



Perbandingan Kesiapan Regulasi Keamanan Siber Pada Penyelenggaraan Kendaraan Listrik di Indonesia

Najmi Ariansyah Ijlal Gusti^{1*}, Benedict Matthew¹

¹ Universitas Airlangga, Indonesia

*Corresponding author email: nai.gusti@gmail.com, benedict251@gmail.com

Article Info

Article history:

Received April 23, 2026

Approved August 15, 2026

Keywords:

Electric Vehicles, Lack of Regulation, CyberSecurity

ABSTRACT

The lack of regulations regarding EVs in Indonesia has prompted the government to consider implementing appropriate regulatory frameworks to encourage the use of EVs in Indonesia, specifically about cybersecurity of EVs. The lack of regulation about cybersecurity can pose significant threats to both drivers and passengers, expose sensitive information, and leading to potentially devastating consequences. The aim of this research is to create regulations that can support and maximize the positive potential of EVs while minimize the negative impacts that can occur with the existence of EVs. The research method in this writing is normative juridical methodology, utilizing 2 (two) approaches, namely the statutory and conceptual approaches to identify and analyze relevant legal frameworks. The results show that regulations regarding EVs are still lacking compared to other states, especially regarding EVs cybersecurity. The government must be able to emulate other countries in regulating the regulation of cybersecurity in Indonesia. Where there are already several countries that have suffered losses from cybercrime and already regulated cybersecurity on EVs. To deal with the potential of EV software and cybersecurity threats, the government can carry out repressive efforts, because repressive efforts have a greater impact in reducing the number of accidents that occur. Efforts that the government can make are by providing SOPs for EV business actors and improving cybersecurity for EV business actors.

ABSTRAK

Kurangnya regulasi terkait kendaraan listrik (EV) di Indonesia telah mendorong pemerintah untuk mempertimbangkan penerapan kerangka regulasi yang tepat guna mendorong penggunaan EV di Indonesia, khususnya mengenai keamanan siber EV. Kurangnya regulasi terkait keamanan siber dapat menimbulkan ancaman signifikan bagi pengemudi dan penumpang, mengekspos informasi sensitif, dan berpotensi menyebabkan konsekuensi yang sangat merugikan. Tujuan penelitian ini adalah untuk menciptakan regulasi yang dapat mendukung dan memaksimalkan potensi positif EV sekaligus meminimalkan dampak negatif yang dapat terjadi dengan keberadaan EV. Metode penelitian dalam tulisan ini adalah metodologi yuridis normatif, menggunakan 2 (dua) pendekatan, yaitu pendekatan statutori dan konseptual untuk mengidentifikasi dan menganalisis kerangka hukum yang relevan. Hasil penelitian menunjukkan bahwa regulasi terkait EV masih kurang dibandingkan dengan negara lain, terutama terkait keamanan siber EV. Pemerintah harus mampu meniru negara lain dalam mengatur regulasi keamanan siber di Indonesia. Padahal sudah ada beberapa negara yang telah mengalami kerugian akibat kejahatan siber dan telah mengatur keamanan siber pada EV. Untuk mengatasi potensi ancaman perangkat lunak dan keamanan siber pada kendaraan listrik (EV), pemerintah dapat melakukan upaya represif, karena upaya represif memiliki dampak yang lebih besar dalam mengurangi jumlah kecelakaan yang terjadi. Upaya yang dapat dilakukan pemerintah adalah dengan menyediakan SOP (Prosedur Operasi Standar) bagi pelaku bisnis EV dan meningkatkan keamanan siber bagi pelaku bisnis EV.

Copyright © 2026, The Author(s).
This is an open access article under the CC-BY-SA license



How to cite: Gusti, N. A. I., & Matthew, B. (2026). Perbandingan Kesiapan Regulasi Keamanan Siber Pada Penyelenggaraan Kendaraan Listrik di Indonesia. *Jurnal Ilmiah Global Education*, 7(3), 2704–2717. <https://doi.org/10.55681/jige.v7i3.6187>

PENDAHULUAN

Indonesia merupakan negara yang tergolong baru mengenal kendaraan listrik atau electric vehicles (selanjutnya disebut EV) dibanding negara-negara lain. EV pertama dikenalkan di negara California pada tahun 1970 karena adanya krisis minyak di sana (Tulus & Sidabutar, 2020). Meskipun Indonesia sebagai negara yang tergolong baru menggunakan EV, Indonesia tidak boleh acuh dan harus segera membuat pengaturan terkait EV. Hal ini dikarenakan semakin berkembangnya zaman, peperangan tidak lagi terjadi secara fisik, melainkan juga di ranah teknologi (Anwar, 2018). Belajar dari negara lain, Indonesia dapat mengembangkan industri EV dengan efektif dan efisien agar pengaturan hukum yang ada dapat mendukung penggunaan EV sehingga akan mempercepat transisi dari mobil konvensional ke EV. Hal ini dikarenakan masyarakat sudah mulai beralih dari kendaraan berbahan minyak menjadi EV. Dimana kenaikan ini dapat dilihat dari perkembangan penjualan EV dari tahun 2020 hingga 2022. Pada tahun 2020 pertama kali masyarakat dikenalkan dengan EV.

Pada tahun 2021 penjualan kendaraan EV telah mencapai sekitar 3.192 unit, pada tahun 2022 penjualan mobil listrik mengalami kenaikan hingga 382,62% (Ardiyanti et al., 2023). Angka ini menunjukkan adanya peningkatan penggunaan kendaraan EV di Indonesia, hal ini juga didorong dengan pemerintah yang melakukan insentif-insentif bagi pengguna EV. Kejahatan siber merupakan salah satu poin penting yang perlu diperhatikan pemerintah dalam penggunaan EV. Kejahatan siber adalah tindakan kriminal yang dilakukan dengan menggunakan perangkat elektronik dan koneksi internet (Maskun, 2022). Negara-negara lain yang telah menggunakan EV jauh sebelum Indonesia, telah menemukan beberapa celah baru yang dapat menciptakan model kejahatan baru. Adapun pengaturan di Indonesia terkait keamanan siber pada EV masih cenderung umum, yang artinya masih banyak menggunakan hukum yang sudah ada sebelum eksistensi EV di Indonesia muncul seperti Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disebut UU PDP) dan Undang-Undang Nomor 22 Tahun 2009 tentang Lalu Lintas dan Angkutan Jalan (selanjutnya disebut UU LLAJ). Hal ini menyebabkan terbukanya celah bagi pihak-pihak yang tidak bertanggung jawab untuk mengganggu keamanan siber pada mobil EV di Indonesia.

