Finansuoja Europos Sąjunga
NextGenerationEU

Mykolo Romerio universitetas

NAUJOS KARTOS LIETUVA

Project „Misijomis grįstų mokslo ir inovacijų programų įgyvendinimas“ (Project Nr. 02-002-P-0001) report

Project name: ***EPMwDC***

Responsible/Implementation partner (-s): ***MRU***

Action result: ***Literature Review: Privacy and Cybersecurity Issues in AI-Powered Dual-Use Surveillance Systems***

Table of contents

1. Introduction

Artificial intelligence systems are increasingly embedded in socio-technical infrastructures spanning transport, healthcare, public administration, finance, and defence. As these systems grow more autonomous, adaptive, and scalable, the regulatory environment governing their development and deployment has expanded in both scope and complexity. This literature review examines the current state of knowledge regarding privacy and cybersecurity issues arising from the development of AI-powered dual-use systems, systems developed for civilian markets that may also be deployed in military or security contexts.

The review is structured as follows. Section 2 introduces AI systems and their development lifecycle as defined by EU and international standards. Section 3 surveys the regulatory landscape applicable to dual-use AI systems, covering EU-level legislation, national frameworks, defence-specific governance instruments, and international humanitarian law. Section 4 examines the AI Act's risk classification scheme as it applies to dual-use contexts. Section 5 reviews current practices in regulatory compliance, including recent EU and NATO policy guidance and emerging case law from the Court of Justice of the European Union (CJEU). Section 6 surveys the state of the art in automating regulatory compliance, with particular attention to ontology-based approaches. Section 7 provides a dedicated synthesis of privacy and cybersecurity issues that cut across the preceding sections. Section 8 concludes with a summary of identified gaps and directions for future research.

This review draws upon and extends the analysis presented in Sabaliauskaite et al. (2026), supplemented by additional sources from the regulatory, policy, and technical literature.

The evidence base was extended through a structured supplementary search of the Web of Science Core Collection, covering publications indexed for 2025 and 2026. Three Boolean queries were run: the first targeted ontology and knowledge-graph work on regulatory compliance for AI and dual-use systems; the second targeted privacy-by-design and security-by-design work on AI governance; the third targeted SHACL, SPARQL, RDF, and OWL work on legal and regulatory requirements.

Primary search: TS=(("ontology" OR "knowledge graph" OR "semantic web") AND ("regulatory compliance" OR "AI Act" OR "GDPR" OR "NIS2" OR "cybersecurity") AND ("dual-use" OR "artificial intelligence" OR "AI system")) AND PY=(2025 OR 2026). Result: 20 records.

Supplementary search 1: TS=(("privacy by design" OR "security by design") AND ("artificial intelligence" OR "AI" OR "machine learning") AND ("compliance" OR "regulation" OR "governance")) AND PY=(2025 OR 2026). Result: 42 records.

Supplementary search 2: TS=(("SHACL" OR "SPARQL" OR "RDF" OR "OWL") AND ("compliance" OR "regulatory" OR "legal requirements")) AND PY=(2025 OR 2026). Result: 53 records.

After removing 2 overlapping records, 110 unique entries remained. These were triaged by title and abstract into directly relevant, tangentially relevant, and out-of-scope categories. A large share of the third query's results were false positives, where the search terms matched unrelated domains: RDF as refuse-derived fuel or radial distribution function, OWL as an avian species, and SHACL or SPARQL in building information modelling. These were excluded. Twenty-four publications were classified as directly relevant; they are integrated into the relevant sections below, and the full retrieved corpus is listed in the supplementary search bibliography. One of the twenty-four, Topalli and Badii (2025), is already cited in the main review.

2. AI systems and the development lifecycle

The European Commission's 2025 Guidelines define an AI system as a machine-based system designed to operate with varying degrees of autonomy, potentially exhibiting adaptiveness after deployment, and capable of generating outputs such as predictions, content, recommendations, or decisions that influence

physical or virtual environments (European Commission, 2025a). This definition encompasses seven core elements: machine-based architecture (hardware and software), autonomy from human involvement, adaptiveness through self-learning, explicit or implicit objectives, output generation from inputs, the capacity to influence environments, and active interaction with those environments.

The development lifecycle of AI systems, as specified by ISO/IEC 22989 (ISO/IEC, 2022), comprises seven phases: inception, design and development, verification and validation, deployment, operation and monitoring, re-evaluation, and retirement. These are commonly grouped into a pre-deployment ("building") phase (stages 1–3) and a post-deployment ("use") phase (stages 4-7) (European Commission, 2025a). This lifecycle decomposition is significant for regulatory compliance because different obligations attach to different phases, privacy-by-design obligations, for instance, principally govern the design and development phase, while operational cybersecurity obligations apply to deployment and maintenance.

AI systems are frequently integrated into broader software ecosystems with comparable lifecycle models encompassing requirements analysis, system design, development and implementation, testing, deployment, maintenance, and decommissioning (ENISA, 2019). Understanding this lifecycle structure is essential for mapping regulatory requirements to concrete engineering decisions, particularly in dual-use contexts where civilian and defence deployments may diverge at the operational phase while sharing a common design foundation.

3. The regulatory landscape for dual-use AI systems

3.1 EU-level regulation

The EU's digital regulatory ecosystem has expanded rapidly in recent years, creating a complex web of overlapping obligations for developers and deployers of AI systems.

The AI Act. Adopted in June 2024, the EU AI Act (European Commission, 2024a) is the first comprehensive regulatory framework for AI globally. It imposes obligations on AI providers and deployers categorised by risk level: unacceptable risk, high risk, limited risk, and minimal risk. For high-risk systems, obligations include risk management systems (Art. 9), data governance measures (Art. 10), technical documentation (Art. 11), logging capabilities (Art. 12), transparency and information provision (Art. 13), human oversight (Art. 14), and accuracy, robustness, and cybersecurity requirements (Art. 15). Art. 2(3) excludes AI systems used exclusively for military, defence, or national security purposes, a narrow exemption whose implications for dual-use systems are discussed in Section 4.

GDPR. The General Data Protection Regulation (European Commission, 2016a) applies whenever an AI system processes personal data wholly or partly by automated means, which effectively encompasses most AI systems. GDPR establishes principles of data minimisation and storage limitation, requires a Data Protection Impact Assessment (DPIA) for processing likely to pose high risks to individuals (Art. 35), mandates data protection by design and by default (Art. 25), and imposes security-of-processing obligations (Art. 32). Like the AI Act, GDPR contains exclusions for common foreign and security policy (Art. 2(2)(b)) and for law enforcement processing (Art. 2(2)(d)), the latter being governed instead by the Law Enforcement Directive (European Commission, 2016b).

NIS2 Directive. The NIS2 Directive (European Commission, 2022a) strengthens EU cyber resilience by imposing management and technical cybersecurity requirements on critical infrastructure entities operating in designated sectors. While AI system providers are not always classified as cybersecurity subjects under NIS2, supply chain obligations may extend compliance requirements to them. NIS2's cybersecurity risk management measures (Art. 21) are particularly relevant for AI systems that transmit or process sensitive data.

Cyber Resilience Act (CRA). The CRA (European Commission, 2024b) applies to products with digital elements made available on the EU market whose intended or foreseeable use involves a logical or physical

data connection to a device or network (Art. 2(1)). However, products developed exclusively for national security or defence purposes, or designed to process classified information, are exempt (Art. 2(7)).

Dual Use Regulation. Regulation (EU) 2021/821 (European Commission, 2021a) defines dual-use items as goods, software, and technology that can serve both civil and military purposes and establishes a Union-wide framework for controlling their export, brokering, technical assistance, transit, and transfer.

Other relevant instruments. Additional legislative instruments that may affect AI systems depending on context include the Digital Services Act, the Digital Markets Act, the Directive on Copyright and Related Rights in the Digital Single Market (European Commission, 2019), and, for the financial sector, the Digital Operational Resilience Act (DORA) (European Commission, 2022c). The European Parliament (2025) has examined the interplay between the AI Act and this broader digital legislative framework, highlighting the cumulative compliance burden that results.

3.2 National legislation

EU directives such as NIS2 require transposition into national law. Lithuania, for example, has transposed NIS2 through its Cybersecurity Law (Lietuvos Respublikos Seimas, 2024). Member States also frequently adopt supplementary data protection laws introducing additional requirements beyond GDPR, and establish their own rules for personal data processed for national security purposes. Lithuania's Law on the Legal Protection of Personal Data Processed for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences, the Execution of Sentences or National Security or Defence (Lietuvos Respublikos Seimas, 2011) implements the Law Enforcement Directive while also setting additional rules for defence and national security data processing, including DPIA obligations (Art. 25).

3.3 Defence governance frameworks

As the EU lacks exclusive competence in defence regulation, frameworks governing AI in this domain are established at the national level and through alliance-level governance instruments.

NATO policy and governance. NATO's AI Strategy, adopted in 2021 and revised in 2024, emphasises reliable implementation of AI within NATO structures while adhering to principles of lawfulness, responsibility, accountability, explainability, traceability, reliability, governability, and bias mitigation (NATO, 2024a). The Data Strategy for the Alliance (NATO, 2025) emphasises the transition to a data-centric organisation implementing security-by-design and privacy-by-design principles, referencing modern standards such as STANAG 5636 for semantic interoperability (NATO, 2022). NATO's Digital Transformation Implementation Strategy (NATO, 2024b) underscores the requirement for interoperability across domains and the integration of cybersecurity and cyber defence practices into operational environments.

NATO accreditation frameworks. AI-enabled systems deployed in NATO environments are subject to security accreditation requirements defined by the NATO Information Assurance Policy (NIAP), the NATO Security Policy (NSP), and the NATO Cyber Defence Policy. These instruments establish mandatory requirements for encryption, access management, incident reporting, secure data exchange, and personnel vetting. Compliance in defence contexts is principally achieved through accreditation processes and security authorisation rather than through conformity assessment under EU market legislation. For dual-use systems, this creates a layered compliance environment: EU regulatory obligations apply where the system is placed on the EU market or processes personal data within EU jurisdiction, while NATO accreditation requirements apply where the system is deployed within Alliance-controlled infrastructures.

International humanitarian law (IHL). The development and applicability of AI technologies in armed conflict is governed by IHL, principally the four Geneva Conventions of 1949 and their Additional Protocols (ICRC, 2026a) and customary international humanitarian law (ICRC, 2026b). The International Committee of the Red Cross (ICRC) has highlighted AI integration in weapon systems, cyber and information operations, and military decision support systems as areas raising significant legal questions (ICRC, 2023). The ICRC's

position is that human combatants must retain responsibility for actions in warfare and that AI system design must ensure IHL compliance from inception (ICRC, 2021).

Fundamental rights. AI development and deployment, including for military purposes, must respect fundamental rights established in the European Convention on Human Rights (European Court of Human Rights, 1950), the Charter of Fundamental Rights of the EU (European Commission, 2012), and national constitutions.

