmniej 90%, a liczba błędnych identyfikacji nie może przekroczyć 10%;
- e. **usuwanie danych:** dane osobowe powinny się kasować po osiągnięciu celu przetwarzania, wycofaniu zgody lub zakończeniu świadczenia usług. Użytkownik ma prawo zażądać usunięcia danych, a podmiot przetwarzający musi tego dokonać w ciągu 10 dni roboczych;
- f. **kontrolę dostępu:** dane muszą być zabezpieczone przed nieautoryzowanym dostępem. Funkcje identyfikacji kierowcy/właściciela w pojeździe nie mogą się opierać wyłącznie na danych biometrycznych¹⁶.

¹⁶ *Postanowienia dotyczące zarządzania bezpieczeństwem danych samochodowych (wersja próbna)* (汽车数据安全管理若干规定 (试行)), op. cit.

III. CYBERBEZPIECZEŃSTWO INTELIGENTNYCH SAMOCHODÓW

Inteligentne samochody dysponują szeregiem kanałów, które narażają je na **potencjalny atak cybernetyczny**. Przykładowo manipulacja sygnałami czujników czy zakłócenia w komunikacji V2X (*vehicle-to-everything*) – umożliwiając pojazdom komunikowanie się z infrastrukturą drogową, innymi pojazdami oraz uczestnikami ruchu – a także przejęcie zdalnej kontroli nad funkcjami pojazdu mogłyby prowadzić do **kolizji, paraliżu infrastruktury transportowej i katastrof w ruchu lądowym**.

Zestaw chińskich regulacji z zakresu cyberbezpieczeństwa ma na celu zabezpieczenie inteligentnych samochodów przed wrogimi działaniami podmiotów trzecich, np. atakami hakerskimi czy ofensywnymi działaniami cybernetycznymi. Przepisy ChRL obejmują m.in.:

- a. **zakaz transferu danych za granicę:** zabrania się bezpośredniego przesyłania danych pojazdu za granicę.
- b. **ochronę infrastruktury krytycznej:** producenci inteligentnych pojazdów podlegają pośrednio regulacjom dotyczącym ochrony infrastruktury krytycznej ChRL. Zabrania się ingerencji w nią, hakowania i uszkodzania. Naruszenia tych regulacji podlegają sankcjom administracyjnym (m.in. karze grzywny, zawieszenia działalności, cofnięcia licencji biznesowej) oraz odpowiedzialności karnej w przypadku poważnych naruszeń.
- c. **ustanowienie systemu cyberbezpieczeństwa pojazdu:** producent musi wdrożyć system cyberbezpieczeństwa obejmujący cały cykl życia pojazdu – od projektowania, poprzez produkcję, aż po eksploatację i wycofanie z użycia. System powinien obejmować identyfikację i ocenę ryzyka, monitorowanie zagrożeń i luk oraz procedury reagowania na incydenty.
- d. **bezpieczeństwo połączeń zewnętrznych:** pojazdy muszą być wolne od niezafatanych luk wysokiego ryzyka w oprogramowaniu. Wszystkie nieużywane porty komunikacyjne powinny pozostawać zamknięte. Z kolei aplikacje zewnętrzne muszą przechodzić proces autoryzacji pod kątem integralności, a instalacja nieautoryzowanych powinna być blokowana lub ograniczana. Ważnym elementem jest też ochrona interfejsów fizycznych, takich jak USB czy porty diagnostyczne, poprzez kontrolę dostępu, zabezpieczenia antywirusowe i uwierzytelnianie przy próbach zmiany

krytycznych parametrów pojazdu. Zdalne sterowanie pojazdem wymaga weryfikacji integralności i autentyczności komend oraz prowadzenia logów bezpieczeństwa.