Pengaturan yang secara khusus dibentuk pemerintah Indonesia dalam pelaksanaan kendaraan listrik antara lain adalah Peraturan Presiden Republik No 55 Tahun 2019 tentang Percepatan Program Kendaraan Bermotor Listrik (selanjutnya disebut PP No. 55 Tahun 2019), yang kemudian diubah dengan Peraturan Presiden Republik Indonesia No. 79 Tahun 2023 tentang Perubahan atas PP 55 Tahun 2019 tentang Percepatan Program Kendaraan Bermotor Listrik Berbasis Baterai (Battery Electric Vehicle) Untuk Transportasi Jalan (selanjutnya disebut PP No. 79 Tahun 2023). Peraturan ini dibentuk sebagai urgensi untuk mempercepat peningkatan penggunaan EV, namun belum secara khusus dapat mengatasi ancaman kejahatan siber dari penggunaan EV.

Keamanan siber menjadi perhatian penting bagi pengguna EV. Semakin canggih mobil EV akan menciptakan teknologi yang terintegrasi. Hal ini dapat membuat teknologi tersebut rentan untuk terkena serangan dan malfungsi siber (Sjafrie, 2019). Hal yang perlu diwaspadai bagi pengguna EV adalah kerentanan pada titik pengisian daya, keamanan dan malfungsi perangkat lunak EV. Stasiun pengisian daya yang terhubung ke internet untuk berbagai keperluan seperti monitoring fungsi atau transaksi pembayaran. Celah tersebut yang bisa

dimanfaatkan peretas untuk masuk ke sistem. Selain itu, mobil listrik yang bergantung pada software atau perangkat lunak dalam menjalankan fungsinya dapat menimbulkan kelemahan keamanan siber yang perlu diwaspadai. EV yang dipenuhi dengan perangkat lunak yang digunakan untuk mengendalikan berbagai hal dari manajemen baterai hingga fitur bantuan pengemudi dapat menciptakan potensi terkena serangan lebih luas oleh pihak peretas dibandingkan dengan kendaraan yang menggunakan bahan bakar tradisional. Sebagai contoh yaitu ada korban jiwa akibat mobil autonomous drive terdapat kesalahan sistem pada desain dan perpindahan gigi Tesla yang membingungkan menyebabkan mobil Angela Chou (selanjutnya disebut AC) menabrak pagar pembatas dan terjun ke danau sedalam 25 meter (Rohman, 2024). Hal ini menunjukkan bahwa semakin banyak titik kontrol pada autonomous drive yang dikendalikan perangkat lunak, semakin banyak pula potensi celah keamanan yang bisa dimanfaatkan (Fariza Ramadhani, 2023). Potensi yang dapat terjadi pada saat peretas mengeksploitasi perangkat lunak antara lain adalah menonaktifkan fitur keselamatan, mengganggu pengisian daya, dan pelanggaran data. Hal-hal tersebut tentu dapat membahayakan pengemudi dan penumpang, bocornya data pengemudi dan penumpang, bahkan bisa mengakibatkan kecelakaan.

Atas potensi serangan siber yang dapat menimpa pengguna EV, tentu mendorong pemerintah Indonesia untuk mengambil tindakan tegas untuk melindungi para pengguna EV. Keamanan siber memainkan peranan penting untuk melindungi para pengguna EV tersebut. Indonesia tidak boleh tinggal diam dan harus segera membuat peraturan terkait EV, karena sektor EV akan semakin bertumbuh pesat melihat banyaknya manfaat yang didapat dari penggunaan EV. Ramah lingkungan, biaya yang lebih rendah, pembayaran pajak yang lebih kecil dibanding kendaraan konvensional tentu menarik masyarakat untuk membeli EV (Cakrawati Sudjoko, n.d.). Oleh karena itu, menuju masa depan transportasi yang berkelanjutan dan ramah lingkungan pemerintah harus dapat mengikuti perkembangan zaman dengan mengatasi permasalahan-permasalahan kejahatan siber yang dapat menimpa para pengguna EV. Dari permasalahan yang ada, rumusan masalah yang dapat digunakan untuk mengatasi permasalahan tersebut adalah apa regulasi yang perlu dibentuk pemerintah dalam mengatasi kejahatan siber dari penggunaan EV apabila disandingkan dengan negara lain yang lebih siap menghadapi serangan siber tersebut. Dari rumusan masalah tersebut akan menjawab mengenai peran yang dapat dilakukan pemerintah untuk mengatasi potensi serangan siber yang dapat terjadi dari penggunaan EV.

METODE

Metode yang digunakan untuk menjawab permasalahan penulisan ini adalah metode penulisan yuridis normatif. Adapun pendekatan yang digunakan adalah pendekatan perundang-undangan dan pendekatan konseptual untuk mengidentifikasi dan menganalisis kerangka hukum yang relevan. Pendekatan perundang-undangan akan berfokus pada studi dan analisis terhadap peraturan perundang-undangan yang relevan dengan permasalahan hukum yang dibahas, sedangkan pendekatan konseptual adalah pendekatan yang menggunakan konsep-konsep hukum yang ada dalam doktrin dan teori hukum untuk memahami dan menganalisis permasalahan hukum. Pendekatan konseptual akan mengkaji pendapat ahli hukum, teori-teori hukum yang relevan, dan prinsip-prinsip hukum umum untuk memperkuat analisisnya.

HASIL DAN PEMBAHASAN

1. Potensi Kerentanan Pengisian Daya EV serta Pengaturan Hukum Indonesia

Perkembangan teknologi telah membawa dampak baik bagi kehidupan manusia, dimana teknologi ini mempermudah kehidupan manusia. Salah satu contohnya yaitu adanya kendaraan, kendaraan ini memudahkan manusia untuk pergi dari satu tempat ke tempat lain atau memindahkan barang dari satu tempat ke tujuannya. Dengan berkembangnya jaman saat ini kendaraan sudah ada yang menggunakan tenaga baterai, yaitu kendaraan elektrik atau Electric Vehicle atau EV. EV merupakan kendaraan yang dijalankan dengan tenaga listrik dan diisi dengan baterai, baterai ini berfungsi sebagai sumber dari arus listrik dari EV tersebut (Cakrawati Sudjoko, 2021). Namun, berkembangnya teknologi, tidak luput juga dengan berkembangnya jenis kejahatan. Saat ini kejahatan sudah bukan lagi dapat dirasakan secara fisik, namun saat ini kejahatan dapat berupa kejahatan siber yang menyerang perangkat-perangkat teknologi manusia. Kejahatan siber ini dapat terjadi tidak hanya dalam satu negara tetapi dapat lintas negara dan dapat dilakukan oleh siapa saja individu, organisasi, maupun teroris (Rahmawati, n.d.).