3.4 The compliance matrix for dual-use AI

Taken together, the regulatory landscape requires that prior to development, it is essential to define: (a) the intended end user, (b) the categories of data the system will process, (c) the system's primary purpose, and (d) the geographical location of development and deployment. A comprehensive compliance matrix can then be developed, enabling the identification and resolution of potential regulatory conflicts. Legal scholarship increasingly recognises that in practice, the exemptions included in regulations such as the GDPR and AI Act for defence-related processing are rarely clean-cut, given that governments and militaries frequently rely on private companies to develop AI. Dual-use AI systems may therefore remain subject to GDPR/LED and the AI Act for non-military use-case scenarios, with only a narrow category of in-house defence or national security processing being purely exempt (Powell, 2024; Vogiatzoglou, 2024; Juric, 2024).

4. AI Act risk classification in dual-use contexts

The regulatory classification of AI systems under the AI Act depends primarily on intended purpose and deployment context. Under Article 6, an AI system is classified as high-risk where it is either intended to be used as a safety component of a product subject to third-party conformity assessment under Union harmonisation legislation, or listed in Annex III. Annex III categories relevant to surveillance and security applications include biometric identification and categorisation of natural persons, management and operation of critical infrastructure, law enforcement, migration and border control, and access to essential public and private services.

For dual-use systems, classification requires careful distinction between civilian market placement and defence-only application. A system that detects unauthorised photography attempts without performing identity recognition may not automatically fall within the biometric identification category, classification depends on functional scope rather than technological capability alone. Providers must also assess whether the system falls within the AI Act's list of prohibited practices under Article 5, which includes specific forms of remote biometric identification in publicly accessible spaces.

The Art. 2(3) exemption for exclusively military, defence, or national security purposes is narrow. Where a system is placed on the EU market for civilian use, even if technically capable of defence deployment, the AI Act applies to that civilian deployment. Providers of dual-use systems must therefore design compliance mechanisms that accommodate both regulated civilian contexts and defence accreditation environments simultaneously.

The AI Act's standardisation framework is itself a significant challenge. CEN-CENELEC JTC 21 is developing approximately 35 technical standards to support AI Act implementation (Kilian et al., 2025). The standardisation landscape is characterised by an overwhelming volume and fragmentation of relevant standards, high compliance costs, and limited participation of start-ups and SMEs in standardisation processes (Kilian et al., 2025).

5. Current practices in regulatory compliance

5.1 EU policy guidance

Several EU policy instruments address the dual-use dimension of AI and emerging technologies. The Action Plan on Synergies between Civil, Defence and Space Industries (European Commission, 2021b) promotes the use of dual-use technologies for both commercial and military applications. The Commission's Roadmap on Critical Technologies for Security and Defence (European Commission, 2022b) defines a strategic framework for EU technological sovereignty. The European Defence Industrial Strategy (European Parliament, 2024) promotes integrating civilian innovation into the defence sector.

More recently, the Commission Guidelines on Prohibited AI Practices (European Commission, 2025b) clarify that unacceptable-risk practices must be removed from AI technologies intended for dissemination in the EU, whether in civilian or dual-use domains.

A significant policy contribution is the European Policy Centre report arguing that traditional dual-use classifications are no longer adequate (Kremidas-Courtney, 2025). The report proposes a shift toward "omni-use by design" in research and innovation frameworks, recognising that advanced technologies increasingly operate simultaneously across defence, health, industry, and other domains. This analysis is supported by research exploring AI's dual offensive-defensive role in maritime cybersecurity (Cichocki, 2025) and by recent work examining safety and cybersecurity under emerging EU legislation through industry use-case perspectives (Ndiaye et al., 2026).

5.2 CJEU case law

Emerging case law from the CJEU is establishing important precedents for AI systems that process personal data across civilian and security domains.

In *La Quadrature du Net* (CJEU Case C-511/18, 2020), the Court ruled that Member States cannot invoke national security to mandate blanket mass data retention, while establishing a narrow exception permitting temporary general retention only in the face of a genuine, present, or foreseeable serious threat, subject to strict time limits and effective judicial or independent review. This ruling constrains the ability of governments to reclassify civilian AI surveillance tools as national security instruments to bypass EU regulation.

In Ligue des droits humains (CJEU Case C-817/19, 2022), the Court emphasised that automated processing systems must employ reliable, non-discriminatory criteria and human review, setting a judicial standard for the "human oversight" and "human in the loop" requirements that the AI Act subsequently codified.

In *SCHUFA Holding AG* (CJEU Case C-634/21, 2023), the Court clarified that organisations providing automated risk-based scores are subject to the strict requirements of GDPR Article 22, under which automated decisions with significant effects are generally prohibited unless necessary for a contract or authorised by law.

In *Dun & Bradstreet Austria GmbH* (CJEU Case C-203/22, 2025), the Court established that individuals have a right to know the logic involved in automated decisions, with direct implications for providers of high-risk dual-use AI systems.

Collectively, these rulings confirm that regardless of the deployment domain, AI-enabled technologies must not exceed the limits set by the AI Act and GDPR, a position reinforced by both policy documents and emerging jurisprudence.

5.3 NATO best practices

NATO's strategic documents reflect a significant shift toward AI governance, emphasising responsible AI certification standards, continuous monitoring of technology trends, and increased cooperation with the EU on AI safety and accreditation. The NATO AI Strategy requires that all technologies applied in NATO or dual-use contexts ensure security-by-design principles and confirm compliance with international law before deployment. The Data Strategy for the Alliance operationalises this through a Data Centric Reference Architecture and compliance with approved NATO data protection policies. The Digital Transformation

Implementation Strategy requires that data-driven decision-making across the Alliance possess interoperability across domains, supported by consistent governance frameworks.

6. Automating regulatory compliance: state of the art

6.1 Persistent challenges

A recent systematic mapping study on requirements engineering for regulatory compliance in software systems (Kosenkov et al., 2025), reviewing 280 publications, identified numerous persistent challenges: the abstract nature of regulations, conflicts with existing practices, the need for new expertise, the lack of established principles and methods, regulatory complexity, resource demands, enforcement difficulties, evolving system dynamics, overlapping regulatory frameworks, organisational barriers, and regulatory gaps. Ninety-one per cent of the reviewed publications reported at least one of these challenges. The interpretation and application of regulatory frameworks remains heavily dependent on specialised legal expertise (Elahidoost, 2024).

6.2 Generative AI for compliance

Generative AI has been identified as having potential to improve regulatory compliance (Imperial et al., 2025). However, significant barriers persist: overlapping regulatory frameworks, regulatory gaps, conflicts with existing practices, questions of liability and accountability regarding misinterpretations or incomplete outputs, the need for continuous model retraining to track regulatory updates, and the continued requirement for substantial domain expertise. Current standards and regulations are not yet fully aligned with GenAI capabilities.

6.3 Ontology-based approaches

The first step toward automating compliance is the abstraction and formal structuring of legal provisions into machine-interpretable representations (Abualhaija et al., 2025). Ontologies, formal specifications of conceptualisations that define concepts, relationships, and constraints, provide a rigorous foundation for this. Their reliance on strict logical formalisms enables automated validation of knowledge consistency and semantic reasoning to derive new insights, while their abstraction from implementation details supports interoperability across heterogeneous systems.

Ontology-based Requirements Engineering (ObRE) is emerging as a promising pathway for regulatory compliance automation (Amaral et al., 2021; Guizzardi et al., 2023). Recent examples include:

- Hosseini et al. (2025) proposed an ontological framework for security-by-design of industrial control systems conforming to IEC 62443.
- Hernandez et al. (2024) introduced the Trustworthy AI Requirements (TAIR) ontology, providing a basis for mapping AI Act concepts and requirements.
- Guizzardi et al. (2023) proposed an ontological approach for specifying "ethicality requirements" for AI systems.
- Paskauskas (2025) developed an ontology for 5G network security ensuring compliance with EU cybersecurity requirements, employing SHACL constraints and logical reasoners such as HermiT.
- Orlando & Santoro (2025) proposed a framework integrating natural language processing with semantic and topic modelling techniques for automated analysis of GDPR enforcement decisions.

Publications indexed in 2025 and 2026 confirm rapid growth in ontology-based regulatory compliance and extend the examples above. Several research groups have formalised specific regulatory instruments as machine-readable ontologies.

Castiglione et al. (2025) present NIS2Onto, an OWL ontology that translates the NIS2 Directive into an ontological format for cybersecurity professionals and legal experts, supporting automated compliance

verification and risk assessment. It complements the EPMwDC framework's treatment of NIS2 requirements and shows independent convergence on ontology-based approaches to the same instrument.

Turaga et al. (2025) propose CO2 (Co-Compliance Officer), an LLM-based method for generating knowledge graphs from legal documents, specifically the EU AI Act, using named-entity recognition and dependency parsing to extract regulatory triplets. It offers an NLP-driven alternative to the expert-driven ontology engineering used in the EPMwDC framework.

Ahmed et al. (2026) introduce an automated AI Act compliance evaluation method for health data spaces, using NLP to extract compliance information from system documentation and feed it into a compliance knowledge graph for automated gap detection.

Oranekwu et al. (2026) present a scalable ontology-driven framework for IoT cybersecurity compliance that combines SWRL, SPARQL, OWL, LLMs, and retrieval-augmented generation to assess compliance against NISTIR 8259, with a knowledge graph populated from more than 800 manufacturer privacy-policy instances.

Gallina et al. (2026) propose an ontology-based representation for regulatory compliance-aware system change management in the automotive domain, using SHACL constraints to validate configurations against safety and cybersecurity regulations, which shows the applicability of ontology-based compliance beyond the AI domain.

Corazza et al. (2025) develop a hybrid AI approach for detecting and tracking reporting requests in EU legislation, converting extracted legal knowledge into RDF knowledge graphs, relevant to the problem of tracking evolving regulatory obligations.

Schubert et al. (2025) present an ontology-based automation framework for continuous compliance of airborne software, integrated with CI/CD environments and storing lifecycle artefacts in a unified knowledge graph for automated checks.

Montecchiari (2026) validates enterprise architecture principles using SHACL constraints and SPARQL queries over ontology-based representations of ArchiMate models, with explainable violation reports.

Baimuratov and Turygin (2025) argue for modelling normative regulations in OWL DL rather than SHACL, on the grounds that OWL DL offers more human-readable syntax, decidable semantics, and the ability to detect redundant or inconsistent regulations through reasoning. This is a methodological alternative to the SHACL-based validation used in the EPMwDC framework.

On the technical foundations of semantic validation, three further studies are relevant. Ke (2025) addresses the efficiency of semantic-aware SHACL validation when implicit information encoded in the ontology must be considered, relevant to scaling the framework to larger regulatory ontologies. Tauqeer et al. (2026) present an integrated approach to GDPR-compliant data sharing using consent, contracts, and licences, with SHACL validation for compliance checks and SHACL repairs to fix data inconsistencies automatically, extending SHACL from validation to remediation. Han (2025) proposes AIRPoC, a blockchain consensus framework integrating AI legal agents with SPARQL-based inference for real-time GDPR compliance validation, reporting 88.9% compliance accuracy.