- e. **kanały komunikacji z chmurą:** komunikacja z chmurą producenta powinna odbywać się przy użyciu bezpiecznych protokołów (np. TLS 1.2), a systemy V2X muszą wykorzystywać certyfikaty do uwierzytelniania i zapewniać ochronę integralności danych. Wewnętrzne sieci pojazdu mają być dzielone na strefy bezpieczeństwa. Oprogramowanie powinno wykrywać i odpierać ataki typu DoS oraz identyfikować i neutralizować złośliwe dane przesyłane w komunikacji V2X czy w wiadomościach.
- f. **bezpieczeństwo aktualizacji oprogramowania:** systemy aktualizacji muszą wspierać bezpieczny rozruch, chronić integralność firmware'u i być wolne od znanych luk wysokiego ryzyka. Zarówno aktualizacje OTA (*over-the-air*), jak i offline muszą być weryfikowane pod względem autentyczności i integralności. Proces aktualizacji powinien być monitorowany i rejestrowany w logach, zwłaszcza w przypadku nieudanych prób.
- g. **ochronę danych i kodów:** producenci są zobowiązani do bezpiecznego przechowywania kluczy kryptograficznych i danych uwierzytelniających, najlepiej w dedykowanych modułach HSM (*hardware security module*). Dane osobowe i inne wrażliwe informacje muszą być zabezpieczone przed nieautoryzowanym dostępem dzięki szyfrowaniu i mechanizmom kontroli dostępu. Szczególną ochroną są objęte krytyczne parametry pojazdu, takie jak konfiguracja systemów hamulcowych czy progów aktywacji poduszek powietrznych, które nie mogą być modyfikowane ani usuwane bez autoryzacji. Pojazdy powinny posiadać funkcję bezpiecznego usuwania danych osobowych oraz mechanizmy uniemożliwiające ich odzyskanie (ma to szczególne znaczenie w przypadku odsprzedaży czy złomowania pojazdu)¹⁷.

¹⁷ Wymagania dotyczące bezpieczeństwa danych dla inteligentnych pojazdów połączonych (智能网联汽车数据安全要求), op. cit.

IV. IMPLIKACJE DLA EUROPY I REKOMENDACJE DZIAŁAŃ

Dotychczas ChRL podchodziła do kwestii inteligentnych samochodów defensywnie, budując liczne narzędzia regulacyjne mające chronić ją przed zagrożeniami w zakresie nieautoryzowanego gromadzenia danych czy cyberbezpieczeństwa pojazdów. **W przyszłości Chiny mogą jednak podjąć działania ofensywne.** Wskazują na to niezwykle zaawansowane zdolności ofensywne ChRL w cyberprzestrzeni, rozwinięty ekosystem wywiadowczy oraz niektóre dokumenty strategiczne (np. zalecenie państwowe w sprawie łączenia technologii cywilnych i wojskowych w rozwoju inteligentnych samochodów). Logika i poziom rozbudowania wewnętrznych regulacji dotyczących inteligentnych samochodów, jak również chińskie oceny ryzyk dla cyberbezpieczeństwa wskazują wyraźnie na jednoznaczne postrzeganie tej technologii przez pryzmat bezpieczeństwa.

Na mocy art. 7 Ustawy o wywiadzie narodowym ChRL, a także w ramach nieformalnych mechanizmów, **istnieje możliwość zobowiązania chińskich producentów samochodów do przekazania rządowi chińskiemu danych zgromadzonych za granicą**¹⁸. W konsekwencji dane zbierane w Europie przez inteligentne pojazdy z Chin potencjalnie mogą być wykorzystywane do celów wywiadowczych, np. śledzenia osób, przepływu towarów i badania wzorców ruchu oraz do szkolenia sztucznej inteligencji, również w wymiarze wojskowym. Doniesienia medialne wskazują, że w przeszłości ChRL używała samochodów w celach szpiegowskich: w 2023 r. w pojazdach należących do brytyjskiego rządu miano wykryć chińskie urządzenia śledzące¹⁹. Rodzi to potrzebę szczególnie wnikliwych działań sprawdzających inteligentne auta pod kątem np. wykorzystywania ich do skanowania infrastruktury krytycznej przez liczne sensory oraz zbierania informacji wrażliwych.

Ma to szczególne znaczenie dla wschodniej flanki NATO w związku z **pogłębiającymi się relacjami Chiny-Rosja** i ryzykiem ewentualnego przekazywania Federacji Rosyjskiej danych zgromadzonych przez chińskie inteligentne samochody poruszające się po europejskich drogach. Należy mieć jednak na uwadze, że **inteligentne samochody, niezależnie od kraju pochodzenia producenta, są też podatne na cyberataki i wykorzystanie ich sensorów do celów wywiadowczych, a ze względu na możliwości zdalnego**

¹⁸ Ustawa o wywiadzie krajowym (中华人民共和国国家情报法), Ogólnochińskie Zgromadzenie Przedstawicieli Ludowych, 12.06.2018, npc.gov.cn, wersja anglojęzyczna: [PRC National Intelligence Law \(as amended in 2018\)](#), China Law Translate, 27.06.2017, china-law-translate.com.