Kejahatan siber saat ini sedang menjadi perhatian pemerintah, hal ini karena meningkatnya kejahatan siber seperti hacking yang terjadi pada media sosial. Menurut Badan Siber dan Sandi Negara (BSSN) telah tercatat sebanyak 8.414.296 kasus serangan siber yang terjadi di Indonesia dalam rentang waktu kurang dari setengah tahun (Kajian Strategik Ketahanan Nasional, 2021). Kejahatan siber ini dapat menargetkan siapa saja, tidak memandang umur dan latar belakang orang tersebut. Oleh karena itu, pentingnya ada perlindungan dalam dunia siber. Hal ini mengingat saat ini internet merupakan salah satu kebutuhan pokok manusia. Saat ini internet dapat digunakan untuk mengontrol rumah yang disebut smart house, selain itu internet juga dapat digunakan untuk mengontrol mobil yaitu smart car.

Smart car ini merupakan salah satu bentuk dari EV, dimana smart car ini berpusat dengan satu perangkat. Keunggulan dari smart car ini adalah kemudahan yang diberikan, yaitu adanya kontrol menggunakan suara (Kusumah et al., n.d.). Selain untuk pengontrolan, ada pula autodrive yang memungkinkan mobil melaju dengan otomatis tanpa pengemudi mengemudi (Nazmul Hasan et al., 2011). Masih banyak lagi keunggulan dari smart car, namun dengan smart car yang bertumpu pada satu perangkat hal ini menimbulkan peluang untuk melakukan kejahatan siber. Dimana sama halnya dengan smartphone yang dimiliki oleh masyarakat, yang dapat dengan mudah diretas oleh hacker dari jarak yang jauh bahkan lintas negara. Peningkatan ini dapat menciptakan ancaman untuk privasi bahkan keselamatan pengguna kendaraan (Muhammad et al., 2023a). Dimana peretas dapat memanfaatkan kerentanan perangkat dalam EV untuk mengendalikan EV. Peretas dapat mengakses bahkan memanipulasi informasi, data lokasi, kinerja kendaraan, dan mengidentifikasi pengguna EV (Muhammad et al., 2023a). Menurut laporan dari Global Automotive Cybersecurity Report, terdapat peningkatan sebesar 380% dari ancaman terhadap Application Programming Interface pada tahun 2022, dimana ini hanya 12% dari keseluruhan insiden yang terjadi (Nugroho, 2023).

Terdapat celah-celah yang dapat dimanfaatkan oleh peretas untuk meretas EV. Peretasan dapat meluncurkan aksinya melalui cela dari Tire Pressure Monitoring System (TPMS), TPMS merupakan alat untuk mengukur dan memonitor kondisi dari tekanan ban (Acharya et al., 2020). Tekanan pada ban merupakan hal yang penting untuk diperhatikan karena ban menjadi salah satu penggerak kendaraan. Dimana dengan tekanan ban yang rendah dapat membuat ban menjadi rusak bahkan dapat berdampak pada keselamatan penumpang. Saat ini tekanan ban dapat diketahui secara otomatis, dimana TPMS ini akan memberikan informasi mengenai

tekanan ban dan akan memberikan tekanan secara otomatis bila sensor menyatakan ada kekurangan tekanan pada ban (Silalahi et al., 2019). Namun, perangkat TPMS ini dapat dengan mudah diretas karena tekanan ban ini tidak memiliki perlindungan yang ketat seperti perangkat-perangkat yang lain. Sensor tekanan ini tidak ada pengidentifikasian maupun penyaringan keotentikan. Sehingga sangat mudah bagi peretas untuk meretas menggunakan perangkat TPMS ini. Peretas dapat melakukan serangan secara remote dari jarak jauh (Acharya et al., 2020). Akibat dari peretasan pada TPMS dapat merusak tekanan pada ban, dimana tekanan ban ini memiliki pengaruh terhadap stabilitas, dan keseimbangan mobil. Hal ini dikarenakan TPMS memiliki hubungan dengan perangkat lunak pada EV sehingga, bila TPMS ini diretas maka perangkat lunak pada EV juga dapat berdampak (Heary, 2010).

Selanjutnya peretas dapat menggunakan celah pada charging station, hal ini karena tempat cas EV memiliki kemampuan untuk mengisi EV lebih cepat dan mudah diakses oleh pengguna EV. Hal ini sama halnya dengan pom bensin yang menjadi sarana seseorang untuk mengisi bahan bakar. Charging station juga merupakan salah satu fasilitas yang diberikan oleh pemerintah untuk meningkatkan penggunaan EV. Pengguna EV akan memilih untuk mengisi baterai EV di tempat-tempat yang telah disediakan oleh pemerintah daripada harus menambah biaya listrik di rumah pribadinya. Oleh karena itu, keberadaan dari charging station sangat dibutuhkan untuk meningkatkan penggunaan EV. Tempat stasiun pengisian EV di Indonesia disebut sebagai Stasiun Pengisian Kendaraan Listrik Umum (SPKLU) yang diatur dengan Peraturan Presiden No 55 Tahun 2019. Saat ini Indonesia sedang mengembangkan charging station di berbagai daerah, hal ini untuk meningkatkan penggunaan kendaraan listrik, pengembangan ini juga didukung oleh perusahaan-perusahaan transportasi lainnya (Dharmawan et al., 2021).

Namun, charging station merupakan salah satu tempat yang rawan digunakan untuk melakukan kejahatan siber. Hal ini dikarenakan kabel cas yang terhubung kepada EV dapat menyalurkan virus-virus yang dapat merusak perangkat EV (Nugroho, 2023). Hal ini dikarenakan area kontrol dari EV diatur dengan sistem yang saling berhubungan satu sama lain, sehingga dapat dimungkinkan untuk terkena malware yang disebabkan dari faktor eksternal. Faktor eksternal yang dimaksud disini adalah cas yang digunakan EV tersebut. Dimana bila penyerang tersebut dapat masuk, maka area kontrol dapat memiliki kontrol penuh. Hal ini menyebabkan penyerang dapat melakukan hack seperti menyadap, memodifikasi, memalsukan, dll (Acharya et al., 2020). Peretas dapat menyerap data dengan perangkat cas yang dapat disensor dengan kebiasaan pengguna EV (Nugroho, 2023). Ada pula pengisian daya Vehicle to Grid (V2G) yang dapat mengontrol pengisian daya baterai EV, sehingga fungsinya untuk mencegah adanya pemasukan jaringan listrik yang berlebihan dan untuk meminimalkan biaya yang dikeluarkan pengguna EV. V2G dapat menghubungkan EV dengan jaringan listrik menggunakan perangkat pengisi daya yang telah termasuk pertukaran data dan kontrol dari beberapa entitas pada EV. Penghubungan ini lah yang membuat bahaya terhadap peretasan EV, dimana hubungan ini bila diretas maka data yang ditransfer akan bocor ke pihak peretas (metere et al., 2021).