A related strand applies ontologies to AI risk management and ethics. Ikhsan (2026) presents an ontology-driven AI risk management framework using RDF that incorporates fairness, transparency, and accountability and supports automated querying, compliance tracking, and cross-domain governance, relevant to the framework's treatment of AI Act requirements. Sharma et al. (2025) propose a modular ethical assessment framework built on ontological blocks of meaning and integrated with FAIR principles, supporting EU AI Act compliance. Kioskli et al. (2025) introduce trustSense, a framework and tool for evaluating human-oversight maturity in AI governance, drawing on trustworthy AI, cybersecurity readiness, and privacy-by-design, relevant to the human-oversight requirement of AI Act Article 14.

6.4 Limitations of existing frameworks

The major limitations of currently available ontological frameworks for regulatory compliance are twofold:

1. *Limited scope:* existing frameworks typically address single standards or regulations and do not model the cumulative interaction of multiple overlapping instruments.
2. *Insufficient for dual-use:* no prior framework explicitly addresses the needs of systems deployable across civilian and defence domains, where compliance obligations are additive rather than substitutive and where the governing instruments differ fundamentally in normative status (binding EU legislation vs. NATO governance and accreditation frameworks).

6.5 Adjacent technical contributions

Several adjacent research streams address technical dimensions relevant to privacy and cybersecurity in dual-use AI systems:

- Semantic interoperability in multi-cloud environments, including federated-fog computing approaches to mitigate latency and optimise resources for real-time IoT applications (Huaranga-Junco et al., 2024; Brabra et al., 2016).
- Security architectures for next-generation networks, including the Smart Service-based Security Architecture (ES3A) for 6G (Duan et al., 2025) and edge-cloud IoT frameworks for real-time privacy-preserving analytics (Xia, 2025).
- Decentralised compliance approaches using Blockchain Hyperledger and Federated Learning for privacy-preserving financial and security compliance (Khan et al., 2025).
- Context-aware privacy protection frameworks employing Re-Identifiability Indices (RII) for real-time optimisation of multimedia data privacy within multimodal AI systems (Topalli & Badii, 2025).
- Deepfake and biometric security techniques relevant to the integrity of visual monitoring systems (Pn et al., 2024).
- Scene interpretation frameworks using ontology-based context representation for video-based object tracking (Gómez-Romero et al., 2011).

7. Synthesis: privacy and cybersecurity issues

This section draws together the privacy and cybersecurity threads that run through the preceding sections, organised around the key issues that developers of dual-use AI surveillance systems must address.

7.1 Privacy issues

Data protection by design and by default. Both EU regulation (GDPR Art. 25) and NATO governance frameworks require that privacy safeguards be embedded into system architecture from inception. For AI-powered surveillance systems, this means that image capture design must be governed by data minimisation principles, the system should capture only what is essential for security verification, avoiding unnecessary recording of bystander activity or facial features. Retention periods must be defined during the design phase, not as a post-deployment afterthought.

Data Protection Impact Assessments. DPIA obligations arise under GDPR (Art. 35) for civilian deployments and under national legislation (e.g., Lithuanian law, Art. 25) for defence-related processing. The DPIA is a universal entry point for compliance in both domains, even though the legal basis differs. For dual-use systems, this means DPIAs must be conducted for each intended deployment context.

Data subject rights. In civilian deployments, GDPR mandates rights of access (Art. 15), erasure (Art. 17), and restriction (Art. 18). Transparency notices are required in deployment locations informing individuals of

monitoring. In defence contexts, these rights may be limited, but they are not automatically extinguished, and the scope of any limitation must be legally justified.

Re-identifiability and privacy obfuscation. Recent research has demonstrated that semantic reasoning is required to distinguish legitimate mobile phone use from actual espionage in monitored environments. The integration of a Re-Identifiability Index (RII) can mitigate identity leakage during visual monitoring, ensuring that only the threat is processed while preserving bystander privacy through adaptive obfuscation (Topalli & Badii, 2025). This is a technical operationalisation of the privacy-by-design principle.

Breach notification. Personal data breaches must be reported to supervisory authorities within 72 hours under GDPR (Art. 33), with high-risk breaches requiring communication to affected data subjects (Art. 34). In defence contexts, incident reporting follows different channels, secure, encrypted communications to NATO entities, but the underlying obligation to detect and report breaches is common across domains.

GDPR scope exemptions and their limits. While GDPR Art. 2(2) excludes certain processing activities (common foreign and security policy, law enforcement), the practical applicability of these exemptions for dual-use systems is narrow. Legal scholarship increasingly recognises that governments' and militaries' reliance on private-sector AI developers means that most dual-use systems remain subject to GDPR and/or the Law Enforcement Directive. Only a narrow category of purely in-house defence processing may fall outside EU data protection law (Powell, 2024; Vogiatzoglou, 2024; Juric, 2024). CJEU case law, particularly La Quadrature du Net, constrains the ability to invoke national security as a blanket exemption.

Recent work indexed in 2025 and 2026 sharpens the privacy-by-design and GDPR analysis for AI systems and reinforces the points above. Campillo (2025) examines privacy-by-design as a requirement for police AI, analysing phases and requirements for users, deployers, and developers under the Police Directive and the AI Act, directly relevant to the law-enforcement dimension of dual-use deployment. Feretzakis et al. (2025) analyse the technical and legal obstacles to reconciling large language model design with GDPR, proposing a four-layer governance framework covering data governance, technical privacy enhancements, continuous compliance monitoring, and explainability.

Chemlali and Benseddik (2025) examine the relationship between privacy-by-design and Emotion AI within the GDPR and the AI Act, including CJEU and ECtHR jurisprudence, extending the analysis to affective computing. Medina (2025) explores regulatory harmonisation between the GDPR and the AI Act in the EU and Spain, addressing privacy-by-design and the risk of overregulation. Ozparlak and Metin (2025) examine the role of legal design in AI Act compliance, analysing how human-centred design can strengthen privacy-by-design, AI literacy, informed consent, and transparency. Korchenko et al. (2026) propose a regulatory and technical mapping that implements GDPR and NIS2 across the lifecycle of environmental data, from reception and transport through storage, analytics, sharing, and publication, including a DPIA checklist, a lifecycle-based approach analogous to the EPMwDC methodology.

The context-aware framework of Topalli and Badii (2025), already discussed above, belongs to this cluster: it integrates a Re-Identifiability Index to preserve privacy in real time within multimodal AI systems.

7.2 Cybersecurity issues

Security-by-design. Both GDPR (Art. 32) and NIS2 (Art. 21) require that security measures be built into systems from the outset. For AI surveillance systems, this encompasses encryption architecture, secure communication protocols for data transmission, hardened firmware, secure boot mechanisms, and access control frameworks. In NATO contexts, these requirements are supplemented by NIAP and NSP standards mandating NATO-approved cryptographic modules, physical security requirements, personnel security clearances, and, in some cases, TEMPEST certification for electromagnetic emissions security.

Operational cybersecurity. Post-deployment cybersecurity obligations include encrypted data transmission for all communications, access controls restricting data to authorised personnel, comprehensive audit logging, documented and tested incident response procedures, vulnerability management, patch deployment processes, and regular security assessments and penetration testing. For

defence deployments, additional obligations include sharing threat intelligence across NATO entities (per the NATO Cyber Defence Policy) and deploying detection mechanisms to prevent unauthorised data capture via non-networked means.

5G network security. Where AI systems rely on 5G for data transmission (as in the remote notification link to monitoring stations), network-level security becomes a critical concern. Research has demonstrated the value of ontology-based approaches to 5G security compliance, employing SHACL constraints and logical reasoners to validate system configurations against regulatory requirements (Paskauskas, 2025). Hybrid ANN-ISM modelling has been used to identify security interdependencies in 5G network architectures (Khan et al., 2025).

Divergent security frameworks across domains. A fundamental challenge for dual-use systems is that security-related requirements are sourced from different regulatory frameworks depending on the deployment context. Civilian deployments rely on GDPR Art. 32 and NIS2 Art. 21 (commercial encryption standards such as TLS/AES); defence deployments require NATO-approved cryptography, personnel vetting, and accreditation under NIAP/NSP. The compliance burden is additive: defence deployments must satisfy all applicable civilian requirements *as well as* NATO-specific obligations. This divergence means a single set of security controls cannot serve both contexts; the system architecture must support configurable security profiles.

Supply chain cybersecurity. The CRA and NIS2 supply chain obligations may extend cybersecurity requirements to AI system providers who are not themselves classified as critical infrastructure entities. For dual-use systems incorporating commercial off-the-shelf components, this introduces additional compliance layers.

Emerging threats and evolving architectures. The transition to 6G networks, edge-cloud computing, and federated learning introduces new security considerations. Research on agile service-based security architectures for 6G (Duan et al., 2025), privacy-preserving edge-cloud IoT analytics (Xia, 2025), and decentralised compliance approaches using blockchain and federated learning (Khan et al., 2025) points to the evolving technical landscape that compliance frameworks must accommodate.

Two further 2025 studies address cybersecurity compliance and threat intelligence relevant to dual-use systems. Mpatziakas et al. (2025) present an LLM-based application for simplified cybersecurity compliance in Industry 4.0, addressing IEC 62443 and related standards for industrial IoT, relevant to the security-by-design dimension. Roothaert et al. (2025) introduce TIDO (Threat Intelligence Decision Ontology), an OWL-based ontology for capturing decision-making within strict legal and policy frameworks in national intelligence agencies, validated with competency questions from the Dutch Defence Intelligence and Security Service, directly relevant to the defence domain.

7.3 Cross-cutting issues

The additive compliance burden. The single most important structural finding for dual-use systems is that defence compliance adds to civilian obligations rather than replacing them. EU market placement obligations operate alongside defence accreditation requirements, subject to applicable (but narrow) exemptions. This cumulative model means that prototype developers must design for the most stringent requirement set and enable civilian deployment as a subset configuration.

Regulatory fragmentation and interpretative burden. EU regulations, sector-specific standards (e.g., IEC 61508, ISA/IEC 62443), and defence frameworks differ considerably in scope, language, and application level, creating both regulatory and technical gaps (Ndiaye et al., 2026). AI system developers must navigate ambiguous interactions among multiple digital laws, in which concepts such as risk, accountability, transparency, and security are defined differently across instruments. This interpretative burden is disproportionately heavy for SMEs and start-ups.

The gap between legal norms and technical specifications. A persistent challenge across both the privacy and cybersecurity domains is translating abstract legal requirements into actionable, system-level

specifications. Ontology-based approaches offer a pathway to bridge this gap by formalising regulatory obligations as machine-readable, queryable entities linked to specific system components, lifecycle phases, and deployment contexts (Sabaliauskaite et al., 2026).