¹⁹ M. Ross, *Chinese tracking device is 'discovered inside UK government car', as senior politician slams Beijing as a 'systematic' threat to Britain's security*, Daily Mail, 6.01.2023, dailymail.co.uk.

sterowania – również do aktów dywersji. Oprócz refleksji dotyczące potencjalnych cyberzagrożeń specyficznych dla kierunku chińskiego myślenie o regulacjach tego typu pojazdów w Polsce i Europie powinno uwzględniać narzucenie wyższych standardów cyberbezpieczeństwa dla wszystkich uczestników rynku.

1. Wnioski dla Europy płynące z chińskich regulacji

Rozwiązania chińskie mogą stanowić punkt wyjścia do zrozumienia ryzyk związanych z inteligentnymi samochodami, a pośrednio także tworzenia środowiska regulacyjnego dla ich ograniczania. Regulatorzy chińscy podkreślają, że inteligentne pojazdy mogą gromadzić i przekazywać za granicę dane geoprzestrzenne o obszarach wrażliwych, np. infrastrukturze krytycznej, co może prowadzić do ujawnienia tajemnic państwowych. Oprócz samej klasyfikacji ryzyk chińskie dokumenty dają też wzorce sposobów certyfikacji zagranicznych producentów oraz diagnozowania i sprawdzania, jakie dane są przesyłane za granicę. Sugerują również konkretne rozwiązania techniczne (np. tryb wyłączający zbieranie danych z otoczenia pojazdu) ułatwiające identyfikację przez służby państwowe, kiedy samochód gromadzi dane. Rozwiązania chińskie stanowią nie tylko istotny zbiór dobrych praktyk – wzorowanie się na nich dałoby UE istotny argument w komunikowaniu władzom ChRL ewentualnej decyzji o wprowadzeniu ściślejszych regulacji wobec chińskich inteligentnych samochodów.

Działania Pekinu wobec zagranicznych producentów, takich jak Tesla, pokazują, że Chiny stosują wyjątkowo ostrożne i restrykcyjne podejście do podmiotów spoza kraju. Obejmuje ono zarówno państwową certyfikację inteligentnych pojazdów pod kątem bezpieczeństwa danych, jak i obowiązek lokalnego przechowywania informacji gromadzonych przez auta na terytorium Chin. W praktyce spełnienie tych wymogów staje się kluczowym warunkiem sprawnego funkcjonowania na rynku chińskim. Proces certyfikacji wprowadzony w ChRL może posłużyć jako istotny wzór dla UE do podwyższenia poziomu cyberbezpieczeństwa pojazdów, zwiększenia suwerenności cyfrowej (np. poprzez wprowadzenie wymogu lokalnego przechowywania danych), a także wspierania zaufanych dostawców usług pochodzących z Unii Europejskiej w takich branżach jak IT, przetwarzanie danych, AI i jazda autonomiczna.

Konieczność nadania ram regulacyjnych funkcjonowaniu inteligentnych samochodów w Europie staje się kwestią palącą ze względu na skokowy przyrost pojazdów z Chin na rynku UE. Europa pozostaje jednym

z najatrakcyjniejszych rynków dla chińskich producentów samochodów – wielkość ich importu oraz lokalnej produkcji w Europie będzie się znacząco zwiększać w najbliższych latach. Nawet po wprowadzeniu ceł antysubsydyjnych na chińskie pojazdy elektryczne (BEV) ich poziom (17–35,3% plus 10% wspólnej taryfy celnej) jest relatywnie niski na tle polityki handlowej innych państw, np. USA i Kanady, gdzie stawki celne wynoszą 100%²⁰. Jednocześnie część chińskich producentów ogranicza wpływ unijnych ceł, zwiększając eksport pojazdów hybrydowych typu PHEV oraz modeli spalinowych, które nie są w UE objęte dodatkowymi obciążeniami²¹. Co istotne, rozbudowaną warstwę cyfrową mają obecnie nie tylko samochody elektryczne, lecz także pojazdy o wszystkich rodzajach napędów. Należy się spodziewać, że wraz ze wzrostem liczby inteligentnych samochodów z Chin opór konsumentów przed nowymi regulacjami – a tym samym koszt polityczny – będzie coraz wyższy.

