Towards Semantic Coherence: Understanding Cybersecurity and Digital Sovereignty in the Automotive Landscape

1st Elisa Sorrentino
Institute of Informatics and Telematics
National Research Council
Rende(CS), Italy
elisa.sorrentino@iit.cnr.it

2nd Anna Federica Spagnuolo
Institute of Informatics and Telematics
National Research Council
Rende(CS), Italy
annafederica.spagnuolo@cnr.it

3rd Alessio Portaro
Institute of Informatics and Telematics
National Research Council
Rende(CS), Italy
alessio.portaro@iit.cnr.it

4th Maria Taverniti
Institute of Informatics and Telematics
National Research Council
Rende(CS), Italy
maria.taverniti@cnr.it

5th Elena Cardillo
Institute of Informatics and Telematics
National Research Council
Rende(CS), Italy
elena.cardillo@iit.cnr.it

2025 IEEE 31st International Symposium on On-Line Testing and Robust System Design (IOLTS) | 979-8-3315-3334-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/IOLTS65288.2025.11116851

Abstract—The relationship between cybersecurity and digital sovereignty is increasingly viewed as complementary. Cybersecurity focuses on the technical and operational protection of digital infrastructures, while digital sovereignty encompasses the political and strategic dimensions related to technological autonomy and the ability to regulate and make decisions. This intersection is particularly noticeable in technology and regulation-heavy sectors, such as the automotive industry, where vehicles are transforming into connected and intelligent platforms capable of generating, processing, and transmitting large amounts of data. In this context, protecting user privacy emerges as a critical challenge, closely linked to cybersecurity needs and the control over the cross-border flow of information. These dynamics show how difficult it is to coordinate cybersecurity, data management, and compliance across different countries, especially when foreign suppliers and supply chains are involved. Consequently, there is an urgent need for a coherent, shared, and relevant technical-conceptual framework that integrates operational requirements, fundamental rights, and strategic objectives. This paper proposes a semantic approach to analyze, systematize, and map emerging key concepts from normative sources, policy documents, and standards, using both expert-based approach and Artificial Intelligence models, to facilitate the extraction and organization of domain-specific terminology enhancing the population or enrichment of semantic resources. Results show the importance of controlled vocabularies, such as thesauri, which serve as fundamental tools for facilitating classification, interoperability, and for supporting normative production. In the case of the automotive sector, it becomes an operational support to address challenges related to cybersecurity, privacy protection, and regulatory autonomy.

Keywords—Semantic analysis, Cybersecurity, Digital Sovereignty, Automotive, Artificial intelligence

I. INTRODUCTION

Nowadays, we live in a hyper-connected world that involves every aspect of our daily actions and devices. In this scenario, road vehicles can no longer be considered mere means of transportation, they are becoming complex data collection systems, exposed to risks and threats that are not only physical but also digital, due to attacks aimed at stealing personal data and more. According to the UK's National Cyber Security Centre (NCSC), "Cyber security is how individuals and organizations reduce the risk of cyber-attack. Its core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access – both online and at work – from theft or damage. It's also about preventing unauthorized access to the vast amounts of personal information we store on these devices, and online" [1]. From another point of view "Cyber security" means the condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components" [2].

In the automotive field, this definition takes on a critical dimension: the "devices" are increasingly embedded control units, onboard networks, and cloud-connected interfaces, all of which interact continuously with external digital ecosystems. Within this context, "Risk" means the potential that a given threat will exploit vulnerabilities of a vehicle and thereby cause harm to the organization or to an individual [2]. Addressing this risk requires a clear, standardized, and context-aware understanding of the concepts involved.

Moreover, it is important to be aware that the relationship between cybersecurity and digital sovereignty is increasingly viewed as complementary. The former addresses the technical and operational defense of digital infrastructures, whereas digital sovereignty encompasses the strategic, political, and regulatory capacity of governments, organizations, and individuals to autonomously manage and control their digital resources, technologies, infrastructures, data, and decision-making processes [3].

The interrelation between these concepts has been studied in different contexts of the industry domain, bringing in some cases to the proposal of conceptual frameworks to provide structured approaches to internal and external governance in specific- data sharing environment. See for example [4] which integrates three pillars (Cybersecurity, Data Sovereignty and trustworthiness) into a single framework to evaluate the reliability of agri-data sharing environments, aligned with international regulatory frameworks to ensure that agri-data is managed in compliance with existing laws and best practices.