Permasalahan mengenai peretasan terhadap EV memang masih belum ditemui di Indonesia. Tetapi sudah terdapat beberapa negara yang telah mengalami hal tersebut. Hal ini terjadi pada Februari 2022 pada salah satu charging station di Rusia, yang diretas karena akibat dari serangan ke Ukraine (strom, 2024). Pada peretasan ini memang tidak mengakibatkan korban jiwa atau pembobolan data pada perangkat lunak, tetapi hanya ada pesan-pesan yang muncul

pada layar kendaraan EV. Adapula kasus yang terjadi di Amerika Utara, dimana pada tahun 2019 terdapat serangan siber yang membuat ada celah dalam mentransfer data di firewall operator energi yang membuat peralatan menyala ulang dan menyebabkan konsumen tidak dapat mengakses beberapa layanan (Macharia et al., 2023). Dari 2 kasus diatas, menunjukkan bahwa peretasan terhadap kendaraan EV bukanlah hal yang tidak dapat terjadi. Kasus diatas menunjukkan adanya peretasan yang terjadi karena faktor eksternal seperti charging station dan juga dapat dari faktor internal yaitu dengan penghubung internet. Hal ini menunjukkan adanya kepentingan untuk membuat pengaturan mengenai perlindungan siber bagi pengguna kendaraan EV. Dimana terdapat kasus nyata terjadinya peretasan pada EV melalui charging station maupun dari jarak jauh.

Indonesia sendiri telah membentuk pengaturan tentang kejahatan siber dengan Undang-Undang No 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang diubah dengan Undang-Undang No. 11 Tahun 2016 Tentang Perubahan atas Undang-Undang No 11 Tahun 2008 dan perubahan yang kedua yaitu Undang-Undang No 1 Tahun 2024 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 (UU ITE). Selain itu, ada pula pengaturan mengenai perlindungan data pribadi yaitu Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Pengaturan yang diberikan oleh Indonesia masih belum dapat menjadi alat yang ampuh untuk mengurangi kejahatan siber. Hal ini karena UU ITE ini dianggap masih belum memberi kejelasan dan masih memiliki celah untuk dilakukan pelanggaran (Mohammad & Mustam, 2023). Dimana UU ITE ini masih bersifat umum sehingga belum dapat menjangkau kejahatan siber yang terus berkembang (Hadi, 2024). Indonesia harus dapat mencontoh negara-negara lain yang telah mengatur atau memiliki upaya untuk kejahatan siber pada EV. Walaupun kejahatan ini belum terjadi di Indonesia, ada baiknya Indonesia untuk memiliki pengaturan yang dapat mencegah terjadinya kejahatan siber ini.

Salah satu negara yang telah membuat upaya untuk memerangi kejahatan siber terhadap EV adalah negara United State atau Amerika. Dimana US melakukan penelitian, pengembangan, dan demonstrasi keamanan siber baru atas alat dan teknologi yang akan menjadi alat pengisian daya lebih aman untuk EV. Pada tahun 2023, Cybersecurity, Energy Security, and Emergency Response (CESER) secara langsung mengeluarkan dana sebesar 5 miliar dollar untuk dialokasikan ke laboratorium nasional DOE untuk mengatasi permasalahan EV dan keamanan siber. Proyek ini akan menghasilkan solusi yang inovatif untuk memastikan charging station di seluruh negeri aman, andal, dan mudah diakses (Securing EV Charging Infrastructure Part 1: Why Cybersecurity Matters, 2024). Hal ini dikarenakan pemerintah US menargetkan pada tahun 2030 untuk pembangunan 500.000 charging station publik diseluruh negara US. Dimana CESER akan menginvestasikan sebesar 8 miliar dolar untuk melakukan penelitian terhadap standar keamanan siber dan teknologi untuk mencegah dan memitigasi kejahatan siber dari charging station (Securing EV Charging Infrastructure Part 2: Game-Changing Research, 2024).

Pada pasal 26 UU ITE telah mengatur mengenai persetujuan pengaksesan data diri seseorang. Dimana setiap media elektronik yang berhubungan dengan data pribadi perlu mendapat persetujuan dari orang yang bersangkutan. Hal ini menjelaskan bahwa Indonesia telah mengatur mengenai persetujuan penggunaan data pribadi seseorang. Namun, pengaturan ini masih belum dapat mencegah angka kebocoran data diri masyarakat Indonesia. Sehingga perlu adanya pengembangan pengaturan mengenai kebocoran data dari EV. Pada UU perlindungan data pribadi hanya menjelaskan mengenai larangan mengenai penggunaan data pribadi. Seseorang dilarang menggunakan data pribadi orang lain untuk mencari keuntungan sendiri atau

dapat mengakibatkan kerugian pada pemilik data, dilarang pula mengungkapkan data pribadi yang bukan miliknya, dan larangan untuk menggunakan data orang lain. Larangan yang dijelaskan ini dapat melindungi seseorang dari kebocoran data. Namun, pengaturan ini tidak dapat terlaksana dengan baik bila dilakukan secara online. Hal ini dikarenakan bila seseorang melakukan peretasan akan sulit untuk dilacak. Selain itu, pengaturan mengenai perlindungan data diri pada EV perlu dilakukan karena adanya rencana pengembangan infrastruktur charging station di Indonesia, dimana dengan pemberlakuan charging station maka dimungkinkan akan ada serangan siber yang telah terjadi pada negara-negara maju (Khosim & Hamdi, 2023). Oleh karena itu, pemerintah Indonesia harus melihat beberapa pengaturan yang telah dilakukan oleh negara-negara maju.

Di United Kingdom atau UK telah membuat regulasi dan tata cara IoT dan panduan prinsip keamanan siber untuk menghubungkan dengan kendaraan otomatis. Menurut General Data Protection (GDPR) yang dilaksanakan tahun 2018, dimana pengaturan ini memberi pengaturan yang lebih khusus terhadap hak yang berhubungan dengan data pribadi pengguna. GDPR menjelaskan bahwa pengguna memiliki hak untuk mendapat informasi, mengakses, memperbaiki, atau menghapus data, dll. GDPR ini selanjutnya ditegaskan lagi pada publikasi pemerintah tentang IoT. Dimana dokumen ini mempertegas tentang persyaratan perlindungan dan proses data pribadi telah sesuai dengan Undang-Undang perlindungan data. Namun, dokumen ini masih belum menyebutkan EV secara jelas, tetapi pengaturan ini dapat mencakup EV. Hal ini karena adanya definisi yang sesuai yaitu perangkat Iot yang terhubung dan pelaku yang terlibat dalam pengisian daya EV harus mematuhi hal tersebut. Terdapat pula perlindungan dari ICO yang memberi saran, bimbingan, kepada organisasi dan konsumen dan memberi hukuman sebesar 400.000 euro bagi perusahaan yang gagal melindungi data pelanggan dengan benar. Hal ini juga diatur pada DfT yang berkolaborasi dengan Center for the Protection of Nation Infrastructure (CPNI) dan Centre for Connected and Autonomous Vehicles yang mempublikasi 8 principle. Pada principle 7.1 menjelaskan bahwa data yang disimpan maupun akan ditransfer harus cukup aman dan hanya penerima atau sistem yang dituju saja yang dapat menerima atau mengakses, dan menganggap bahwa komunikasi yang akan masuk dianggap tidak aman hingga divalidasi. Pada principle 7.3 menjelaskan bahwa pengguna dapat menghapus data yang ada dan terhubung pada sistem (metere et al., 2021).