8. Conclusions and identified gaps

This review has surveyed the regulatory, policy, and technical landscape governing privacy and cybersecurity in AI-powered dual-use surveillance systems. The following gaps and directions for future research are identified:

1. *Integrated multi-regulatory compliance frameworks.* Existing ontological approaches typically address single regulations. Frameworks capable of modelling the cumulative interaction of GDPR, NIS2, the AI Act, the CRA, and defence governance instruments within a unified knowledge representation remain underdeveloped.
2. *Dual-use compliance methodology.* No prior work provides a systematic, validated methodology for specifying compliance requirements across civilian and defence deployment domains for the same technology, maintaining traceability between legal obligations and technical system components.
3. *Dynamic regulatory tracking***.** Current compliance representations are largely static. As the AI Act's implementing standards are developed by CEN-CENELEC JTC 21 and as CJEU case law evolves, mechanisms for ontology versioning and automated update propagation are needed.
4. *Scalable validation.* While SHACL constraints and logical reasoners have been demonstrated for specific domains (e.g., 5G security), their application to comprehensive dual-use compliance validation at article and paragraph granularity has not been fully explored.
5. *Privacy-preserving AI for surveillance.* The integration of context-aware privacy frameworks (e.g., Re-Identifiability Indices) into the design of AI surveillance systems represents a promising but nascent research direction for operationalising privacy-by-design in dual-use contexts.
6. Empirical validation. Most existing frameworks have been validated through structural queries and case studies. Validation with legal experts, compliance officers, and certification bodies, and across multiple dual-use technology types, remains an open need.

The supplementary search for 2025 and 2026 confirms several of the trends identified above and points to emerging directions.

Convergence on ontology-based compliance. Multiple independent groups are building OWL/RDF ontologies for regulatory compliance across NIS2, the AI Act, GDPR, IoT cybersecurity, and automotive safety. This validates the framework's foundational approach and shows how fragmented and domain-specific current efforts remain.

SHACL as a validation mechanism. SHACL is increasingly used not only for structural validation but for automated compliance checking and automated remediation through SHACL repairs. The efficiency of semantic-aware SHACL validation remains an open research problem.

LLM-augmented knowledge graph construction. Several studies use LLMs and NLP to speed up extraction of regulatory knowledge from legal text into ontologies, although reliability, transparency, and liability concerns persist, consistent with the limitations noted by Imperial et al. (2025).

Lifecycle-based compliance mapping. The approach of mapping regulatory requirements to lifecycle phases recurs in recent work on environmental data (Korchenko et al., 2026), continuous software compliance (Schubert et al., 2025), and automotive change management (Gallina et al., 2026).

Privacy-by-design operationalisation. Research continues to move from abstract principles toward concrete implementations, including context-aware privacy frameworks (Topalli and Badii, 2025),

governance frameworks for large language models (Feretzakis et al., 2025), and lifecycle data-protection mappings (Korchenko et al., 2026).

Defence and intelligence domain. The TIDO ontology (Roothaert et al., 2025) is a rare example of ontology-based decision support in defence intelligence, validated with a national service, complementing the framework's NATO compliance modelling.

No integrated dual-use framework. Across all results, no 2025 or 2026 publication presents an integrated ontology-based framework for dual-use AI regulatory compliance spanning both civilian EU instruments and defence governance, which confirms the novelty of the EPMwDC contribution.

These supplementary findings carry the search's own limitations. The third query returned a high false-positive rate because of homonymous acronyms (RDF, OWL, SHACL, SPARQL) in unrelated fields. Results are limited to records indexed in the Web of Science Core Collection at the search date, so preprints and unindexed work may be absent, and only English-language entries were captured, which may underrepresent legal scholarship in other EU languages. Some retrieved works are already cited in the main review, such as Topalli and Badii (2025).

Table 1. Directly relevant publications identified in the supplementary search (2025–2026). An asterisk marks a work already cited in the main review.

#	Authors (Year)	Title	Source	Cluster
1	Turaga et al. (2025)	CO2: LLM-Based Ontology-Driven Methodology for KGs and AI Compliance Checking	IEEE Access	A.2.1
2	Ahmed et al. (2026)	AI Act Compliance in Health Data Spaces: Requirement Modeling and Architectural Solutions	WorldCIST 2025	A.2.1
3	Sharma et al. (2025)	Ethical AI: Towards Defining a Collective Evaluation Framework	COMPSAC 2025	A.2.3
4	Campillo (2025)	Privacy by Design as a Requirement for Police Artificial Intelligence	Rev. Gen. Derecho Admin.	A.2.4
5	Feretzakis et al. (2025)	GDPR and Large Language Models: Technical and Legal Obstacles	Future Internet	A.2.4
6	Kioskli et al. (2025)	trustSense: Measuring Human Oversight Maturity for Trustworthy AI	Computers	A.2.3
7	Chemlali & Benseddik (2025)	Privacy-by-Design in Emotion AI: Data Protection Frameworks and Compliance Strategies	Access to Justice in Eastern Europe	A.2.4
8	Medina (2025)	AI and Privacy: Regulatory Harmonization and Challenges in the EU and Spain	IDP–Internet Law and Politics	A.2.4
9	Ozparlak & Metin (2025)	Designing Trust and Privacy: Legal Design in Ensuring Compliance with the EU AI Act	HCI-CPT 2025	A.2.4
10	Mpatziakas et al. (2025)	Deciphering Standards for Cybersecurity in Industry 4.0: Advisory AI for Cybersecure IIoT	IEEE CSR 2025	A.2.5
11	Korchenko et al. (2026)	Multi-Layered Open Data, Differential Privacy, and Secure Engineering: Environmental Digital Twins	Sustainability	A.2.4

12	Topalli & Badii (2025)*	A User-Centric Context-Aware Framework for Real-Time Privacy Protection in Multimodal AI	Sensors	A.2.4
13	Ke (2025)	Enabling Efficient and Semantic-Aware Constraint Validation in Knowledge Graphs	ESWC 2024 Satellite	A.2.2
14	Baimuratov & Turygin (2025)	Representing Normative Regulations in OWL DL for Automated Compliance Checking	LDAC 2025	A.2.2
15	Han (2025)	AIRPoC: AI-Enhanced Blockchain Consensus Framework for Autonomous Regulatory Compliance	Electronics	A.2.2
16	Montecchiari (2026)	Ontology-Based Validation of Enterprise Architecture Principles	Applied Sciences	A.2.2
17	Oranekwu et al. (2026)	Scalable Automation for IoT Cybersecurity Compliance: Ontology-Driven Reasoning	Computers & Security	A.2.1
18	Tauqeer et al. (2026)	An Integrated Approach to GDPR-Compliant Data Sharing Employing Consent, Contracts, and Licences	Data & Knowledge Engineering	A.2.2
19	Gallina et al. (2026)	Regulatory Compliance-Aware System Change Management via an Ontology-Based Approach	EuroSPI 2025	A.2.1
20	Castiglione et al. (2025)	Guiding Cybersecurity Compliance: An Ontology for the NIS 2 Directive	Computers & Security	A.2.1
21	Schubert et al. (2025)	An Ontology-Based Automation Framework for Continuous Compliance of Airborne Software	DASC 2025	A.2.1
22	Ikhsan (2026)	AI Risk Management for System Design: An Ontology-Driven Approach	ESWC 2025 Satellite	A.2.3
23	Corazza et al. (2025)	Reporting Requests Modelling in EU Legislation with a Hybrid AI Approach	ICAIL 2025	A.2.1
24	Roothaert et al. (2025)	TIDO: The Threat Intelligence Decision Ontology	K-CAP 2025	A.2.5

References

Abualhaija S, Ceci M, Briand L (2025). Legal Requirements Analysis: A Regulatory Compliance Perspective. In: Ferrari A, Ginde G (eds.) *Handbook on Natural Language Processing for Requirements Engineering*. Springer, 209–242.

Amaral G, Guizzardi R, Guizzardi G et al. (2021). Trustworthiness Requirements: The Pix Case Study. In: Ghose A et al. (eds.) *Conceptual Modeling*. Springer, 13011: 257–267.

Brabra H, Mtibaa A, Sliman L et al. (2016). Semantic Web Technologies in Cloud Computing: A Systematic Literature Review. *IEEE International Conference on Services Computing (SCC)*, 744–751.

Cichocki R (2025). Artificial Intelligence in Maritime Cybersecurity: Dual-Use Applications for Defense and Offense in the Age of Digital Seas. *TransNav International Journal of Marine Navigation and Safety of Sea Transportation*, 19(2): 617–623.

Court of Justice of the European Union (2020). CJEU Case C-511/18, *La Quadrature du Net and Others*.

Court of Justice of the European Union (2022). CJEU Case C-817/19, *Ligue des droits humains*.

Court of Justice of the European Union (2023). CJEU Case C-634/21, *SCHUFA Holding AG*.

Court of Justice of the European Union (2025). CJEU Case C-203/22, *Dun & Bradstreet Austria GmbH*.

Cuypers M (2023). Artificial Intelligence and International Humanitarian Law: Brothers in Arms or Rather the Opposite? KU Leuven Blog.

Duan Z, Nan G, Li R et al. (2025). Agile Orchestration at Will: An Entire Smart Service-Based Security Architecture Towards 6G. *IEEE Wireless Communications*, 32: 87–94.

Elahidoost P (2024). Towards a Tool Supported Approach for Regulatory Requirements Engineering. *IEEE 32nd International Requirements Engineering Conference (RE)*, 520–524.

ENISA (2019). *Good practices for security of IoT: secure software development lifecycle*. European Network and Information Security Agency.

European Commission (2012). Charter of Fundamental Rights of the European Union. 2012/C 326/02.

European Commission (2016a). Regulation (EU) 2016/679 (GDPR).

European Commission (2016b). Directive (EU) 2016/680 (Law Enforcement Directive).

European Commission (2019). Directive (EU) 2019/790 (Copyright in the Digital Single Market).

European Commission (2021a). Regulation (EU) 2021/821 (Dual Use Regulation, recast).

European Commission (2021b). Action Plan on Synergies between Civil, Defence and Space Industries, COM(2021) 70 final.

European Commission (2022a). Directive (EU) 2022/2555 (NIS2 Directive).

European Commission (2022b). Roadmap on Critical Technologies for Security and Defence, COM(2022) 61 final.

European Commission (2022c). Regulation (EU) 2022/2554 (DORA).

European Commission (2024a). Regulation (EU) 2024/1689 (AI Act).

European Commission (2024b). Regulation (EU) 2024/2847 (Cyber Resilience Act).

European Commission (2025a). Commission Guidelines on the Definition of an Artificial Intelligence System, C(2025) 5053 final.

European Commission (2025b). Commission Guidelines on Prohibited Artificial Intelligence Practices.

European Court of Human Rights (1950). European Convention on Human Rights.

European Parliament (2024). Joint Communication on a New European Defence Industrial Strategy.

European Parliament (2025). Interplay between the AI Act and the EU Digital Legislative Framework. Policy Department for Transformation, Innovation and Health.

Gómez-Romero J, Patricio MA, García J et al. (2011). Ontology-based context representation and reasoning for object tracking and scene interpretation in video. *Expert Systems with Applications*, 38(6): 7494–7510.