979-8-3315-3334-2/25/$31.00 ©2025 IEEE

This intersection is noticeable in technology- and regulation-heavy sectors, due to global supply chains, international regulatory frameworks, and the growing adoption of non-European technologies. In the automotive context this is particularly relevant, considering that vehicles are transforming into connected and intelligent platforms capable of generating, processing, and transmitting large amounts of data (to allow features like autonomous driving and predictive maintenance). In this context, protecting user privacy emerges as a critical challenge [5], closely linked to cybersecurity needs and the control over the cross-border flow of information. These dynamics show how difficult it is to coordinate cybersecurity, data management, and compliance across different countries, especially when foreign suppliers and supply chains are involved. Consequently, there is an urgent need for a coherent, shared, and relevant technical-conceptual framework that integrates operational requirements, fundamental rights, and strategic objectives.

This paper proposes a semantic approach to analyze, systematize, and map emerging key concepts from normative sources, policy documents, and scholarly literature with final aim to highlight the interrelations among the two concepts and their relevance in the Automotive domain, providing a semantic tool useful for facilitating classification, interoperability among databases, and for supporting normative production. The final output could be also open the way for an operational support to address challenges related to cybersecurity, privacy protection, and regulatory autonomy in the automotive sector [6].

II. Cybersecurity and Digital Sovereignty in the Automotive Domain

The digitalization of mobility, as said above, has transformed vehicles into cyber-physical systems based on complex software, cloud platforms, and real-time data exchange. The concept of cyber-physical systems in the automotive sector is extensively explored in both technical and legal literature, highlighting the implications for safety and privacy [7]. This paradigm introduces unprecedented risks: vulnerabilities in software components, third-party integrations, and remote communication channels can be exploited to compromise vehicle safety, user privacy, or even critical infrastructures[1].

Digital sovereignty in the automotive sector can be articulated through several key dimensions:

- Data control and localization: Ensuring that data generated by vehicles is managed in compliance with regulations such as GDPR [8].
- Technological autonomy: Promoting European alternatives to reduce dependence on foreign providers.
- Infrastructure resilience: Adopting frameworks like ISO/SAE 21434 [9] and the World Forum for Harmonization of Vehicle Regulations (UNECE WP.29) to secure connected systems.
- Regulatory alignment: Coordinating national and European cybersecurity policies (e.g., NIS2 Directive - Directive (EU) 2022/2555) [10].

III. Semantic Analysis of Normative Concepts

In any semantic or terminological extraction task—especially when aimed at building systems for facilitating knowledge organization, representation and retrieval—the fundamental question is: *What information and knowledge units should we identify to effectively represent a specialized domain?* Answering this requires first identifying the elements that can recognize the domain-specific meaningful units. This step is especially critical when employing automatic term extraction systems, where such an activity represents both a feasibility assessment and a benchmark for system accuracy. This conceptual groundwork also helps clarify whether the purpose of the activity affects the choice of methods and the specificity of the terms to be extracted. As stated in [11] "those who use terms, whether to assert, deny, or ask and presuppose shared definitions within a community". Similarly, in [12] is asserted that specialists always operate with a set of terminology, whether formalized or not, capable of describing their domain with precision.

This theoretical foundation becomes even more relevant when applied to domains considered complex such as automotive cybersecurity, where the fragmentation of regulatory sources, normative and the convergence of multiple disciplines (i.e. information technology, automotive engineering, privacy and data protection, cybersecurity, legal and regulatory studies, standardization, data governance and ethics, etc.) [13] demands a rigorous and consistent semantic framework.

To address the above-mentioned issue in this work a hybrid semantic approach is proposed to identify and systematize key concepts related to the interconnected cybersecurity and digital sovereignty topics in the automotive domain, emerging from standards and policy documents. The sources, although originating from different backgrounds, frequently exhibit conceptual overlap. They often use similar terms that refer to different concepts or have slightly different meanings based on their technical, legal, or operational contexts. This redundancy and variability in meaning can create ambiguity, which may compromise clarity in both compliance and information interoperability.