Melihat dari negara-negara diatas maka dapat dilihat bahwa negara-negara maju telah menganggap pentingnya pengaturan perlindungan data pada EV. Dimana negara-negara maju telah memiliki pengaturan maupun pengembangan dengan menggunakan kerjasama secara khusus untuk mengatasi permasalahan perlindungan data pada EV. Berbanding dengan Indonesia yang masih menggunakan UU ITE dan UU perlindungan data pribadi sebagai acuan pencegahan peretasan.

2. Potensi Masalah Sistem EV

Potensi masalah bahkan peretasan perangkat lunak pada EV sangat mungkin terjadi. EV yang merupakan kendaraan berbasis listrik yang menggunakan banyak perangkat lunak dapat mengalami kegagalan sistem yang tidak terduga karena kesalahan sistem itu sendiri (Saputra & Sewu, 2023). Sebagai contoh adanya inovasi mobil otonom atau kendaraan tanpa mengemudi yang mampu bergerak dan bernavigasi tanpa campur tangan manusia (Achyunda Putra et al., 2020). Kendaraan otonom tersebut menggunakan berbagai macam teknologi seperti GPS dan sensor yang diserap oleh perangkat lunak untuk beroperasi selayaknya manusia. Tentu tidak

akan menutup kemungkinan apabila terjadi malfungsi teknologi pada kendaraan yang berbasis teknologi. Sebagai contoh mobil google yang ditilang oleh polisi karena kesalahan sistem sehingga menyebabkan antrian panjang di jalan (Prakken, 2017). Apabila hal tersebut terjadi di Indonesia, belum terdapat peraturan hukum yang mengatur bagaimana penggunaan mobil otonom di jalan raya. Selama ini Indonesia masih menggunakan UU LLAJ sebagai peraturan yang mengatur terkait lalu lintas angkutan darat, yang mana pada aturan tersebut dibuat untuk mobil yang dikendarai oleh tenaga manusia dan bukan teknologi (Juliansyah, 2022).

Ditinjau dari Peraturan Pemerintah Nomor 44 Tahun 1993 tentang Kendaraan dan Pengemudi (selanjutnya disebut PP No. 41 Tahun 1993) maka kendaraan otonom masuk dalam kategori mobil penumpang namun menggunakan mesin teknologi karena belum adanya peraturan yang secara khusus yang membahas mengenai mobil otonom. Oleh karena itu apabila terjadi malfungsi terhadap kendaraan berbasis teknologi hingga menyebabkan kecelakaan maka akan kembali pada Pasal 234 UU LLAJ yang artinya pengemudi atau pengendara yang akan bertanggung jawab penuh apabila terjadi kecelakaan atau permasalahan di jalan. Pasal 106 UU LLAJ juga menjelaskan bahwa salah satu kewajiban pengemudi harus mengemudikan kendaraan dengan benar dan penuh konsentrasi, tetapi hal ini tidak bisa berlaku apabila kendaraan tersebut autopilot. Oleh karena UU LLAJ menganut *performance liability* dan *strict liability* yang menyebabkan pengemudi harus bertanggung jawab apabila dapat dibuktikan kesalahan tersebut memiliki hubungan yang erat dengan tindakan pelaku.

Prinsip dalam UU LLAJ tersebut dapat merugikan pihak pengemudi yang mana pengemudi yang telah membeli otomotif dengan teknologi autopilot dengan berharap dapat mempermudah hidupnya namun harus menanggung kerugian akibat kesalahan yang terjadi pada sistem otomotif tersebut (Saputra & Sewu, 2023). Karena pasal 1 angka 23 UU LLAJ menjelaskan bahwa pengemudi adalah pengendali kendaraan tersebut. Tidak adil rasanya apabila kesalahan yang terjadi karena faktor teknologi dijerat dengan hukuman yang sama dengan kesalahan yang terjadi karena akibat kesalahan manusia. Sehingga istilah pengemudi perlu diubah untuk mencerminkan peran baru yang dimainkan oleh sistem autopilot. Hal ini untuk menghindari pengguna mobil listrik dengan autopilot dibebankan tanggung jawab atas konsekuensi dari kecelakaan yang terjadi akibat korban dari malfungsi teknologi dari pelaku usaha. Sehingga ada urgensi untuk merubah atau memperluas definisi ketentuan yang terdapat pada UU LLAJ agar dapat memberi kepastian hukum pada pengendara mobil otonom.

Upaya yang dapat dilakukan pemerintah untuk mencegah terjadinya malfungsi teknologi dari kendaraan otonom akan terbagi menjadi 2 (dua) jenis yakni upaya represif dan upaya preventif. Dalam kasus ini upaya preventif berperan lebih besar dibanding peran represif, karena membahas mengenai kecelakaan, upaya preventif memiliki peran yang lebih besar untuk mengurangi angka kecelakaan (Ratnawaty, 2022). Upaya represif akan berkaitan dengan upaya pencegahan, dimana pemerintah mengambil andil yang besar untuk mencegah terjadinya kecelakaan yang diakibatkan kendaraan berbasis teknologi. Pemerintah dapat membuat standar operasional prosedur (selanjutnya disebut SOP) bagi pelaku usaha untuk dapat menyesuaikan pengaturan fitur dalam kendaraan tersebut agar sesuai dengan peraturan dan budaya lalu lintas berkendara di Indonesia. Apabila pelaku usaha tidak mematuhi SOP yang ditetapkan pemerintah dalam mengembangkan dan memasarkan mobil listrik, maka pemerintah dapat mengenai sanksi administratif kepada pelaku usaha.

