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: ***CTI-Balanced***

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

Action result: ***CTI-balanced Case, Comparative, and Content Analysis***

CTI-balanced Case, Comparative, and Content Analysis

Table of Contents

Introduction

Since the cyber threat intelligence-based sector and national collective cybersecurity are relatively new phenomenon, there are not enough effective methods developed. Moreover, there are no well-tested methodologies, approaches, processes, procedures and automation for cyber threat intelligence management; therefore, most countries are struggling in this domain with non-functioning solutions.

The project "Cyber threat intelligence-based Sectorial and National collective cybersecurity balanced incentives system (CTI-balanced)" concentrates on the above-mentioned problem by developing a prototype (later on developed into a product), allowing nations to implement national or a sectorial cyber threat management.

This document provides a comprehensive case, comparative, and content analysis regarding implementation aspects related to CTI-related data sharing on cyber incidents, GDPR requirement implementation and other relevant challenges

A cyber threat management system under development should operate across different EU Member States and utilize a plug-in for data monitoring. Therefore it requires navigating a balance between necessary security measures and strict privacy (GDPR) and Artificial Intelligence (AI Act) requirements.

This document explores real-world examples of cyber threat intelligence and how they are currently being addressed. This will provide insights into the challenges and limitations of existing approaches and inform the development of new models and methods for cyber threat intelligence.

The case analysis involves examining real-world cases to gain insights into the implementation of similar projects. This approach can provide valuable information on how GDPR and cybersecurity principles have been applied in practice and what challenges or limitations may exist.

The comparative and content analysis involves comparing and contrasting different approaches to privacy and security legal issues, also in order to identify best practices or areas for improvement.

1. Hypothetical Case Study: Implementation of the "CTI-Balanced" System

This analysis outlines the practical implementation of the "Cyber threat intelligence-based Sectorial and National collective cybersecurity balanced incentives system" (CTI-balanced). The system functions as a plug-in for data monitoring, collecting IP addresses, hostnames, and metadata to manage cyber threats across EU Member States.

1.1. Analysis of the Regulatory Environment

The regulatory environment for the CTI-balanced system is defined by a convergence of data protection laws, AI regulation, and cybersecurity directives. The system operates in a "dual-use" context, requiring a strict distinction between civil applications (subject to GDPR and AI Act) and national security/defense applications.

- The AI Act[1] (Risk-Based Approach): The system uses AI for threat analysis and anomaly detection. Under the AI Act, tools used in critical infrastructure or democratic processes (e.g., election protection) are classified as **High-Risk AI Systems**. This mandates conformity assessments, risk management systems, and human oversight. Furthermore, strict "red lines" exist: the system is prohibited from using AI for "untargeted scraping of facial images" (e.g., to build bot databases) or biometric categorization of political opinions (Article 5).
- GDPR[2] and CJEU Jurisprudence (Data Retention & Automated Decisions): Since the system processes IP addresses and traffic data (metadata), it handles personal data.

[1] Artificial Intelligence Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689
[2] General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

- Data Retention: The CJEU ruling in *La Quadrature du Net* (C-511/18)[3] establishes that "mass and indiscriminate" retention of traffic data for preventive purposes is banned for general crime-fighting. It is only permissible when there is a "genuine and present or foreseeable" threat to national security. For civil/commercial use, the system must utilize a **"Quick Freeze"** approach, retaining data only when a specific suspicion arises.
- Automated Decision-Making: If the CTI-balanced system assigns a "risk score" to an IP address that results in automatic blocking, this falls under **GDPR Article 22.** The *SCHUFA Holding* (C-634/21)[4] ruling confirms that an algorithmic score determining a decision constitutes ADM, requiring human intervention options and safeguards.
- Transparency: Under the *Dun & Bradstreet* (C-203/22) [5]ruling, users blocked by the system have a right to know the "logic involved." Trade secrets cannot be used to withhold the key parameters of the decision.

- NIS2 Directive[6] and National Transposition (Lithuania): The system supports the NIS2 objective of strengthening resilience in critical sectors. In Lithuania, the Law on Cybersecurity[7] transposes NIS2, mandating information sharing and incident management. The system must facilitate data exchange between the National Cybersecurity Center (NKSC) and private "cybersecurity entities".