The first step of the proposed approach consists in a symbiotic analysis of the regulatory sources and key sector guidelines, carried out by domain experts. The regulations and guidelines considered are shown is Table 1. The output of this task is the identification of keywords distributed among specific clusters (see Table 1); thanks to the application of a hierarchical classification criterion that distinguishes between supranational sources, international technical standards, and national initiatives. This approach made it possible to assess the weight and relevance of each regulatory level in relation to different application areas and the stakeholders involved. More specifically, the hierarchical classification assumes that regulations issued at the supranational level, such as those from the European Union or international bodies, take precedence and provide the general framework of reference

[1] The vulnerabilities of such systems have been the subject of analysis within the European regulatory framework, with particular attention to the ISO/SAE 21434 standard and the NIS2 Directive for the protection of critical infrastructures

for all member states. International technical standards, developed by recognized standardization bodies, instead provide operational guidelines and specific requirements for the design and management of security in various sectors. Finally, initiatives and regulations adopted at the national level complete the regulatory framework by adapting general provisions to the needs and specificities of the local context and introducing targeted measures for governance, resilience, and technological innovation. This hierarchical structure makes it possible to clearly assess which regulatory level has the greatest impact on each area of application and to identify the interconnections between the various sources [14], thus supporting the adoption of integrated and coherent strategies. As an example, the analysis highlights how the GDPR and the NIS2 Directive are interconnected in their requirements regarding data protection and the management of security incidents, underscoring the importance of adopting integrated strategies.

TABLE I. CONCEPTUAL CLUSTERS, KEYWORDS, AND SOURCES

Clusters	Keywords	Normative References
Digital Identity	authentication, e-identity	eIDAS2, GDPR, NIS2
Software Security	vulnerabilities, OTA	UNECE WP.29, ISO/SAE 21434
Infrastructure Resilience	continuity, recovery	NIS2, National Cybersecurity Strategy
Technological Sovereignty	autonomy, data control	National Strategy, Strategic Hub
Data Protection	privacy, data ownership	GDPR, Strategic Hub, CAN
Interoperability	Data Protection	privacy, data ownership
Technological Autonomy	innovation, local development	National Strategy, ACN
Open Standards	transparency, compatibility	ISO/SAE 21434, ISO 26262, WP.29
Functional Safety	reliability, fail-safe	ISO 26262, WP.29
Regulatory Compliance	compliance, audit, reporting	NIS2, GDPR, ACN

The second step of the methodology consisted in a semi-automated systematic analysis of the above-mentioned sources by leveraging AI models to understand the semantic representativeness of the key concepts and clusters identified during Step 1 and so to validate them. To perform this task, the approach proposed in [15] was applied, previously tested for a use case aimed to enhance and populate a domain thesaurus on the cybersecurity domain. The motivation of this choice lay in the similarity of the corpus used (norms, standards, guidelines, and reports related to cybersecurity) and the possibility to identify not only concepts but also semantic relationships which are compliant to thesauri (e.g., hierarchical, equivalence and associative relationships) [16]. From an architectural point of view, the approach used here leverages from two modules for identifying and put in relation domain concepts. Initially it extracts knowledge from the corpus in the form of a Knowledge Graph (KG), and then a Bidirectional Encoder Representations from Transformers module finetuned for Natural Language Inference task (i.e., BERT-NLI) uses the KG as input to identify and extract thesaurus-compliant relationships between domain concepts (see [15] for more details).