Adapun pengenaan sanksi administratif kepada pelaku usaha dapat dikenakan secara bertahap dari peringatan tertulis, tindakan paksaan pemerintah (*bestuursdwang*), penarikan

kembali keputusan yang menguntungkan, denda administratif, dan bahkan pengenaan uang paksa (dwangsom) (Setiadi, 2009). Selain membuat SOP, pemerintah juga dapat menambahkan klausul terkait kendaraan otonom dan berbasis listrik dalam UU LLAJ ataupun membuat peraturan baru untuk memastikan keamanan teknologi kendaraan otonom yang semakin berkembang di Indonesia. Klausul yang perlu diatur dalam peraturan tersebut paling sedikit adalah standar keamanan tanggung jawab pengemudi kendaraan otonom dan berbasis listrik. Adapun standar keamanan yang diatur dapat berkaitan dengan standar pengoperasian mobil otonom di jalan raya, sedangkan tanggung jawab pengemudi akan berkaitan dengan penentuan pihak yang bertanggung jawab atas kejadian yang terjadi apabila terjadi berbagai situasi di jalan. Sebagai contoh negara Austria yang telah mengeluarkan undang-undang terkait pengujian dan penggunaan kendaraan listrik di jalan umum berdasarkan aturan Austrian Civil Code (ABGB), Austrian Railway and Motor Vehicle Liability Act (EKHG) dan Austrian Product Liability Act (PHG).

Pada undang-undang tersebut mengatur bahwa pelaku usaha bertanggung jawab atas kerusakan yang disebabkan oleh kendaraan dalam situasi dimana kendaraan tersebut beroperasi secara otonom sepenuhnya, sedangkan pengemudi tidak bertanggung jawab atas kerusakan yang disebabkan oleh mobil otonom dalam situasi mobil tersebut beroperasi otonom sepenuhnya (Zehetner et al., 2024). Pengecualian diatur apabila pengemudi tidak mengikuti instruksi dari sistem otonom atau melakukan tindakan yang membahayakan maka pengemudi bertanggung jawab atas kerusakan yang disebabkan oleh tindakan pengemudi. Kedua hal tersebut perlu diatur agar terciptanya kepastian hukum dalam pelaksanaan kendaraan berbasis teknologi di Indonesia. Oleh karena itu pemerintah dapat membuat pengaturan baru terkait SOP bagi pelaku usaha pada kendaraan EV yang mereka operasionalkan di Indonesia agar mengurangi potensi terjadinya kesalahan sistem pada EV.

3. Potensi Ancaman Keamanan Siber pada EV Karena Pihak Ketiga

Selain potensi permasalahan pada perangkat lunak EV, masalah juga bisa muncul akibat ancaman keamanan siber EV karena pihak ke-3. Peretasan terhadap perangkat lunak EV sangat mungkin terjadi karena EV memiliki berbagai macam teknologi dalam menjalankan fungsinya sebagai alat transportasi. Perlu diketahui bahwa kendaraan EV memiliki potensi yang besar untuk diretas. Adapun yang menjadi penyebab kerentanan untuk terjadi peretasan pada EV karena EV dilengkapi banyak sensor, penggunaan perangkat lunak pihak ketiga, dan perangkat keras yang cacat (Muhammad et al., 2023b). Ancaman terhadap EV tersebut dapat dibagi menjadi beberapa kategori yakni malware, serangan aplikasi pihak ketiga, dan serangan berbasis sensor (Muhammad et al., 2023b).

Malware adalah perangkat lunak yang jahat yang dapat merusak sistem EV yang dapat mengenkripsi dan mencuri data pada EV, apabila serangan aplikasi pihak ketiga terjadi pada saat EV bekerja sama dengan perusahaan lain seperti google maps atau EVgo sebagai perangkat penunjang pada EV (Rieck et al., n.d.). Sedangkan serangan berbasis sensor adalah serangan yang dilakukan peretas yang dapat mengganggu dan memanipulasi data sensor EV untuk mengendalikan kendaraan (Fraiji et al., 2018). Ketiga serangan tersebut memiliki kesamaan, yakni sama-sama terjadi karena tindakan peretas. Sebagai contoh Colombo yang merupakan white hackers mampu mengontrol mobil autonomous sehingga bisa berjalan sendiri dengan menentukan lokasi tujuan. Namun karena Colombo merupakan white hackers, yang artinya bukan hackers yang memiliki niatan buruk, Colombo menyampaikan celah keamanan tersebut

kepada pemilik mobil dan perusahaan Tesla (Ramadhan, 2022). Ancaman ini dapat berdampak serius karena dapat menimbulkan bahaya bagi pemilik mobil bahkan menimbulkan kecelakaan. Memang dalam UU ITE telah diatur bahwa terdapat larangan untuk meretas berdasarkan pasal 30 ayat (1), (2), dan (3), dan pasal 46. Teknologi saja hanya berpotensi menimbulkan kerugian materi, namun kolaborasi teknologi dengan transportasi dapat menyebabkan kerugian materi dan korban jiwa. Oleh karena itu pemerintah masih perlu ambil andil untuk mencegah terjadinya peretasan dari pihak ke-3.

Upaya yang dapat dilakukan oleh pemerintah untuk mencegah permasalahan yang terjadi akibat peretas adalah dengan meningkatkan standar keamanan siber untuk pelaku usaha EV. Pemerintah bisa bekerja sama dengan pihak lain untuk membuat regulasi yang dapat meningkatkan keamanan siber bagi pelaku usaha dibidang transportasi. Adapun solusi yang dapat diberikan terhadap permasalahan tersebut adalah memberikan pertahanan terhadap malware dengan menerapkan Sistem Deteksi Intrusi Berbasis Anomali (selanjutnya disebut IDS) untuk dapat mendeteksi pola perilaku yang tidak normal pada jaringan EV, menguji keamanan aplikasi pihak ketiga sebelum terintegrasi dengan sistem EV, dan menggunakan autentikasi dua faktor yang menggabungkan antar aplikasi-aplikasi terkait (Aslan & Samet, 2020). Hal tersebut dapat dituangkan pemerintah melalui SOP bagi pelaku usaha EV agar pelaku usaha dapat benar-benar menjamin keamanan konsumennya. Negara-negara di Eropa telah memulai langkah terlebih dulu dalam pencegahan dan penanggulangan peretasan EV melalui pengaturan khusus. The EU Product Liability Directive (selanjutnya disebut Directive 85/374/EEC) adalah regulasi yang mengatur mengenai kejahatan siber. Dalam pasal 7 Directive 85/374/EEC menjelaskan bahwa produk yang memiliki kerentanan keamanan siber, maka pelaku usaha tersebut akan bertanggung jawab terhadap kerugian yang terjadi. Pengaturan tersebut akan mendorong agar pelaku usaha dapat meningkatkan keamanan siber terhadap transportasi yang dikomersilkan (Vellinga, 2023).