Guizzardi R, Amaral G, Guizzardi G et al. (2023). An ontology-based approach to engineering ethicality requirements. *Software and Systems Modeling*, 22(6): 1897–1923.

Hernandez J, Golpayegani D, Lewis D (2024). Ontology-Based Approach for Mapping Concepts and Requirements from Regulations and Standards: The Case of the EU AI Act and International Standards. In: Savelka J et al. (eds.) *Frontiers in Artificial Intelligence and Applications*. IOS Press.

Hosseini AM, Kastner W, Sauter T (2025). Ontology Framework Supporting Security-By-Design of Industrial Control Systems. *IEEE Transactions on Industrial Informatics*, 21(9): 7188–7197.

Huaranga-Junco E, González-Gerpe S, Castillo-Cara M et al. (2024). From cloud and fog computing to federated-fog computing: A comparative analysis of computational resources in real-time IoT applications based on semantic interoperability. *Future Generation Computer Systems*, 159: 134–150.

ICRC (2021). Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach. ICRC Position Paper.

ICRC (2023). What You Need to Know about Artificial Intelligence in Armed Conflict.

ICRC (2026a). The Geneva Conventions and their Commentaries.

ICRC (2026b). Customary IHL.

Imperial JM, Jones MD, Tayyar Madabushi H (2025). Standardizing Intelligence: Aligning Generative AI for Regulatory and Operational Compliance. SSRN.

ISO/IEC (2022). ISO/IEC 22989:2022 – Information Technology – Artificial Intelligence – Concepts and Terminology.

Juric M (2024). Legal regulation on the use of artificial intelligence for national security purposes in Europe. *European Integration Studies*, 20(2): 107–136.

Khan AA, Alsufyani A, Alsufyani N et al. (2025). BAML: A decentralized approach to secure, privacy-preserving financial compliance for enhancing anti-money laundering with blockchain hyperledger and federated learning. *Peer-to-Peer Networking and Applications*, 18(5): 270.

Kilian R, Jäck L, Ebel D (2025). European AI Standards – Technical Standardisation and Implementation Challenges under the EU AI Act. *European Journal of Risk Regulation*, 16(3): 1038–1062.

Kosenkov O, Elahidoost P, Gorschek T et al. (2025). Systematic mapping study on requirements engineering for regulatory compliance of software systems. *Information and Software Technology*, 178: 107622.

Kremidas-Courtney C (2025). From Dual-Use to Omni-Use: Securing Europe's Future. European Policy Centre.

Lietuvos Respublikos Seimas (2011). Law on the Legal Protection of Personal Data Processed for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences, the Execution of Sentences or National Security or Defence. Nr. XI-1336.

Lietuvos Respublikos Seimas (2024). Cybersecurity Law of the Republic of Lithuania. Nr. XII-1428.

NATO (2022). NATO Core Metadata Specification (NCMS) – ADatP-5636 Edition A.

NATO (2024a). Summary of NATO's Revised Artificial Intelligence (AI) Strategy.

NATO (2024b). NATO's Digital Transformation Implementation Strategy.

NATO (2025). Data Strategy for the Alliance.

Ndiaye NG, Waedt K, Dejon N et al. (2026). Safety and Cybersecurity Under Emerging EU Legislation for Industry: A Use-Case Driven Perspective. In: Coppens B et al. (eds.) *Availability, Reliability and Security, ARES 2025*, Pt I. Springer, 15994: 304–321.

OECD (2025). Intellectual Property Issues in Artificial Intelligence Trained on Scraped Data. OECD AI Papers, No. 33.

Orlando A, Santoro M (2025). A semantic approach to understanding GDPR fines: From text to compliance insights. *Computer Law & Security Review*, 59: 106187.

Paskauskas RA (2025). A Preliminary Ontology for 5G Network Resilience: Hybrid Threats, Risk Reduction, Compliance. *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, 496–503.

Paskauskas RA (2026). SecOntologyLab/regulatory-compliance-ontology: Initial Public Release. Zenodo. DOI: 10.5281/zenodo.18763491.

Pn AR, Ramachandra R, Rao KS et al. (2024). Straight Through Gumbel Softmax Estimator based Bimodal Neural Architecture Search for Audio-Visual Deepfake Detection. *IEEE International Joint Conference on Biometrics (IJCB)*, 1–9.

Powell R (2024). The EU AI Act: National Security Implications. CETaS Explainers.

RAND (2024). General-Purpose Artificial Intelligence (GPAI) Models and GPAI Models with Systemic Risk: Classification and Requirements for Providers. RAND Corporation.

Sabaliauskaite G, Paskauskas RA, Bružė E, Matulytė R, Lavišius T (2026). Automated regulatory compliance for AI systems in the security domain: The case of dual-use deployment. *Open Research Europe*, 6:83. DOI: 10.12688/openreseurope.23137.1.

Topalli N, Badii A (2025). A User-Centric Context-Aware Framework for Real-Time Optimisation of Multimedia Data Privacy Protection, and Information Retention Within Multimodal AI Systems. *Sensors*, 25(19): 6105.

Vogiatzoglou P (2024). The AI Act National Security Exception.

Wang L (2025). Can machines think beyond words? A critique of AI's meaning-production process. *AI & Society*, 41.

Xia L (2025). Enabling University Mental Health Monitoring Through 6G Edge-Cloud IoT Environmental Perception Frameworks. *IEEE Communications Standards Magazine*, 1–8.

Supplementary search corpus (Web of Science Core Collection, 2025–2026)

The following lists record the full set of entries retrieved by the three supplementary queries, including items later excluded as out of scope. They are reproduced to document the search and are kept separate from the cited references above.

Primary search. 19 records.

Abdelsalam, M., Nwokolo, S., Iwuji, P., Meyer, E., Ahia, C., & Egdair, I. (2026). Hazardous waste risk detection powered by artificial intelligence and machine learning for resilient monitoring and mitigation of potential environmental threats. RESULTS IN ENGINEERING, 29. (WOS:001705653000001). https://doi.org/10.1016/j.rineng.2026.109655

Ahmed, M., Khalid, M., & Helfert, M. (2026). AI Act Compliance in Health Data Spaces: Requirement Modeling and Architectural Solutions (A. Rocha, H. Adeli, A. Poniszewska-Maranda, F. Moreira, & I. Bianchi, Eds.; Vol. 1524, pp. 397–408). (WOS:001695428100032). https://doi.org/10.1007/978-3-031-97799-2_32

Alduweib, E., Alahmadi, A., & Alromema, W. (2026). Enhancing Social Networks Services: An Ontology-Based Approach. INTERNATIONAL ARAB JOURNAL OF INFORMATION TECHNOLOGY, 23(2), 274–282. (WOS:001743645500001). https://doi.org/10.34028/iajit/23/2/8

Arazzi, M., Arikkat, D., Nicolazzo, S., Nocera, A., Rehiman, K., Vinod, P., & Conti, M. (2025). NLP-based techniques for Cyber Threat Intelligence. COMPUTER SCIENCE REVIEW, 58. (WOS:001504858600001). https://doi.org/10.1016/j.cosrev.2025.100765

Arif, I., Baykal, T., Inanç, S., Ergün, S., Dincer, E., Sen, M., Atalay, A., Ergün, S., Kanak, A., & IEEE. (2025). Ontology-Driven Metrology Data Management for Wireless Charging, Battery Management and Predictive Maintenance in Electrical Vehicles. 198–203. (WOS:001568936500035). https://doi.org/10.1109/METROAUTOMOTIVE64646.2025.11119204

Dahir, S., & El Qadi, A. (2025). Assessing the Role of Ontologies in Enhancing Various Modern Systems. PERTANIKA JOURNAL OF SCIENCE AND TECHNOLOGY, 33(5), 2049–2068. (WOS:001576867400002). https://doi.org/10.47836/pjst.33.5.02

Guerra, P., Nunes, R., & Silva, L. (2025). A cases and clusters framework for recording, retrieving, and reusing response plans in structured cybersecurity incident management. ENGINEERING APPLICATIONS OF ARTIFICIAL INTELLIGENCE, 160. (WOS:001546959800005). https://doi.org/10.1016/j.engappai.2025.111831

Henry, J. (2025). Population health management through human phenotype ontology with policy for ecosystem improvement. FRONTIERS IN ARTIFICIAL INTELLIGENCE, 8. (WOS:001550150700001). https://doi.org/10.3389/frai.2025.1496937

Iovane, G., & Iovane, G. (2025). Bridging Computational Structures with Philosophical Categories in Sophimatics and Data Protection Policy with AI Reasoning. APPLIED SCIENCES-BASEL, 15(20). (WOS:001602546000001). https://doi.org/10.3390/app152010879

Kalutharage, C., Liu, X., & Chrysoulas, C. (2025). Neurosymbolic learning and domain knowledge-driven explainable AI for enhanced IoT network attack detection and response. COMPUTERS & SECURITY, 151. (WOS:001422652000001). https://doi.org/10.1016/j.cose.2025.104318

Kim, Y., Hwang, J., Lee, S., & Lee, S. (2026). A Systematic Review of Ontology-AI Integration for Construction Image Recognition. INFORMATION, 17(1). (WOS:001670570800001). https://doi.org/10.3390/info17010048

Le, T., Vuong, N., Dung, L., & Le, B. (2025). T-GNN plus plus: Advancing Stock Market Forecasting with Knowledge Representation and Explainable AI (D. VanHai, S. Hasegawa, H. Vo, & S. Nguyen, Eds.; pp. 340–345). (WOS:001679963600058). https://doi.org/10.1109/KSE68178.2025.11309510

Pursnani, V., Sermet, Y., & Demir, I. (2025). A conversational intelligent assistant for enhanced operational support in floodplain management with multimodal data. INTERNATIONAL JOURNAL OF DISASTER RISK REDUCTION, 122. (WOS:001466344400001). https://doi.org/10.1016/j.ijdrr.2025.105422

Sharma, A., Kyosev, D., & Kunkel, J. (2025). Ethical AI: Towards Defining a Collective Evaluation Framework (H. Shahriar, K. Alam, H. Ohsaki, S. Cimato, M. Capretz, S. Ahmed, S. Ahamed, A. Majumder, M. Haque, T. Yoshihisa, A. Cuzzocrea, M. Takemoto, N. Sakib, & M. Elsayed, Eds.; pp. 1665–1670). (WOS:001575960000215). https://doi.org/10.1109/COMPSAC65507.2025.00344

Tiwari, M., Zhou, Y., Lee, J., Naraspuram, K., Bewong, M., & Rathore, V. (2026). Generative AI and financial crimes: A quantitative systematic literature review. CRIME SCIENCE, 15(1). (WOS:001720778100001). https://doi.org/10.1186/s40163-026-00268-y

Turaga, V., Pahi, T., Tjoa, S., Siami-Namini, S., & Namin, A. (2025). CO2 (Co-Compliance Officer): An LLM-Based Ontology-Driven Methodology for Generating Knowledge Graphs and AI Compliance Checking. IEEE ACCESS, 13, 210576–210606. (WOS:001643474000040). https://doi.org/10.1109/ACCESS.2025.3639228

Wang, L., Wang, Y., & Li, N. (2025). Architecting Resilience in Global Freight Forwarding with a Causal AI Framework. JOVE-JOURNAL OF VISUALIZED EXPERIMENTS, (225). (WOS:001634948000024). https://doi.org/10.3791/69436

Wang, Y., Bi, Y., Yu, H., Yao, X., Ren, Y., & Rong, W. (2025). AI-driven proactive security defense in distributed iov systems: Cyber threat intelligence modeling for connected autonomous vehicles. PEER-TO-PEER NETWORKING AND APPLICATIONS, 18(4). (WOS:001524611100002). https://doi.org/10.1007/s12083-025-02008-6

Zhang, X., Chen, L., & Wang, J. (2025). The research landscape and evolutionary trends of robot-assisted orthopedic telesurgery: A bibliometric and visualized analysis. JOURNAL OF ROBOTIC SURGERY, 19(1). (WOS:001607978300011). https://doi.org/10.1007/s11701-025-02913-1

Supplementary search 1. 42 records.