The preliminary results of this second analysis shows a noticeable presence of the concepts related to the three themes investigated (i.e., domains of knowledge). On a total of 152,669 triple in the KG, 9,686 are unique concepts, which include about 200 concepts aligned to the key concepts reported in table 1, and the recognition of eight clusters among 10, showing a strong alignment with the output of Step 1, by confirming that the conceptual framework captures the multi-faceted nature of cybersecurity and digital sovereignty in the automotive domain. From a qualitative point of view, different observations can be reported. The results highlight in some cases the overlap of concepts among the sources collected in the corpus (as said normative sources, guidelines and standards), but with different facets. This is the case, for example, of the concepts “security” and “risk”, present in: i) UNECE WP29, R155 and ISO21434, representing, on one hand the “cyber risk” for integrity, availability and confidentiality of the vehicles, and, on the other hand, the functional safety as a direct consequence of cybersecurity. Those concepts are also present in GDPR, focusing on “privacy” and on security of personal data processing. As also observable during the symbiotic analysis, the AI-based processing of the sources identified several interconnections and semantic dependencies. In fact, there are a lot of cross-references between the regulations, above all UNECE WP 29, R155 and GDPR (e.g., personal data generated by vehicles need to be managed in compliance to GDPR). Other dependencies which were identified were related to cause-effect relationships, where are present concepts like “lack of a technical security measure” (in R155/ISO21434), which is related to “vulnerability” as an effect, and to “attack”, associated in turn to personal data breach, all concepts present in GDPR. Moreover, it must be considered that some of the key concepts are not always explicitly defined in the sources but can be inferred analyzing in depth the context. Regarding this aspect, the in-depth analysis performed by domain experts was crucial. This is specifically true for those concepts related to digital sovereignty, which still results a strategic context not directly regulated, even if within the considered regulations and guidelines there are concepts related to it, such as “data control”, “technology control” or “data localization”. More related to automotive, from the sources, it was possible to identify concepts such as data related to vehicles (e.g., “technical data”, “personal data”, “diagnostic data”, etc.), or concepts related to technical measures or risk classification and security requirements (distinguished for every step of the software/vehicle life cycle).

A final step of the methodology was more concentrated on the comparative analysis of the identified key concepts and their intersections (from Step1 and Step2) to understand if these are possible candidate terms for the enhancement of a previously developed thesaurus on cybersecurity (i.e., the OCS Thesaurus) [17] with the final aim to extend its semantic coverage, considering the increasing convergence of information technology, operational technology, the focus on digital sovereignty, and the role of the automotive sector. Considering that the OCS thesaurus is specifically focused on cybersecurity, was not surprising to find a very high degree of conceptual overlap with the concepts extracted from Step2 (it is worth remembering that some normative sources were also part of the corpus used to build the thesaurus itself), and above all the concepts if the 10 clusters in table 1, which in some way directly address cybersecurity facets.

The perfect matches are in most cases related to broader terms in the thesaurus (e.g. privacy, vulnerability, risk management, security mechanisms, data, personal data, etc.), while it was relevant to identify candidate narrower terms to be reported in some of the thesaurus broader terms, while on the contrary our clusters contain more generic terms that can be broader conceptual umbrella for some preferred terms in the thesaurus (e.g., "organizational resilience (cluster 1) is a broader term for some cybersecurity practices present in the thesaurus like "business continuity"). Moreover, many possible related terms (RT) where found from the comparative analysis (e.g., data breach can have a new RT like "data protection", identified in Step 1 and Step2). Finally, regarding the key concepts / clusters related to the automotive domain, not surprisingly they were not mapped to the thesaurus (e.g., "automotive CSMS", "vehicle data sovereignty", etc.) since, as said, the focus of the thesaurus is different, but they need to be included to allow the composition of other elements (concepts) present in the thesaurus (e.g., CSMS is related to risk management, incident response, and in the same way "vehicle data sovereignty" can be related to the new candidate term data protection, and a to a broader term to be integrate "digital sovereignty", etc.).

At this stage, the results of this comparative analysis are going to be validated by a domain expert to finalize the list of candidate terms to be included in the OCS thesaurus.

Once enhanced, such a thesaurus can serve as a useful tool for actors involved in the definition of regulations and for stakeholders of the automotive domain, to be compliant with the granularity of information shared by the communities of experts and to represent semantic connections among the domain-dependent concepts, thus guaranteeing semantic coherence and semantic interoperability.