Pemerintah dapat menambahkan pemberian sanksi administratif bagi pelaku usaha yang tidak memenuhi SOP untuk menerapkan sistem IDS dan autentikasi dua faktor. Karena PP No. 55 Tahun 2019 sama sekali tidak mengatur mengenai SOP keamanan siber EV. Dengan pemerintah membuat ketentuan mengenai SOP keamanan siber, maka pelaku usaha akan menjadikan regulasi tersebut sebagai pedoman dalam mengoperasikan keamanan siber pada transportasinya. Apabila pelaku usaha tidak mengikuti pedoman tersebut, maka dapat dikenai sanksi administratif mulai dari teguran tertulis hingga pencabutan izin usaha dan pengenaan uang paksa (dwangsom). Dengan memberikan sanksi administratif pada pelaku usaha akan secara efektif mencegah terjadinya peretasan yang tentu merugikan konsumen (Yudistira & Ramadani, 2023). Selain Eropa, Indonesia juga dapat mencontoh Undang-Undang Keamanan Siber Republik Rakyat Tiongkok yang mengumpulkan beberapa data yang disebut “important datas” yang tidak dapat dibagikan ke luar Tiongkok tanpa diperiksa dan diizinkan oleh pihak berwenang (Khan et al., 2023). Dengan membuat regulasi tersebut, secara langsung pemerintah akan mencegah terjadi peretasan EV yang ada di Indonesia yang dilakukan oleh peretas luar negeri. Pemerintah dapat memasukan jaringan yang terdapat dalam EV sebagai “important datas” untuk mencegah peretas mengakses EV pengemudi di Indonesia yang bisa berdampak terhadap keamanan pengemudi EV. Karena sifat kejahatan teknologi adalah lintas negara, kejahatan dapat dilakukan menggunakan teknologi informasi dan komunikasi untuk melakukan tindakan yang melampaui batas negara, sehingga tidak terbatas teritorial (Aulia Agustin et al., 2023).

KESIMPULAN

Indonesia merupakan negara yang tergolong baru dalam penggunaan EV dan masih belum memiliki pengaturan yang komprehensif terkait keamanan siber EV. Hal ini dikarenakan adanya peningkatan penggunaan kendaraan EV di Indonesia. Peningkatan ini dapat dilihat melalui peningkatan penjualan kendaraan EV dari tahun 2020 hingga 2022. Pada tahun 2022 peningkatan penjualan EV meningkat sebesar 383,62% dari tahun sebelumnya (Ardiyanti et al., 2023). Dimana keamanan siber pada EV perlu diperhatikan karena dapat berdampak pada keselamatan, pencurian data, bahkan dapat menyebabkan kecelakaan. Peretasan dalam EV dapat berasal dari peretasan dari penghubung ke EV, dari kelemahan pada sistem EV, dan dari serangan dari pihak ketiga. Indonesia telah memiliki pengaturan mengenai kejahatan siber namun masih bersifat umum. Salah satu kendaraan EV yang mudah diretas adalah smart car, dimana smart car ini berpusat pada satu perangkat lunak untuk menggerakkan mobil tersebut. Peretasan ini dapat melalui TPMS dan saat melakukan pengisian daya pada charging station. Indonesia telah memiliki pengaturan mengenai kejahatan siber namun masih bersifat umum yaitu dengan UU ITE dan UU perlindungan data pribadi. Peretasan pada EV ini memang masih belum ditemukan di Indonesia, namun negara lain seperti Rusia atau Amerika sudah pernah merasakan dari peretasan pada EV.

Sistem pada EV masih dapat ditemukan potensi terjadinya malfungsi pada perangkat lunak pada sistem EV karena kelemahan sistem itu sendiri. Sebagai contoh yaitu mobil otonom yang mengalami malfungsi teknologi pada AC hingga memberikan dampak pada keselamatan jiwa. Indonesia masih belum memiliki pengaturan hukum yang mengatur bagaimana penggunaan mobil otonom di jalan raya. Pengaturan pada LLAJ masih belum dapat dilakukan atau diterapkan pada mobil otonom, hal ini akan merugikan pengemudi yang harus menanggung kerugian yang diakibatkan oleh kesalahan sistem otomotif. Oleh karena itu, pemerintah dapat membuat SOP bagi pelaku usaha untuk pengaturan fitur dalam kendaraan tersebut. Pemerintah juga dapat menambahkan klausul terkait kendaraan otonom dan berbasis listrik dalam UU LLAJ ataupun membuat pengaturan baru untuk memastikan keamanan teknologi kendaraan otonom.

Adapun ancaman bagi keamanan siber pada EV dapat dibagi menjadi beberapa kategori, yaitu malware, serangan aplikasi pihak ketiga dan serangan berbasis sensor. Ancaman ini dapat berakibat serius karena dapat menimbulkan bahaya bagi pemilik mobil. Upaya yang dapat dilakukan oleh pemerintah yaitu dengan meningkatkan standar keamanan siber untuk pelaku usaha EV. Selain itu, pemerintah juga dapat melakukan kerjasama dengan pihak lain untuk membuat regulasi, memberikan sanksi administratif bagi pelaku usaha yang tidak mematuhi SOP. Oleh karena masih banyaknya ditemukan kekurangan pemerintah dalam pengaturan mengenai EV, maka Indonesia perlu mencontoh dari negara-negara lain seperti UK, Amerika, China, Eropa, dan lain-lain.

DAFTAR PUSTAKA

- Acharya, S., Dvorkin, Y., Pandzic, H., & Karri, R. (2020). Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective. In IEEE Access (Vol. 8, pp. 214434–214453). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/ACCESS.2020.3041074>
- Achyunda Putra, F. A. I., Utaminigrum, F., & Mahmudy, W. F. (2020). HOG Feature Extraction and KNN Classification for Detecting Vehicle in The Highway. IJCCS