1.2. Compliance Mapping

This checklist maps the CTI-balanced system's features to specific legal provisions:

- **Prohibited** Practices Check (AI Act Art. 5): Ensure no untargeted scraping of facial images and no biometric categorization of political opinions.
- High-Risk Classification (AI Act): If used for critical infrastructure or democratic processes, perform conformity assessments and implement a risk management system.
- Data Retention Strategy (ePrivacy Directive[8] & ***La Quadrature du Net***): Implement "Quick Freeze" capabilities for civil use; disable mass indiscriminate retention unless a national security threat is declared.
- Automated Decision Safeguards (GDPR Art. 22 & ***SCHUFA***): If the system automatically blocks threats based on scoring, ensure a mechanism for human intervention and contestation is available.
- Right to Explanation (GDPR Art. 15 & ***Dun & Bradstreet***): Prepare intelligible explanations of the "logic involved" in risk scoring, disclosing key parameters without hiding behind trade secrets.
- Pseudonymization Effectiveness (***EDPS v SRB***)[9]: Ensure that shared data cannot be re-identified by the recipient without additional information.
- Data Protection Impact Assessment (DPIA): Conduct a DPIA prior to deployment, as required for high-risk AI and data processing.
- Security Certification (Cyber Resilience Act)[10]: Align with European cybersecurity certification schemes (e.g., Managed Security Services) to demonstrate "presumption of conformity".

1.3. Most Important Stages of Implementation

[3] CJEU Case C-511/18 - La Quadrature du Net and Others, 2020. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18
[4] CJEU Case C-634/21 - SCHUFA Holding AG, 2023. https://curia.europa.eu/juris/liste.jsf?num=C-634/21
[5] CJEU Case C-203/22 - Dun & Bradstreet Austria GmbH, 2025. https://curia.europa.eu/juris/liste.jsf?num=C-203/22
[6] NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
[7] Law of the Republic of Lithuania on Cybersecurity https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr
[8] Directive on privacy and electronic communications: https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng
[9] CJEU Case C-413/23 - EDPS v SRB, 2025. https://curia.europa.eu/juris/document/document.jsf?text=&docid=305584&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8121207
[10] The Cyber Resilience Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847

1. Design & Architecture (Privacy by Design): Defining data flows and minimizing collection.
2. Pre-Deployment Assessment: Legal classification and risk analysis.
3. Operational Data Processing: Real-time monitoring, retention, and sharing.
4. Incident Response & Transparency: Acting on threats and explaining decisions to affected parties.

1.4. Practical Steps at Each Stage

Stage 1: Design & Architecture

- Implement "Quick Freeze" by Default: Architect the system to monitor traffic in real-time but *only* commit data to storage when a specific anomaly or threat signature is detected.
- Data Minimization: Configure the plug-in to collect only headers and metadata necessary for threat identification, avoiding full packet content unless legally authorized.
- SME-Friendly Automation: Develop a lightweight version for SMEs (similar to the Danish "MinVirksomhed" model)[11] that automates reporting without requiring extensive manual resources.

Stage 2: Pre-Deployment Assessment

- Draft a Template DPIA: Create a standardized Data Protection Impact Assessment template for clients (data controllers), addressing risks like "algorithmic bias" and "loss of human agency".
- Dual-Use Classification[12]: Clearly define the end-user. If the client is a defense entity, specific AI Act exemptions may apply; if civil, full compliance is mandatory.
- Certification Preparation: Apply for certification under the "Managed Security Services" scheme to ensure cross-border validity and avoid market fragmentation.

Stage 3: Operational Data Processing

- Pseudonymization for Sharing: When sharing threat intelligence with EU institutions, use advanced pseudonymization. Ensure the recipient (e.g., another Member State's agency) does not possess the "key" to re-identify the data subjects, complying with *EDPS v SRB*.
- Targeted FIMI Detection: Calibrate AI to detect "inauthentic behavior patterns" (e.g., bot farms) rather than profiling individuals. Document this distinction to prove compliance with the prohibition on political profiling.

Stage 4: Incident Response & Transparency

- Explainable AI Dashboard: Develop a user interface that explains why an IP was blocked. It must display the "key parameters" (e.g., "high frequency of requests," "known malicious signature") to satisfy the *Dun & Bradstreet* requirement.
- Liability Protection: Maintain audit logs proving the system operated within its "security by design" parameters. This is crucial because, under *Deutsche Wohnen*[13], fines are imposed only for "intent or negligence".