IV. IV. DISCUSSION

Building coherent governance for cybersecurity and digital sovereignty in the automotive sector requires rigorous regulatory mapping, the definition of semantic frameworks to precisely organize concepts and their relationships [18], and the adoption of integrated strategies. As highlighted in the previous analysis, applying a hierarchical classification of regulatory sources from supranational directives and international technical standards to national initiatives enables a clearer understanding of the roles and impacts of different regulatory levels on various stakeholders and application domains. This multi-level perspective is essential to capture the complexity of the automotive ecosystem, where vehicles increasingly operate as interconnected digital platforms embedded within global supply chains and diverse regulatory environments. The semantic analysis conducted on our normative sources confirm that "cybersecurity", "data", "digital sovereignty" and "resilience" are central, highly interconnected nodes in the policy and regulatory discourse. In our opinion this underlines their strategic role in influencing digital governance. In fact, the concept of strategic autonomy, particularly in relation to digital sovereignty, appears as semantically linked to national development goals, technological capability, and sovereignty-preserving innovation frameworks. To effectively address the intertwined challenges of cybersecurity and digital sovereignty, integrated strategies must be adopted. These strategies should harmonize technical and operational security measures with political and strategic objectives, ensuring not only the protection of data and systems but also the preservation of technological autonomy and regulatory control. From the semantic point of view, statistical analysis revealed the noticeable alignment of the clusters/key concepts identified by domain experts to concepts automatically extracted by the applied BERT-NLI model, with a high recurrence of terms such as data protection, privacy, and software security especially in contexts related to digital infrastructure and resilience highlighting the prominence of these dimensions also in automotive strategic documentation. Once compared to the OCS thesaurus, the key concepts / clusters identified revealed, as well, a high percentage of exact matching with regard to cybersecurity related concepts, but also a high percentage of concepts which can be used to enhance the thesaurus with new preferred terms (mostly related to digital sovereignty and the automotive sector) and new NT and RT which provide semantic completeness of some terms already present in the thesaurus. A limitation of the approach, in this sense, is the restrictiveness of the comparative analysis to the OCS thesaurus, strictly related to cybersecurity. In fact, the consideration of other semantic resources (e.g., ontologies focused on automotive) could help in defining a more comprehensive semantic tool devoted to cover the interrelation of the reference concepts. The dynamic interplay between standards such as ISO 26262, which focuses on functional safety, and regulations like UNECE WP.29, which mandates cybersecurity management systems, exemplifies the need for coordinated compliance frameworks that bridge safety, security, and sovereignty. Moreover, the rapid pace of technological innovation in automotive driven by Industry 5.0 paradigms and the proliferation of connected and autonomous vehicles requires governance models that are resilient, adaptable, and aligned with international best practices [3]. Such models must foster collaboration among manufacturers, suppliers, regulators, and end-users to promote solutions that balance security, innovation, and the protection of fundamental digital rights. The evolution of regulatory frameworks must continue to anticipate and respond to emerging technological trends, facilitating the development of a secure, sovereign, and competitive automotive sector [19]. The semantic approach discussed in this work provide a foundational toolset to support this ongoing process, enabling clearer interoperability, improved compliance, and strategic decision-making in a complex and evolving landscape.

V. V. CONCLUSIONS AND FUTURE DEVELOPMENTS

The imperative to enhance cybersecurity in the rapidly evolving automotive sector now transitioning to interconnected digital platforms demands a comprehensive framework that harmonizes cybersecurity measures with principles of digital sovereignty. This paper introduces a semantic approach, which combines in-depth analysis (i.e., symbiotic analysis) by domain experts (including legal scholars and terminologists) with semi-automated concept mapping from key normative sources, providing additional comparative analysis across domain-oriented controlled vocabularies. This methodology not only ensures regulatory alignment and mitigates terminological ambiguities but also provides an operational toolset that bridges the gap between regulatory mandates and their technical implementation in the automotive domain, and which can be used for facilitating classification, interoperability, and effective risk management. Ultimately, establishing such a semantically

coherent framework is crucial for enhancing compliance, facilitating clear communication across multidisciplinary teams, and ensuring a secure, sovereign, and competitive automotive landscape that balances innovation with the safeguarding of fundamental digital rights. Possible technical advancements and future works includes the use of cybersecurity and automotive-related ontological models, to better capture the semantic of the domain and the relationships between concepts, as well as the implementation of case studies to apply a more structured semantic framework facilitating interoperability and data interpretation within automotive risk assessment systems.

ACKNOWLEDGMENT

This work was supported by SERICS "SEcurity and RIghts in CyberSpace" (PE00000014) project under the MUR National Recovery and Resilience Plan, funded by the European Union - NextGenerationEU, spoke 7.

REFERENCES

[1] National Cyber Security Centre (NCSC). (2024). *What is cybe security?*. Retrieved from https://www.ncsc.gov.uk/section/information-for/what-is-cyber-security

[2] UNECE. UN Regulation No. 155: Cyber Security and Cybersecurity Management System [CSMS]. 2021. Available: https://www.unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security.