- (Indonesian Journal of Computing and Cybernetics Systems), 14(3), 231.
<https://doi.org/10.22146/ijccs.54050>
- Anwar, S. (2018). Penguasaan Teknologi Pertahanan Oleh SDM Pertahanan Dalam Rangka Menghadapi Peperangan Masa Depan. *Jurnal Pertahanan & Bela Negara*, 5(1).
<https://doi.org/10.33172/jpbh.v5i1.346>
- Ardiyanti, D., Kurniawan, F., Raokter, U., & Wikansari, R. (2023). Analisis Penjualan Mobil Listrik Di Indonesia Dalam Rentang Waktu 2020-2023. *ECOMA: Journal of Economics and Management*, 1(3), 114–122. <https://doi.org/10.55681/ecoma.v1i3.26>
- Aslan, O., & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. *IEEE Access*, 8, 6249–6271. <https://doi.org/10.1109/ACCESS.2019.2963724>
- Aulia Agustin, N., Meilani, R., & Firdos. (2023). Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital. *Jurnal Mahasiswa Teknik Informatika "JAMASTIKA,"* 3(1).
- Cakrawati Sudjoko. (2021). Strategi Pemanfaatan Kendaraan Listrik Berkelanjutan Sebagai Solusi Untuk Mengurangi Emisi Karbo. Departemen Ketahanan Energi, Universitas Pertahanan Indonesia, IPSC Area, Sentul, 2, 1–15.
- Cakrawati Sudjoko. (n.d.). Strategi Pemanfaatan Kendaraan Listrik Berkelanjutan Sebagai Solusi Untuk Mengurangi Emisi Karbon. *Jurnal Paradigma: Jurnal Multidisipliner Mahasiswa Pascasarjana Indonesia*, Vol. 2 No 2 (2021), 1–15.
- Dharmawan, I. P., S Kumara, I. N., & Budiastra, I. (2021). Perkembangan Infrastruktur Pengisian Baterai Kendaraan Listrik di Indonesia. *Jurnal SPEKTRUM*, 8(3).
- Fariza Ramadhani. (2023). Dinamika UU ITE Sebagai Hukum Positif di Indonesia Guna Meminimalisir Kejahatan Siber. *Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora*, 89–97.
- Fraiji, Y., Ben Azzouz, L., Trojet, W., & Saidane, L. A. (2018). Cyber security issues of Internet of electric vehicles. 2018 IEEE Wireless Communications and Networking Conference (WCNC), 1–6. <https://doi.org/10.1109/WCNC.2018.8377181>
- Hadi, A. M. (2024). Cyber Crime in Renewing The ITE Law to Realize The Goals of Legal Justice. <https://doi.org/10.20961/jolsic.v12i1.851>
- Hanief Amarullah, A., Josias Simon Runturambi, A., Widiawan, B., & Hanief, A. (2021). Analisis Ancaman Kejahatan Siber Bagi Keamanan Nasional Pada Masa Pandemi COVID-19. *Strategik Ketahanan Nasional*, 4(2).
- Heary, J. (2010, July 31). Defcon: Hacking Tire Pressure Monitors Remotely. <https://www.networkworld.com/article/756954/cisco-subnet-defcon-hacking-tire-pressure-monitors-remotely.html>
- Juliansyah, F. M. (2022). Kepastian Hukum Terhadap Mobil Berteknologi Auto Pilot Ditinjau Dari Prespektif Hukum Lalu Lintas Jalan di Indonesia. *Bureaucracy Journal*, 2(2), 794–805. <https://doi.org/10.53363/bureau.v2i2.108>
- Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Warren, M. (2023). Cybersecurity Regulatory Challenges for Connected and Automated Vehicles. *Transport Policy*, 143, 58–71. <https://doi.org/10.1016/j.tranpol.2023.09.001>
- Khosim, N., & Hamdi, E. (2023). Financial Management for “eV-Station-Electric Vehicle Charging Station” in Indonesia. *Journal of Social Science Research*, 3, 1–10.
- Kusumah, H., Ari Pradana, O., & STMIK Raharja (n.d.). Perancangan Smart Car Menggunakan Speech Recognition Berbasis Arduino Uno.

- Macharia, V. M., Garg, V. K., & Kumar, D. (2023). A Review of Electric Vehicle Technology. IET Electrical Systems in Transportation, 13(2). <https://doi.org/10.1049/els2.12083>
- Maskun, S. G. (2022). Kejahatan Siber (Cyber Crime): Suatu Pengantar (Vol. 3). Kencana.
- Mohammad, A., & Mustam, A. (2023). Memerangi Kejahatan Siber di Indonesia. Jurnal Gema: Multi Disiplin Ilmu, 35(01).
- Muhammad, Z., Anwar, Z., Saleem, B., & Shahid, J. (2023a). Emerging Cybersecurity and Privacy Threats to Electric Vehicles. Energies, 16(3). <https://doi.org/10.3390/en16031113>
- Muhammad, Z., Anwar, Z., Saleem, B., & Shahid, J. (2023b). Emerging Cybersecurity and Privacy Threats to Electric Vehicles. Energies, 16(3). <https://doi.org/10.3390/en16031113>
- Nazmul Hasan, M., Didar-Al-Alam, S. M., & Rezwanul Huq, S. (2011). Intelligent Car Control for a Smart Car. International Journal of Computer Applications, 14(3).
- Nugroho, S. A. (2023, September 14). Tiga Celah Keamanan yang Bisa Bikin Cemas Pengguna Mobil Listrik. <https://www.oto.com>
- Prakken, H. (2017). On the problem of making autonomous vehicles conform to traffic law. Artificial Intelligence and Law, 25(3), 341–363.
- Ramadhan, R. (2022, January 21). Remaja Hacker Klaim Bobol 25 Mobil Tesla di 13 Negara. Kumparan Tech.
- Ratnawaty, L. (2022). Upaya Pencegahan Terhadap Kecelakaan Lalu Lintas di Kabupaten Bogor. Jurnal Yustisi, 9(2).
- Rieck, K., Holz, T., Willems, C., Düssel, P., & Laskov, P. (n.d.). Learning and Classification of Malware Behavior. Springer.
- Rohman, C. (2024, March 21). Chao meninggal di dalam danau bersama dengan Tesla Model X. Antara News.
- Saputra, G. R., & Sewu, P. L. S. (2023). Corporate Liability and Law Enforcement. Jurnal Hukum Sehasen, 9(2).
- Securing EV Charging Infrastructure Part 1. (2024, April 10). Office of Cybersecurity, Energy Security, and Emergency Response.
- Securing EV Charging Infrastructure Part 2. (2024, April 17). Office of Cybersecurity, Energy Security, and Emergency Response.
- Setiadi, W. (2009). Sanksi Administratif Sebagai Salah Satu Instrumen Penegakan Hukum. Jurnal Legislasi Indonesia, 6(4).
- Silalahi, L. M., Alaydrus, M., Rochendi, A. D., & Muhtar, M. (2019). Design of Tire Pressure Monitoring System. Jurnal Sinergi, 23(1).
- Sjafrie, H. (2019). Introduction to Self-Driving Vehicle Technology. CRC Press.
- Strom, D. (2024, April 10). EV Charging Stations Still Riddled With Cybersecurity Vulnerabilities.
- Tulus, V., & Sidabutar, P. (2020). Kajian pengembangan kendaraan listrik di Indonesia. Jurnal Paradigma Ekonomika, 15(1).
- Vellinga, N. E. (2023). Cyber security in automated vehicles and liability. Transportation Research Procedia, 72, 132–138.
- Yudistira, M., & Ramadani. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber. Unes Law Review, 5(4).

Zehetner, J., Cetin, M., & Holzer, A. (2024). The Civil Liability for Self-Driving Cars in Austria. Springer Cham.