2. Stan obecny i rekomendowane kierunki działania UE

Rosnąca liczba państw na świecie podejmuje działania mające ograniczyć ryzyka dla bezpieczeństwa państwa związane z inteligentnymi samochodami z Chin. Prym wiodą Stany Zjednoczone – w 2024 r., powołując się na klauzulę bezpieczeństwa narodowego, przyjęły przepisy przewidujące stopniowy zakaz stosowania chińskiego i rosyjskiego oprogramowania oraz sprzętu łączności w nowych samochodach. Będą one stopniowo wdrażane dla pojazdów z roku modelowego 2027 i nowszych²². W Wielkiej Brytanii niektóre instytucje obronne stosują zaostrzone wymogi dla poruszania się aut elektrycznych w pobliżu wybranych obiektów²³. Brytyjskie media informują również, że tamtejsze Ministerstwo Obrony ostrzega pracowników przed prowadzeniem rozmów w samochodach na tematy wrażliwe z powodu obaw o szpiegostwo ze strony Chin²⁴. Doniesienia medialne wskazują, że Izrael zabronił wjazdu chińskich aut do baz wojskowych i wycofał chińskie pojazdy używane przez

²⁰ *President Biden Takes Action to Protect American Workers and Businesses from China's Unfair Trade Practices*, Biały Dom, 14.05.2024, [bidenwhitehouse.archives.gov](https://www.bidenwhitehouse.archives.gov); *Surtax on Chinese-made Electric Vehicles*, Departament Finansów Kanady, 26.08.2024, [canada.ca](https://www.canada.ca).

²¹ Z. Yan, Q. Li, B. Goh, *China automakers pivot to hybrids for Europe to counter EV tariffs*, Reuters, 5.12.2024, [reuters.com](https://www.reuters.com).

²² *Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats*, Departament Handlu Stanów Zjednoczonych, 14.01.2025, [bis.gov](https://www.bis.gov).

²³ *China: Electric Vehicles. Question for Ministry of Defence*, Parlament Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej, 6.03.2025, questions-statements.parliament.uk.

²⁴ T. Cotterill, *MoD tells staff not to discuss secrets in cars amid China spying fears*, The Telegraph, 18.11.2025, [telegraph.co.uk](https://www.telegraph.co.uk).

wyższych rangą wojskowych²⁵. Krajowy Urząd ds. Bezpieczeństwa Cybernetycznego i Informacyjnego Republiki Czeskiej (NÚKIB) wydał ostrzeżenie, w którym kwalifikuje zagrożenia związane z transferem danych systemowych i użytkowników oraz zdalną administracją zasobów technicznych z terytorium ChRL jako wysokie. Przytoczone przykłady ryzykownych produktów i usług, które mogą przekazywać dane do ChRL, obejmują inteligentne pojazdy.

Coraz więcej państw wdraża działania ograniczające ryzyka związane z inteligentnymi samochodami z Chin:



USA

- 100% cła na samochody elektryczne z Chin,
- zakaz chińskiego i rosyjskiego oprogramowania oraz sprzętu łączności w inteligentnych samochodach od roku modelowego 2027.



Kanada

- 100% cła na samochody elektryczne z Chin.



Unia Europejska

- 17-35% cła (+10% wspólnej taryfy UE) na samochody elektryczne z Chin.



Wielka Brytania

- zaostrzone wymogi dotyczące poruszania się pojazdów elektrycznych w pobliżu wybranych obiektów obronnych,
- ostrzeżenia Ministerstwa Obrony przed prowadzeniem przez pracowników wrażliwych rozmów oraz ładowaniem telefonów w chińskich pojazdach.



Izrael

- zakaz wjazdu chińskich samochodów do baz wojskowych,
- wycofanie chińskich pojazdów używanych przez wyższych rangą wojskowych.



Czechy

- ostrzeżenie Urzędu ds. Bezpieczeństwa Cybernetycznego i Informacyjnego kwalifikujące samochody z Chin jako produkty wysokiego ryzyka dla cyberbezpieczeństwa.