Aguelal, H., & Palmieri, P. (2025). ECG De-anonymization: Real-world Risks and a Privacy-by-design Mitigation Strategy (R. Sicilia, L. Santamaria, G. Papadopoulos, A. Gonzalez, V. Guarrasi, M. Cazzolato, & B. Kane, Eds.; pp. 449–456). (WOS:001544273800085). https://doi.org/10.1109/CBMS65348.2025.00095

Al-Kfairy, M., Alrabaee, S., Alfandi, O., Mohamed, A., & Khaddaj, S. (2025). Navigating Ethical Dimensions in the Metaverse: Challenges, Frameworks, and Solutions. IEEE ACCESS, 13, 79996–80018. (WOS:001484703100039). https://doi.org/10.1109/ACCESS.2025.3564498

Almeida, R., Freitas, A., Silva, T., Dias, D., Lacroix, J., De Lathauwer, I., Marreiros, G., & Conceiçao, L. (2025). Integrating Privacy by Design Principles into AI-Driven Systems for Human Activity and Health Monitoring (A. Moallem, Ed.; Vol. 15815, pp. 23–41). (WOS:001572075600002). https://doi.org/10.1007/978-3-031-92840-6_2

Almomani, A., Al-Qerem, A., Alauthman, M., Aldweesh, A., Aoudi, S., & Salloum, S. (2025). Ethical Foundations of AI-Driven Avatars in the Metaverse for Innovation and User Privacy. IEEE ACCESS, 13, 130610–130628. (WOS:001540953200018). https://doi.org/10.1109/ACCESS.2025.3589714

Altshuler, T., Hershkovitz, R., Mikulinsky, R., & Müller, B. (2025). Governing phygital spaces: Human rights by design meets speculative design. INTERNET POLICY REVIEW, 14(4). (WOS:001624846600007). https://doi.org/10.14763/2025.4.2048

Alzamil, L., Alhasani, A., & Alshehri, S. (2025). Privacy Concerns in ChatGPT Data Collection and Its Impact on Individuals. FUTURE INTERNET, 17(11). (WOS:001624466900001). https://doi.org/10.3390/fi17110511

Calcaterra, V., Ciriello, U., Medici, S., Pagani, V., Campoy, C., Labati, L., Rossi, V., Escudero-Marin, M., Vandoni, M., Corbellini, C., Verduci, E., Marin, L., Bonillo-Leon, R., Bahdur, K., Gatti, A., Fiore, G., Pellino, V., Mannarino, S., & Zuccotti, G. (2026). PODiaCarD: a prototype of a digital twin platform for the management of pediatric obesity and related cardiometabolic complications. EUROPEAN JOURNAL OF PEDIATRICS, 185(2). (WOS:001663013900002). https://doi.org/10.1007/s00431-025-06708-2

Campillo, L. (2025). PRIVACY BY DESIGN AS A REQUIREMENT FOR POLICE ARTIFICIAL INTELLINGENCE. REVISTA GENERAL DE DERECHO ADMINISTRATIVO, (68). (WOS:001454718900022).

Chemlali, L., & Benseddik, L. (2025). PRIVACY-BY-DESIGN IN EMOTION AI: DATA PROTECTION FRAMEWORKS AND COMPLIANCE STRATEGIES. ACCESS TO JUSTICE IN EASTERN EUROPE, 8. (WOS:001632187100001). https://doi.org/10.33327/AJEE-18-8.S-r000153

Croitoru, I., Turcu, C., & Turcu, C. (2026). Privacy-by-Design in AI-Assisted Systems for Caregivers of Children with Autism: A Secure Multi-Agent Architecture. APPLIED SCIENCES-BASEL, 16(4). (WOS:001699820500001). https://doi.org/10.3390/app16042157

Dkier, S., Sadki, S., & Bakkali, H. (2025). Empowering User Privacy in Edge Computing: Generative AI for Dynamic Policy Compliance. IEEE INTERNET COMPUTING, 29(4), 25–35. (WOS:001661112100007). https://doi.org/10.1109/MIC.2025.3576184

Feretzakis, G., Vagena, E., Kalodanis, K., Peristera, P., Kalles, D., & Anastasiou, A. (2025). GDPR and Large Language Models: Technical and Legal Obstacles. FUTURE INTERNET, 17(4). (WOS:001474998600001). https://doi.org/10.3390/fi17040151

Floridi, L., & Ascani, A. (2025). Augmented Democracy in Action: AI Systems for Legislative Innovation in the Italian Parliament. MINDS AND MACHINES, 35(4). (WOS:001587480900001). https://doi.org/10.1007/s11023-025-09743-y

Ghiurau, D., & Popescu, D. (2026). Data Security and Privacy in GPT Models: Techniques and Challenges. APPLIED SCIENCES-BASEL, 16(4). (WOS:001699853800001). https://doi.org/10.3390/app16041900

Gorostiza-Esquerdeiro, I., Buján-Carballal, D., & Oyarbide-Zubillaga, A. (2026). MWIN (Measure What Is Needed): A strategic framework for privacy-first, AI-ready, and data-driven marketing analytics. JOURNAL OF MARKETING ANALYTICS. (WOS:001751912100001). https://doi.org/10.1057/s41270-026-00471-5

Hossmann, S., Ballhausen, H., & Rothenbühler, M. (2025). Framework of artificial intelligence in diabetology. Artificial intelligence-caught between data protection, ethics, approval, and demand. DIABETOLOGIE, 21(6), 687–694. (WOS:001533063400001). https://doi.org/10.1007/s11428-025-01356-4

Iscan, G., & Çöme, O. (2026). Security and privacy in e-health technologies: A scoping review of challenges and strategies in primary care. FAMILY PRACTICE, 43(2). (WOS:001698544600001). https://doi.org/10.1093/fampra/cmag006

Jacobs-Basadien, M., & Pather, S. (2026). Assessing AI policy and guideline progress within the South African public higher education system: Insights from documented policies. UNIVERSAL ACCESS IN THE INFORMATION SOCIETY, 25(2). (WOS:001746106000002). https://doi.org/10.1007/s10209-026-01340-9

Khan, A., Iqbal, A., Husnain, G., Masood, F., Al-Naeem, M., & Iqbal, S. (2026). Secure and Differentially Private Edge-Cloud Federated Learning Framework for Privacy-Preserving Maritime AIS Intelligence. CMC-COMPUTERS MATERIALS & CONTINUA, 87(3). (WOS:001745381400001). https://doi.org/10.32604/cmc.2026.077222

Khattab, O., Balaji, B., Alghadhoori, F., Almazyad, F., Aldousari, M., Al-Ameeri, A., & Al-Kadri, M. (2025). Real time urban traffic prediction using RFID and a hybrid LSTM random forest model. SCIENTIFIC REPORTS, 15(1). (WOS:001690556000001). https://doi.org/10.1038/s41598-025-27485-w

Kioskli, K., Fotis, T., Seralidou, E., Passaris, M., & Polemi, N. (2025). trustSense: Measuring Human Oversight Maturity for Trustworthy AI. COMPUTERS, 14(11). (WOS:001623550000001). https://doi.org/10.3390/computers14110483

Konstantakis, M., & Iakovaki, E. (2026). ARIA: An AI-Supported Adaptive Augmented Reality Framework for Cultural Heritage. INFORMATION, 17(1). (WOS:001670568100001). https://doi.org/10.3390/info17010090

Korchenko, O., Korchenko, A., Prokopovych-Tkachenko, D., Karpinski, M., & Kazmirchuk, S. (2026). Multi-Layered Open Data, Differential Privacy, and Secure Engineering: The Operational Framework for Environmental Digital Twins. SUSTAINABILITY, 18(4). (WOS:001701239200001). https://doi.org/10.3390/su18041912

Lawelai, H., Purnomo, E., Nurmandi, A., Jovita, H., & Baulete, E. (2025). Cybersecurity policy on smart city infrastructure: A mapping of new threats and protections. JOURNAL OF SCIENCE AND TECHNOLOGY POLICY MANAGEMENT. (WOS:001513154600001). https://doi.org/10.1108/JSTPM-09-2024-0359

Madlenák, R., Madlenáková, L., Cvacho, V., & Gachulinec, D. (2026). Ethical Challenges of Artificial Intelligence in Higher Education: A Four-Pillar Student-Activity Framework for Institutional Governance. EDUCATION SCIENCES, 16(4). (WOS:001749493200001). https://doi.org/10.3390/educsci16040555

Medina, F. (2025). AI and privacy: Regulatory harmonization and regulatory challenges in the European Union and Spain. IDP-INTERNET LAW AND POLITICS, (42). (WOS:001454823600001). https://doi.org/10.7238/idp.v0i42.432084

Morales, A., Reis, T., Panisson, A., Ourique, F., & Sene, I. J. (2026). Affective Intelligent Systems in Healthcare: A Systematic Review. TECHNOLOGIES, 14(3). (WOS:001725243900001). https://doi.org/10.3390/technologies14030188

Mpatziakas, A., Schoinas, I., Lalas, A., Drosou, A., Chatzidiamantis, N., Tzovaras, D., & IEEE. (2025). Deciphering Standards for cybersecurity in Industry 4.0: Advisory AI for Cybersecure IIoT. 893–898. (WOS:001575967100133). https://doi.org/10.1109/CSR64739.2025.11130103

Muñoz, A., Lopez, J., Alcaraz, C., & Martinelli, F. (2025). Trusted Platform and Privacy Management in Cyber Physical Systems: The DUCA Framework (S. Katsikas & B. Shafiq, Eds.; Vol. 15722, pp. 211–230). (WOS:001552193700012). https://doi.org/10.1007/978-3-031-96590-6_12

Ozparlak, B., & Metin, E. (2025). Designing Trust and Privacy: The Role of Legal Design in Ensuring Compliance with the EU AI Act (A. Moallem, Ed.; Vol. 15815, pp. 116–127). (WOS:001572075600007). https://doi.org/10.1007/978-3-031-92840-6_7