1.5. Practical Challenges Due to Lack of Legal Clarity/Specificity

- The "National Security" Boundary:

[11] Visions and recommendations for Denmark as a digital pioneer. Danish government digitization partnership. https://en.digst.dk/media/w4oft5kd/visions-and-recommendations-for-denmark-as-a-digital-pioneer-danish-government-digitisation-partnership.pdf

[12] Dual-Use Regulation (2021/821): https://eur-lex.europa.eu/eli/reg/2021/821/2024-11-08/eng

[13] CJEU Case C-807/21 - Deutsche Wohnen, 2023. https://curia.europa.eu/juris/document/document.jsf?text=&docid=282192&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8123480

- *Challenge:* The CJEU allows mass data retention only for "genuine and present" national security threats. However, the distinction between a "serious crime" (cybercrime) and a "national security threat" (state-sponsored cyberattack) is often blurred in hybrid warfare.
- *Practical Friction:* The CTI-balanced system may struggle to legally justify mass retention of data during a cyber campaign that *looks* like criminal ransomware but is actually state-sponsored sabotage, potentially delaying the "quick freeze" trigger.

- "Logic Involved" vs. Security Secrecy:
  - *Challenge:* The *Dun & Bradstreet* ruling requires revealing the logic of automated decisions.
  - *Practical Friction:* Revealing too much about how the CTI-balanced system detects threats (the "key parameters") could allow malicious actors to reverse-engineer the defense. Finding the balance between the legal right to explanation and operational security (OPSEC) remains a grey area.

- Pseudonymization Re-identification Risks:
  - *Challenge:* Data is considered non-personal only if the recipient cannot re-identify it.
  - *Practical Friction:* In a "collective cybersecurity" environment, different members may have different datasets. By combining the shared pseudonymized CTI data with their own local logs, a recipient might inadvertently re-identify users, retroactively triggering GDPR obligations for the sender.

2. Real-world case analysis

Based on the analysis of the regulatory environment (GDPR, AI Act), here is a detailed analysis of particular ventures specializing in similar (however, not identical) area of activity. Each company is evaluated separately using the criteria established in the hypothetical case analysis of the CTI-balanced.

2.1. Anomali

As it is seen from official sources, core philosophy of Anomali is the "Agentic SOC" and Unified Security Data Lake. Primary Focus: Transitioning from a traditional Threat Intelligence Platform (TIP) to a complete security analytics and autonomous response platform[14].

AI Implementation & Compliance (AI Act)

- **Agentic AI:** Anomali utilizes "Agentic AI" which goes beyond simple chatbots. These agents autonomously reason across the data lake to recommend actions and automate response workflows.
- **Proprietary Algorithms:** The platform uses the **MACULA** machine learning algorithm to automate risk scoring and remove false positives.
- **Regulatory Context:** The use of autonomous agents (Agentic AI) in critical infrastructure protection likely categorizes this as a High-Risk AI system under the EU AI Act, requiring strict human oversight capabilities. Anomali addresses this by keeping the human analyst in the loop for final decision-making while automating the "triage" phase.

Data Governance & Sovereignty (GDPR)

- **Unified Security Data Lake:** Anomali has moved away from the limitations of traditional SIEMs by creating a data lake that allows for massive retention of historical logs. This supports the GDPR requirement for accountability (audit trails) but requires strict data minimization policies to avoid hoarding unnecessary personal data.
- **Deployment Flexibility:** Anomali supports on-premises and **air-gapped** environments. This is a critical feature for EU entities requiring strict data sovereignty to ensure sensitive personal data does not leave their jurisdiction, complying with strict GDPR data transfer rules.
- **Privacy Controls:** The platform supports "Private Tags" and "Trusted Circles," allowing organizations to share intelligence (e.g., via ISACs) while controlling exactly what data is exposed to partners, ensuring pseudonymization protocols are respected.

Operational Implementation

- **Speed:** The architecture claims to reduce threat investigation time by 96% and allows searching years of data in seconds. This supports the "Quick Freeze" requirement discussed previously, enabling analysts to rapidly isolate data relevant to a threat before it is overwritten.