Obecnie nie istnieją kompleksowe przepisy unijne, które regulowałyby funkcjonowanie inteligentnych aut. Europejskie działania rozwijają się dotychczas następująco:

- a. Komisja Europejska prowadzi ocenę ryzyka cyberbezpieczeństwa inteligentnych pojazdów w ramach dyrektywy NIS 2²⁶. Na podstawie oceny podejmie decyzję o działaniach regulacyjnych lub przedstawieniu

²⁵ H. Sugars, *IDF recalls 700 Chinese EVs used by senior officers over security concerns*, The Jewish Chronicle, 4.11.2025, thejc.com.

²⁶ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), „Dziennik Urzędowy Unii Europejskiej”, 27.12.2022, eur-lex.europa.eu.

państwom członkowskim rekomendacji. Kwestia inteligentnych samochodów może również zostać uwzględniona w trwającym **przeglądzie unijnego aktu o cyberbezpieczeństwie**²⁷ z 2019 r.

- b. Akt w sprawie danych wskazuje pojazdy jako jedną z kluczowych kategorii produktów skomunikowanych oraz reguluje zarówno dostęp administracji rządowych państw trzecich do danych, jak i zasady ich międzynarodowego przekazywania. Artykuł 32 dokumentu ustanawia zakaz przekazywania takich danych lub udostępniania ich organom zagranicznym, jeżeli stoi to w sprzeczności z prawem UE lub państw członkowskich (z wyjątkiem zawarcia stosownych umów międzynarodowych).
- c. Przepisy UE dotyczące homologacji typu pojazdów silnikowych²⁸ nakładają na producentów inteligentnych samochodów obowiązek przestrzegania wymogów dotyczących konstrukcji pojazdu i organizacyjnych środków cyberbezpieczeństwa. Wymogi regulacyjne uzupełniane są rekomendacjami, np. Agencja UE ds. Cyberbezpieczeństwa (ENISA) opracowała rekomendacje dotyczące bezpieczeństwa połączonej i zautomatyzowanej mobilności²⁹, stanowiące punkt odniesienia dla projektowania i wdrażania rozwiązań w zakresie cyberbezpieczeństwa pojazdów.
- d. Producenci inteligentnych samochodów wprowadzający auta na rynek UE są zobowiązani do przestrzegania regulaminów ONZ: o homologacji pojazdów w zakresie cyberbezpieczeństwa i systemu zarządzania cyberbezpieczeństwem (nr 155)³⁰, o aktualizacji oprogramowania i systemu zarządzania aktualizacjami oprogramowania (nr 156)³¹ oraz o automatycznym systemie utrzymania pasa ruchu (nr 157)³². W zakresie, w jakim czujniki pojazdów gromadzą dane osobowe użytkowników, zastosowanie ma też

²⁷ *Komisja rozpoczyna konsultacje w sprawie przeglądu unijnego aktu o cyberbezpieczeństwie*, Komisja Europejska, 11.04.2025, digital-strategy.ec.europa.eu.

²⁸ *Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019*, „Official Journal of the European Union”, 16.12.2019, eur-lex.europa.eu.

²⁹ *How to Secure the Connected & Automated Mobility (CAM) Ecosystem*, European Union Agency for Cybersecurity, 5.05.2021, enisa.europa.eu.

³⁰ *Regulamin ONZ nr 155 – Jednolite przepisy dotyczące homologacji pojazdów w zakresie cyberbezpieczeństwa i systemu zarządzania bezpieczeństwem [2021/387]*, „Dziennik Urzędowy Unii Europejskiej”, 9.03.2021, eur-lex.europa.eu.

³¹ *Regulamin ONZ nr 156 – Jednolite przepisy dotyczące homologacji pojazdów w zakresie aktualizacji oprogramowania i systemu zarządzania aktualizacjami oprogramowania [2021/388]*, „Dziennik Urzędowy Unii Europejskiej”, 9.03.2021, eur-lex.europa.eu.

³² *Regulamin ONZ nr 157 – Jednolite przepisy dotyczące homologacji pojazdów w zakresie automatycznego systemu utrzymania pasa ruchu [2021/389]*, „Dziennik Urzędowy Unii Europejskiej”, 9.03.2021, eur-lex.europa.eu.