Phang, K., & Kaabi, J. (2025). Privacy in Flux: A 35-Year Systematic Review of Legal Evolution, Effectiveness, and Global Challenges (US/EU Focus with International Comparisons). JOURNAL OF CYBERSECURITY AND PRIVACY, 5(4). (WOS:001646805800001). https://doi.org/10.3390/jcp5040103

Ramesh, G., Pai, T., Birau, R., Poojary, K., Abhay, Shingad, A., Sowjanya, N., Popescu, V., Mitroi, A., Nioata, R., & Raj, K. (2025). A Comprehensive Review on Scaling Machine Learning Workflows Using Cloud Technologies and DevOps. IEEE ACCESS, 13, 148559–148594. (WOS:001565196100012). https://doi.org/10.1109/ACCESS.2025.3599281

Ray, P. (2026). A Review of TRiSM Frameworks in Artificial Intelligence Systems: Fundamentals, Taxonomy, Use Cases, Key Challenges and Future Directions. EXPERT SYSTEMS, 43(3). (WOS:001698737900020). https://doi.org/10.1111/exsy.70213

Rehman, A., Daehlen, A., Heldal, I., & Lin, J. (2026). Privacy Preservation and Identity Tracing Prevention in AI-Driven Eye Tracking for Interactive Learning Environments. IEEE ACCESS, 14, 11403–11423. (WOS:001673800400006). https://doi.org/10.1109/ACCESS.2025.3645115

Sakka, S., Liagkou, V., Ferreira, A., & Stylios, C. (2026). Digital Boundaries and Consent in the Metaverse: A Comparative Review of Privacy Risks. JOURNAL OF CYBERSECURITY AND PRIVACY, 6(1). (WOS:001700453700001). https://doi.org/10.3390/jcp6010024

Seheult, J., Malone, J., Jackson, B., Malik, M., & Yazer, M. (2026). Ethical dilemmas in the use of artificial intelligence in transfusion medicine. VOX SANGUINIS, 121(4), 417–429. (WOS:001692564000001). https://doi.org/10.1111/vox.70183

Stelea, G., Sangeorzan, L., & Enache-David, N. (2025). Accessible IoT Dashboard Design with AI-Enhanced Descriptions for Visually Impaired Users. FUTURE INTERNET, 17(7). (WOS:001535600200001). https://doi.org/10.3390/fi17070274

Süwer, S., Ullah, M., Probul, N., Maier, A., & Baumbach, J. (2026). Privacy-by-Design with Federated Learning will drive future Rare Disease Research. JOURNAL OF NEUROMUSCULAR DISEASES, 13(1), 6–19. (WOS:001459511600001). https://doi.org/10.1177/22143602241296276

Szpilko, D., Rzepka, A., Nica, E., Lazaroiu, G., & Gedeon, T. (2025). WHAT FACTORS WILL SHAPE THE FUTURE OF SUSTAINABLE AND SMART CITIES IN EUROPE? EVIDENCE FROM THE DELPHI STUDY. ECONOMICS AND ENVIRONMENT, 94(3), 12–24. (WOS:001616013900006). https://doi.org/10.34659/eis.2025.94.3.1272

Tariq, M., Khan, S., Mazhar, T., Shahzad, T., Arooj, S., Ouahada, K., Khan, M., & Hamam, H. (2026). Federated Deep Learning in Intelligent Urban Ecosystems: A Systematic Review of Advancements and Applications in Smart Cities, Homes, Buildings, and Healthcare Systems. CMES-COMPUTER MODELING IN ENGINEERING & SCIENCES, 146(3). (WOS:001740329500001). https://doi.org/10.32604/cmes.2026.078672

Topalli, N., & Badii, A. (2025). A User-Centric Context-Aware Framework for Real-Time Optimisation of Multimedia Data Privacy Protection, and Information Retention Within Multimodal AI Systems. SENSORS, 25(19). (WOS:001593938200001). https://doi.org/10.3390/s25196105

Tsouplaki, A., Kalloniatis, C., & Mikros, G. (2026). Adopting LLMs in Internet of Cloud Ecosystems: Identifying the Key Privacy Challenges (S. Furnell & N. Clarke, Eds.; Vol. 761, pp. 297–317). (WOS:001676371100021). https://doi.org/10.1007/978-3-032-02504-3_21

Supplementary search 2. 49 records.

Alhawarri, M. (2025). Schweinfurthiamide as a Promising Anticancer Agent: Molecular Docking, Dynamics, and ADMET Insights Targeting MTHFD2. JOURNAL OF PHARMACEUTICAL INNOVATION, 20(5). (WOS:001583196800001). https://doi.org/10.1007/s12247-025-10092-7

Altalhoni, H., Ali, N., Yunus, F., Atiewi, S., Alshardan, A., Almiani, M., & AlZu'bi, S. (2026). A novel artificial intelligence based dynamic task scheduling and load awareness. CLUSTER COMPUTING-THE JOURNAL OF NETWORKS SOFTWARE TOOLS AND APPLICATIONS, 29(3). (WOS:001691973700004). https://doi.org/10.1007/s10586-026-05948-7

Baimuratov, I., & Turygin, D. (2025). Representing Normative Regulations in OWL DL for Automated Compliance Checking Supported by Text Annotation (P. Pauwels, M. Poveda-Villalon, & W. Terkaj, Eds.; Vol. 4113, pp. 122–135). (WOS:001661504400009).

Bergier, I., Barbedo, J., Bolfe, É., Drucker, D., & Soares, F. (2026). The AgriTrust Framework: Federated Semantic Governance for Trusted and Interoperable Agricultural Data Sharing. AUTOMATION, 7(2). (WOS:001749216700001). https://doi.org/10.3390/automation7020057

Bhole, M., Sauter, T., Semper, S., & Kastner, W. (2025). Why to Fail Fast and Often: A Strategy for OT Safety and Security Evaluation. IEEE ACCESS, 13, 51793–51812. (WOS:001455525900039). https://doi.org/10.1109/ACCESS.2025.3553011

Canale, C., Arpino, F., Cortellessa, G., & Grossi, G. (2025). Different numerical approaches for the analysis of a waste-to-energy plant. APPLIED THERMAL ENGINEERING, 266. (WOS:001420556200001). https://doi.org/10.1016/j.applthermaleng.2025.125679

Castiglione, G., Santamaria, D., Bella, G., Brisindi, L., & Puccia, G. (2025). Guiding cybersecurity compliance: An ontology for the NIS 2 directive. COMPUTERS & SECURITY, 157. (WOS:001579345100003). https://doi.org/10.1016/j.cose.2025.104617

Chen, X., Yan, S., Zhu, C., Hu, B., & Zhang, C. (2025). Thermodynamic insights into solvent-mediated crystallization and morphology control of high-energy-density hydrazinium cyclo-pentazolate. JOURNAL OF SOLUTION CHEMISTRY, 54(12), 1743–1759. (WOS:001574628100001). https://doi.org/10.1007/s10953-025-01511-x

Chy, T., Lamboro, H., Genest, O., Kung, A., Rabrait, C., Sebilleau, D., & Gyrard, A. (2025). Design of an Ontology-Driven Constraint Tester (ODCT) and Application to SAREF and Smart Energy Appliances (S. Sahri, S. Tiwari, B. Villazon-Terrazas, & F. Ortiz-Rodriguez, Eds.; Vol. 15459, pp. 183–198). (WOS:001549155500013). https://doi.org/10.1007/978-3-031-81221-7_13

Clarke, J., Zehntner, N., Hutchinson, J., Ceballos, M., Tedone, L., Jordan, T., Pay, J., Mooney, N., & Hocking, D. (2025). Unmasking the impact of second-generation anticoagulant rodenticides on Masked owls (Tyto novaehollandiae castanops) in Tasmania. EMU-AUSTRAL ORNITHOLOGY, 125(2), 191–198. (WOS:001510772500001). https://doi.org/10.1080/01584197.2025.2507301

Corazza, M., Palmirani, M., Sapienza, S., & Longo, G. (2025). Reporting Requests Modelling in European Legislation with a Hybrid AI Approach (J. Maranhao, Ed.; pp. 93–102). (WOS:001704118700010). https://doi.org/10.1145/3769126.3769255

Dutta, B., & Arzoo, S. (2026). Towards a Biographical Ontology: The OntoBio Framework and Its Applications. KNOWLEDGE ORGANIZATION, 53(1). (WOS:001702143600001). https://doi.org/10.31083/KO45190

Fatahi, M., Zadeh, D., Noormohammadi-Asl, A., Moshiri, B., Basir, O., Sadjadi, E., García-Herrero, J., & Molina, J. (2026). CB-OWL-ViT: A Multimodal Cost-Effective Framework for Contagious Disease Monitoring. MATHEMATICS, 14(4). (WOS:001700825400001). https://doi.org/10.3390/math14040647

Gallina, B., Schweizer, M., & Dibowski, H. (2026). Regulatory Compliance-Aware System Change Management via an Ontology-Based Approach (M. Yilmaz, P. Clarke, A. Riel, R. Messnarz, M. Zelmenis, & I. Buce, Eds.; Vol. 2657, pp. 245–259). (WOS:001584988500015). https://doi.org/10.1007/978-3-032-04288-0_15

Goh, W., Jang, J., Park, S., Choi, B., Lim, H., & Zi, G. (2024). Automated Compliance Checking System for Structural Design Codes in a BIM Environment. KSCE JOURNAL OF CIVIL ENGINEERING, 28(10), 4175–4189. (WOS:001290676300001). https://doi.org/10.1007/s12205-024-1121-5

Goram, M. (2025). Integrating User Perspectives: A Framework for Ad-Hoc Privacy Preference Implementation in Information Systems (C. Stephanidis, M. Antona, S. Ntoa, & G. Salvendy, Eds.; Vol. 2319, pp. 60–69). (WOS:001436402300006). https://doi.org/10.1007/978-3-031-78516-0_6

Guo, W., Gu, K., Li, Y., Tian, W., Wu, Z., & Liu, J. (2025). Functional valorization of oil shale waste for sustainable pavement materials: Component regulation mechanisms based on molecular simulation and experimental validation. CONSTRUCTION AND BUILDING MATERIALS, 500. (WOS:001616045500001). https://doi.org/10.1016/j.conbuildmat.2025.144207

Gustafson, M., McGinn, K., Heys, J., Sawyer, S., & Wood, C. (2025). Rapid implementation and adaptive design of a large-scale monitoring program for a declining species. BIOLOGICAL CONSERVATION, 311. (WOS:001560573000001). https://doi.org/10.1016/j.biocon.2025.111442

Hagedorn, P., Fauth, J., Zentgraf, S., Seiss, S., König, M., & Brilakis, I. (2025). OntoBPR: An ontology-based framework for performing building permit reviews using standardized information containers. ADVANCED ENGINEERING INFORMATICS, 66. (WOS:001501954600004). https://doi.org/10.1016/j.aei.2025.103369