[3] S. Misra, K. Barik, and K. Petter, "Digital Sovereignty in the Era of Industry 5.0: Challenges and Opportunities", in Procedia Computer Science. 254. 108-117, 2025. DOI: 10.1016/j.procs.2025.02.069.

[4] N. R. Nodehi, F. Berisha, L. Da Silva, Z. Pourzolfaghar and M. Helfert, "Integrating Cybersecurity, Data Sovereignty and Trustworthiness in Agri-data Sharing Environments: A Conceptual Framework," *2024 Cyber Research Conference - Ireland (Cyber-RCI)*, Carlow, Ireland, 2024, pp. 1-8, doi: 10.1109/Cyber-RCI60769.2024.10939388.

[5] E. Sorrentino and A. F. Spagnuolo, "Cybersecurity e sovranità digitale nella protezione dei dati personali," In Rivista Italiana di Informatica e Diritto, Year 6, N. 2, 2024. Available: https://www.rivistaitalianadiinformaticaediritto.it/index.php/RIID/article/download/291/228/54.

[6] S.K. Khan, N. Shiwakoti, P. Stasinopoulos and M. Warren, "Cybersecurity regulatory challenges for connected and automated vehicles – State-of-the-art and future directions," In Transport Policy 143 (2023) 58–71. DOI: 10.1016/j.tranpol.2023.09.001. Available: https://www.sciencedirect.com/science/article/pii/S0967070X23002330?via%3Dihub.

[7] European Commission. *Digital Sovereignty in the European Union: Challenges and Strategies.* European Commission Report, 2024.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[9] International Organization for Standardization, Society of Automotive Engineers, ISO/SAE 21434:2021, Road Vehicles – Cybersecurity Engineering, 2021.

[10] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive).

[11] G. Gobber, "Breve nota sulla doppia natura linguistica e logico-semantica dei termini nelle scienze," In proceedings of "Terminologie specialistiche e tipologie testuali (Milano, 26-27 maggio 2006), eds. M. T. Zangola, Milano, ISU, 2007, p. 31.

[12] M. T. Cabrè L. Codina and R. Estopà (eds.), Terminologia i Documentacio. I Jornada de terminologia i documentacio, Barcellona: IULA, Pompeu Fabra University, 2001.

[13] F. Oberti, F. Abrate, A. Savino, F. Parisi and S. Di Carlo, Navigating the road to automotive cybersecurity compliance. In Proceedings of 30th International Symposium on On-Line Testing and Robust System Design (IOLTS) 2024, IEEE, pp. 1-4, DOI: 10.1109/IOLTS60994.2024.10616052.

[14] G. Costantino, M. De Vincenzi and I. Matteucci, "In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards," in *I*EEE Communications Standards Magazin*e*, vol. 6, no. 1, pp. 84-92, March 2022, doi: 10.1109/MCOMSTD.0001.2100080.

[15] E. Cardillo, A. Portaro and M. Tavernit, "Combining Knowledge graph and LLM to extract thesaural relationship and concepts on Cybersecurity," in Proceedings of the 16th International Conference on Advances in Social Networks Analysis and Mining - ASONAM 2024 Volume 1, 2025 (in press).

[16] International Standard Organization, "ISO 25964-1:2011 Information and documentation - Thesauri and interoperability with other vocabularies — Part 1. Thesauri for information retrieval", August 2011.

[17] C. Lanza, Semantic control for the Cybersecurity domain: Investigation on the representativeness of a domain-specific terminology referring to lexical variation. CRC Press, 2022.

[18] P. Casanovas, M. Hashmi and L. de Koker, L., "The Rule of Law and Compliance: Legal Quadrant and Conceptual Clustering" In: Rodríguez-Doncel, V., Palmirani, M., Araszkiewicz, M., Casanovas, P., Pagallo, U., Sartor, G. (eds) AI Approaches to the Complexity of Legal Systems XI-XII. AICOL AICOL XAILA 2020 2018 2020. Lecture Notes in Computer Science(), vol 13048. Springer, Cham. 2021, DOI: 10.1007/978-3-030-89811-3_15.

[19] P. Timmers, M. Punter, C. Stolwijk, Cybersecurity and Digital sovereignty - Bridging the gaps, Whitepaper, TNO Innovation for life. 2024. Available: https://publications.tno.nl/publication/34643188/DvSKsfCM/timmers-2024-cybersecurity.pdf.