Ogólne rozporządzenie o ochronie danych (RODO)³³, zaś dyrektywa NIS 2³⁴ o zabezpieczaniu sieci i systemów informatycznych kwalifikuje operatorów inteligentnych systemów transportowych jako sektor wysoce krytyczny i nakłada na nich obowiązki m.in. zarządzania ryzykiem, odpowiedzialności zarządu za kwestie cyberbezpieczeństwa, gotowości operacyjnej i współpracy w całym łańcuchu dostaw.

- e. Kwestie bezpieczeństwa związane z chińskimi pojazdami są podnoszone przez europosłów³⁵. Powołują się oni m.in. na doświadczenia rządu Wielkiej Brytanii i ustalenia estońskiego wywiadu. Doniesienia medialne wskazują, że brytyjscy ministrowie mieli przestrzegać, że Chiny mogą wykorzystywać auta elektryczne do celów szpiegowskich³⁶. Estońska Służba Wywiadu Zagranicznego (Välisluureamet, VLA) w raporcie z 2024 r. ostrzega zaś przed transferem do ChRL danych z chińskich samochodów elektrycznych obecnych w Europie oraz zwiększonym zagrożeniem cyberatakami³⁷.

W dotychczasowych regulacjach unijnych i poszczególnych państw członkowskich brakuje szczegółowych norm technicznych oraz obowiązkowych audytów, które zapewniałyby systematyczną i praktyczną weryfikację poziomu cyberbezpieczeństwa oraz ochrony danych gromadzonych przez inteligentne pojazdy. W efekcie większość państw nie ma nawet narzędzi pozwalających na regularne sprawdzanie, na ile ryzyka omawiane w niniejszym raporcie – w tym te wskazywane wprost w chińskich dokumentach – materializują się na terenie UE. Z uwagi na fundamentalną naturę zagrożeń, które niosą ze sobą inteligentne auta, wprowadzenie tych instrumentów jest niezbędne z punktu widzenia cyberbezpieczeństwa, ochrony danych osobowych, a także – szerzej – suwerenności cyfrowej UE.

³³ 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), „Dziennik Urzędowy Unii Europejskiej”, 4.05.2016, eur-lex.europa.eu.

³⁴ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), op. cit.

³⁵ B. Groothuis, C. Nagtegaal, *Security concerns around Chinese electric vehicles*, Parlament Europejski, 26.09.2023; K. Złotowski, *Cybersecurity risks posed by Chinese technology*, Parlament Europejski, 20.02.2024, europarl.europa.eu.

³⁶ W. Hazell, D. Penna, *China 'will use electric cars to spy on Britain'*, The Telegraph, 5.08.2023, telegraph.co.uk.

³⁷ *The Advance of Chinese technology*, Służba Wywiadu Zagranicznego Estonii, raport.valisluureamet.ee.

Optymalnym rozwiązaniem wydaje się opracowanie unijnych przepisów nakładających na producentów samochodów, ze szczególnym uwzględnieniem podmiotów z państw trzecich lub niesojusznicych, obowiązek uzyskania dodatkowej certyfikacji bezpieczeństwa. Mechanizm ten nie tylko pozwoliłby zwiększyć poziom bezpieczeństwa na rynku wewnętrznym, lecz także sprzyjałby pozyskiwaniu know-how technologicznego oraz lokowaniu większej wartości dodanej w Europie. W ten sposób UE mogłaby przeciwdziałać coraz wyraźniejszemu trendowi redukowania jej roli do rynku zbytu lub montowni dla produktów pochodzących z Chin.

Jeśli jednak ustanowienie wspólnych ram regulacyjnych okazałoby się niemożliwe – np. z powodu sprzeciwu części państw członkowskich lub dominujących w UE tendencji deregulacyjnych – należy rozważyć utworzenie koalicji państw gotowych do ich wdrażania. Powinno temu towarzyszyć wypracowanie jednolitego zestawu standardów regulacji na szczeblu UE, np. w postaci sugerowanego przez Komisję Europejską pakietu rozwiązań pozwalającego zainteresowanym państwom na przyjęcie ujednoliconych przepisów. Umożliwiłoby to ograniczenie poziomu fragmentacji rynku unijnego, a jednocześnie podnoszenie standardów bezpieczeństwa i odporności technologicznej w zainteresowanych gospodarkach.