Primary Challenge: Displacement of Legacy Architecture & Platform Rigidity

- **The "SIEM Tax" & Displacement Gamble:** Anomali's 2026 strategy hinges on replacing traditional Security Information and Event Management (SIEM) systems with its "Unified Security Data Lake" and "Agentic SOC". The challenge lies in convincing large enterprises to rip and replace entrenched legacy infrastructure. While Anomali claims to reduce costs by 60% and eliminate data retention trade-offs, displacing legacy vendors remains a high-friction sales cycle requiring proof that their "Agentic AI" can reliably handle tasks previously managed by human teams without hallucination or failure.
- **Customization vs. "Plug-and-Play" Rigidity:** While Anomali is praised for immediate value, user feedback highlights a lack of flexibility for mature organizations. Reviews note that the platform's API

[14] The most of the information about Anomali is retrieved from the official website: https://www.anomali.com/

and customization options can be "rigid," making it difficult to adapt to highly unique or complex internal workflows that fall outside standard use cases.

- **Proof of ROI amid AI Scrutiny:** With Forrester predicting that enterprises will defer 25% of AI spend in 2026 due to inflated promises, Anomali faces the pressure of proving that its "Agentic AI" delivers tangible financial value, not just technical novelty. The market is demanding evidence that these agents actually reduce the need for headcount or tangibly stop breaches, moving beyond the "hype" phase.

2.2. ThreatConnect (Acquired by Dataminr)

Dataminr's core philosophy: Risk-Informed Intelligence and "Client-Tailored" Operations. Primary Focus: Quantifying cyber risk in financial terms and fusing external real-time signals with internal data. Note: In late 2025, Dataminr announced the acquisition of ThreatConnect[15].

AI Implementation & Compliance (AI Act)

- **Client-Tailored Intelligence:** Post-acquisition, the platform integrates Dataminr's "AI Agents" and 50+ proprietary Large Language Models (LLMs). These agents fuse external public data with internal client data to create personalized intelligence.
- **Risk vs. Profiling:** The AI focuses on "Risk Quantification" rather than profiling individuals. This distinction is vital for AI Act compliance, as it avoids prohibited practices related to biometric categorization or social scoring, focusing instead on financial and operational risk.

Data Governance & Sovereignty (GDPR)

- **Risk Quantifier (RQ):** This module translates technical threats into financial terms (e.g., potential loss in euros). This directly supports GDPR Article 32 (Security of Processing) and Article 35 (DPIA) by helping organizations assess the "severity of the risk to the rights and freedoms of natural persons" in economic terms.
- **Internal + External Fusion:** The integration fuses internal client environments with external data. From a GDPR perspective, this requires rigorous data mapping to ensure that internal personal data (employee logs, customer IPs) is not inadvertently exposed to the external "public data" models used by Dataminr.

Operational Implementation

- **TI Ops (Threat Intel Operations):** The platform emphasizes "operationalizing" intelligence via automated playbooks. This aligns with NIS2 requirements for incident response, ensuring that threat intelligence leads to immediate, traceable actions (e.g., blocking an IP) rather than just passive monitoring.

Primary Challenge: Post-Acquisition Integration & Usability Friction

- **The Integration of "Internal" and "External" Worlds:** Following Dataminr's $290M acquisition of ThreatConnect in late 2025, the primary challenge is technical and cultural integration. Merging Dataminr's real-time, public-signal AI (external data) with ThreatConnect's complex internal workflow automation (internal data) is a massive engineering feat. The combined entity must deliver a seamless "Client-Tailored Intelligence" experience without creating a disjointed user interface or data silos.
- **Playbook Complexity and Documentation:** Operational friction remains a hurdle. User reviews explicitly cite "confusion and lack of proper documentation" regarding Playbook design. Users have noted that as playbook complexity increases, the software's potential is hindered, preventing teams

[15] The most of the information about Dataminr is retrieved from the official website: https://www.dataminr.com/

from fully maximizing benefits. The visual coding interface, intended to help non-programmers, has been criticized for lacking the flexibility of a code-centric approach for complex problems.

- **Adoption of Risk Quantification (RQ):** ThreatConnect differentiates itself with "Risk Quantification," translating cyber threats into dollar amounts. The challenge is educational and cultural: convincing CISOs and Boards to trust automated financial modeling over traditional qualitative assessments. As regulatory pressure mounts (e.g., DORA, NIS2), the accuracy of these financial models will be scrutinized by auditors.

2.3. EclecticIQ

The core philosophy of ElectricIQ: Analyst-Centric, "Sovereign" Defense. Primary Focus: Serving European critical infrastructure, National SOCs, and strictly regulated sectors with a focus on "finished intelligence"[16].