Han, S. (2025). AIRPoC: An AI-Enhanced Blockchain Consensus Framework for Autonomous Regulatory Compliance. ELECTRONICS, 14(20). (WOS:001601470500001). https://doi.org/10.3390/electronics14204058

Hejna, M., Lyczko, J., Koziel, J., Armstrong, E., Niri, V., Haddadi, S., Anyszkiewicz, J., & Bialowiec, A. (2026). Characterization and implications of volatile organic compounds release from raw and torrefied biogenic refuse-derived fuel components. JOURNAL OF ENVIRONMENTAL MANAGEMENT, 400. (WOS:001683376900001). https://doi.org/10.1016/j.jenvman.2026.128787

Hejna, M., Łyczko, J., Koziel, J., Armstrong, E., Niri, V., Haddadi, S., Anyszkiewicz, J., & Białowiec, A. (2026). Release of volatile organic compounds from raw and torrefied polymer components of the refuse-derived fuel: Characterization and implications. WASTE MANAGEMENT, 217. (WOS:001736725800001). https://doi.org/10.1016/j.wasman.2026.115506

Ikhsan, M. (2026). AI Risk Management for System Design: An Ontology-Driven Approach Integrating Engineering Principles and Ethical Insights (J. McCrae, E. Curry, V. Presutti, M. Alam, P. Colpaert, J. Parreira, D. Collarana, M. Sabou, A. Harth, & P. Lisena, Eds.; Vol. 15832, pp. 245–253). (WOS:001663396900036). https://doi.org/10.1007/978-3-031-99554-5_39

Ioannidou, P., Vezakis, I., Haritou, M., Petropoulou, R., Miloulis, S., Kouris, I., Bromis, K., Matsopoulos, G., & Koutsouris, D. (2025). HEalthcare Robotics' ONtology (HERON): An Upper Ontology for Communication, Collaboration and Safety in Healthcare Robotics. HEALTHCARE, 13(9). (WOS:001487572600001). https://doi.org/10.3390/healthcare13091031

Jia, L., Chen, M., Chen, C., & Jin, Y. (2025). A Semantic Web and IFC-Based Framework for Automated BIM Compliance Checking. BUILDINGS, 15(15). (WOS:001549402500001). https://doi.org/10.3390/buildings15152633

Ke, J. (2025). Enabling Efficient and Semantic-Aware Constraint Validation in Knowledge Graphs (A. Penuela, O. Corcho, P. Groth, E. Simperl, V. Tamma, A. Nuzzolese, M. Poveda-Villalon, M. Sabou, V. Presutti, I. Celino, A. Revenko, J. Raad, B. Sartini, & P. Lisena, Eds.; Vol. 15345, pp. 104–114). (WOS:001447374000011). https://doi.org/10.1007/978-3-031-78955-7_11

Liu, J., Iwakin, O., Romero, C., Cheng, L., Moazeni, F., Yao, Z., De Saro, R., & Craparo, J. (2025). Rapid characterization of MSW and RDF feedstocks for waste-to-energy process using LIBS and ML techniques. WASTE MANAGEMENT, 206. (WOS:001555499100001). https://doi.org/10.1016/j.wasman.2025.115079

Lu, B., Pham, D., Chang, T., Lovette, M., Bui, T., Ma, S., & IEEE COMPUTER SOC. (2025). SHACL-SKOS based Knowledge Representation of Material Safety Data Sheet (SDS) for the Pharmaceutical Industry. 110–117. (WOS:001540479500015). https://doi.org/10.1109/ICSC64641.2025.00021

Massari, A., Peroni, S., Tomasi, F., & Heibi, I. (2026). Representing provenance and track changes of cultural heritage metadata in RDF: a survey of existing approaches. DIGITAL SCHOLARSHIP IN THE HUMANITIES, 41, i196–i212. (WOS:001540139300001). https://doi.org/10.1093/llc/fqaf076

Merchán, J., & Santana, J. (2025). Assisted Development of an Urban Planning Ontology via Human-AI Collaboration: A Case Study in Algodre (Zamora) (D. DeLaIglesia, J. Santana, & A. Rivero, Eds.; Vol. 1465, pp. 27–35). (WOS:001598871600003). https://doi.org/10.1007/978-3-031-99474-6_3

Mogahed, M., & Mansouri, M. (2026). An Ontology-Based Architecture for Interoperable Healthcare Systems-of-Systems: Structure, Interaction Patterns, and Covenant-Based Governance. SYSTEMS, 14(4). (WOS:001750260800001). https://doi.org/10.3390/systems14040376

Montecchiari, D. (2026). Ontology-Based Validation of Enterprise Architecture Principles. APPLIED SCIENCES-BASEL, 16(7). (WOS:001738515600001). https://doi.org/10.3390/app16073352

Oranekwu, I., Elluri, L., Yus, R., & Kotal, A. (2026). Scalable automation for IoT cyberSecurity compliance: Ontology-driven reasoning for real-time assessment. COMPUTERS & SECURITY, 161. (WOS:001621276400001). https://doi.org/10.1016/j.cose.2025.104711

Racho, P., Nammana, B., Tantemsapya, N., Wichitsathian, B., Riewklang, K., & Tantrakarnapa, K. (2026). Valorization of recycled paper mill sludge via mass-energy integration for sustainable onsite power generation: A case study. WASTE MANAGEMENT, 212. (WOS:001674283800001). https://doi.org/10.1016/j.wasman.2026.115354

Recio-Colmenares, C., Recio-Colmenares, R., Castillo-Barrera, F., & Garcia-Garcia, C. (2026). OntoNanoMat: A Semantic Dataset and Ontology for Green-Synthesized Nanomaterials in Environmental Remediation. DATA, 11(4). (WOS:001751775700001). https://doi.org/10.3390/data11040071

Roothaert, R., Schlobach, S., Massacci, F., Stork, L., & ACM. (2025). TIDO: The Threat Intelligence Decision Ontology. 82–89. (WOS:001665578100013). https://doi.org/10.1145/3731443.3771351

Santipantakis, G., Doulkeridis, C., & Brimos, P. (2026). Semantic data transformation, FAIRification and provenance for data spaces. DATA IN BRIEF, 66. (WOS:001722640200001). https://doi.org/10.1016/j.dib.2026.112675

Sarquah, K., Narra, S., Beck, G., & Derkyi, N. (2026). Multivariate Techno-Economic Feasibility of Refuse-Derived Fuel Production in Ghana Using Response Surface Methodology: Insights from a Pilot-Scale System. CLEAN TECHNOLOGIES, 8(1). (WOS:001700919400001). https://doi.org/10.3390/cleantechnol8010017

Sawant, R., Kumbhar, A., Patil, A., Nalawade, G., Gona, J., & Bansal, S. (2025). KG-ITP: A Knowledge Graph for Intelligent Travel Planning (H. Shahriar, K. Alam, H. Ohsaki, S. Cimato, M. Capretz, S. Ahmed, S. Ahamed, A. Majumder, M. Haque, T. Yoshihisa, A. Cuzzocrea, M. Takemoto, N. Sakib, & M. Elsayed, Eds.; pp. 381–390). (WOS:001575960000050). https://doi.org/10.1109/COMPSAC65507.2025.00058

Schubert, T., Ibrahim, M., Breitmoser-Widdecke, N., Durak, U., & IEEE. (2025). An Ontology-based Automation Framework for Continuous Compliance of Airborne Software. (WOS:001665766800188). 2025 AIAA DATC/IEEE 44TH DIGITAL AVIONICS SYSTEMS CONFERENCE, DASC. https://doi.org/10.1109/DASC66011.2025.11257376

Tafech, A., & Rabhi, F. (2025). CEDAR: An Ontology-Based Framework Using Event Abstractions to Contextualise Financial Data Processes. ELECTRONICS, 15(1). (WOS:001657332700001). https://doi.org/10.3390/electronics15010145

Tauqeer, A., Chhetri, T., David, R., Ahmeti, A., & Fensel, A. (2026). An integrated approach to GDPR-compliant data sharing employing consent, contracts, and licenses. DATA & KNOWLEDGE ENGINEERING, 162. (WOS:001635128500001). https://doi.org/10.1016/j.datak.2025.102510

Thalhath, N., Nagamori, M., & Sakaguchi, T. (2025). Metadata application profile as a mechanism for semantic interoperability in FAIR and open data publishing. DATA AND INFORMATION MANAGEMENT, 9(1). (WOS:001591127500005). https://doi.org/10.1016/j.dim.2024.100068

Tufek, N., Thuluva, A., Just, V., Ekaputra, F., Bandyopadhyay, T., Sabou, M., & Hanbury, A. (2025). Validating Semantic Artifacts with Large Language Models (A. Penuela, O. Corcho, P. Groth, E. Simperl, V. Tamma, A. Nuzzolese, M. Poveda-Villalon, M. Sabou, V. Presutti, I. Celino, A. Revenko, J. Raad, B. Sartini, & P. Lisena, Eds.; Vol. 15344, pp. 92–101). (WOS:001447374600009). https://doi.org/10.1007/978-3-031-78952-6_9

Wang, B., De Sousa, L., Fensel, A., & ACM. (2025). Make soil healthy again: Construction of ontology-compliant soil health knowledge graph with large language models. 56–60. (WOS:001665578100009). https://doi.org/10.1145/3731443.3771730

Wang, S., Wu, J., Wu, Y., & Dong, W. (2025). Study on Separation of Desulfurization Wastewater in Ship Exhaust Gas Cleaning System with Rotating Dynamic Filtration. MEMBRANES, 15(7). (WOS:001535474200001). https://doi.org/10.3390/membranes15070214

Wei, Y., Qian, Y., Su, Z., Xu, X., Kong, D., Zhong, J., & Wang, H. (2025). Experimental investigation of a biomimetic propeller coupled with owl-inspired leading and trailing edges serrations. PHYSICS OF FLUIDS, 37(4). (WOS:001471701100006). https://doi.org/10.1063/5.0266266

Zghal, S., & Kachroudi, M. (2026). The co-evolution of ontologies and extensive knowledge graphs on a web scale. JOURNAL OF SUPERCOMPUTING, 82(5). (WOS:001716951100002). https://doi.org/10.1007/s11227-026-08380-1

Zhang, H., Zhao, H., Ge, H., Zhai, R., Wu, L., & Bai, B. (2025). Regulation mechanisms and kinetic characterization of nonionic surfactants on bituminous coal wettability across multiple scales. SURFACES AND INTERFACES, 79. (WOS:001637724800001). https://doi.org/10.1016/j.surfin.2025.108193

Editor
R. Andrew Paskauskas (MRU)

Contributors
Evaldas Bruze (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)
Saulius Kvedaravičius (MRU)

Reviewers
Evaldas Bružė (MRU)
Giedrė Sabaliauskaitė (MRU)
R. Andrew Paskauskas (MRU)
Tomas Lavišius (MRU)
Saulius Kvedaravičius (MRU)

Disclaimer