AI Implementation & Compliance (AI Act)

- **"Bring Your Own LLM" (BYO-LLM):** This is a standout feature for compliance. EclecticIQ allows customers to choose their own AI models or host them on-premises. This ensures that sensitive data processed by AI does not leave the organization's control, mitigating the risk of data leakage into public AI models, a key concern under the AI Act for high-risk systems.
- **AI Suite:** Features include summarization and translation to speed up investigations, positioning AI as an "assistant" to the human analyst rather than a fully autonomous agent, ensuring "Human-in-the-loop" compliance.

Data Governance & Sovereignty (GDPR)

- **European Sovereignty (The "Cybus" Model):** EclecticIQ explicitly advocates for a "European ecosystem" to ensure digital sovereignty, comparable to Airbus in aerospace. This strategy is designed to meet strict EU regulatory requirements (GDPR, NIS2) by keeping technology and data within the EU jurisdiction.
- **Advanced Data Modeling (Custom Objects):** The platform supports "Custom Objects" based on the STIX standard, allowing users to model complex data (e.g., blockchain flows, GDPR compliance evidence) without forcing it into ill-fitting categories. This flexibility aids in maintaining accurate records of processing activities.

Operational Implementation

- **Standardization:** The platform is built heavily around the **STIX/TAXII** standards, promoting interoperability between EU member states. This is crucial for the "collective cybersecurity" initiatives mandated by EU regulations, allowing cross-border threat sharing without technical friction.

Primary Challenge: Complexity of "Finished Intelligence" & Sovereignty Limits

- **High Skill Barrier for Custom Modeling:** EclecticIQ's differentiator is its handling of "Custom Objects" and complex data modeling (e.g., tracking blockchain flows or fraud) via STIX extensions. The challenge is that this requires highly skilled analysts who understand data modeling. In a market suffering from a "lack of experts", the platform's sophistication may be a barrier to entry for less mature organizations that simply want automated blocklists rather than deep, structured intelligence analysis.
- **The "Sovereign Cloud" Double-Edged Sword:** EclecticIQ champions the "Cybus" model, a distinct European ecosystem to ensure digital sovereignty and reduce reliance on US vendors. While this secures their position in the EU government and defense sectors, it challenges their ability to scale

[16] The most of the information about EclecticIQ is retrieved from the official website: https://www.eclecticiq.com/

globally against US-centric competitors like CrowdStrike or Anomali. They must balance strict European data localization requirements with the need to serve global multinationals.

- **Structuring Unstructured Data:** A core operational challenge is the processing of "messy" intelligence. While their new AI Suite offers summarization and translation, relying on "Bring Your Own LLM" (BYO-LLM) pushes the burden of model selection and governance onto the client. Ensuring that client-selected LLMs do not hallucinate when processing critical "finished intelligence" reports is a significant risk.

2.4. Summary of Common Industry Challenges (2026)

- **The "Agentic" Trust Gap:** All three companies are pivoting to "Agentic AI" (AI that takes action, not just chats). The industry-wide challenge is overcoming the "trust gap", ensuring these autonomous agents do not disrupt critical operations or hallucinate during automated response.
- **Talent Shortage vs. Tool Complexity:** As threats become more complex (e.g., deepfakes, quantum threats), platforms are becoming more sophisticated. However, the "skills gap" means there are fewer analysts capable of utilizing these advanced features (like EclecticIQ's custom STIX objects or ThreatConnect's advanced playbooks).
- **Regulatory Compliance Cost:** Adapting to aggressive new frameworks (NIS2, DORA[17], AI Act) requires constant platform updates to ensure "Digital Provenance" and "Explainability," adding development overhead for all vendors.

[17] Digital Operational Resilience Act: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

3. Comparative analysis of different legal approaches within the EU legal framework

This comparative analysis evaluates implementation scenarios for the CTI-balanced project (Cyber threat intelligence-based Sectorial and National collective cybersecurity balanced incentives system). The analysis draws on the main legal texts (GDPR, AI Act, NIS2, DORA, etc.) and specific case studies regarding the project's operational environment within the EU legal framework.

3.1. Analysis of the Regulatory Environment

The regulatory environment for the CTI-balanced project is characterized by a tension between the mandate to share threat intelligence (NIS2[18], DORA[19]) and strict limitations on processing personal data (GDPR[20], ePrivacy[21], AI Act[22]).

The "Dual-Use" Nature: The project operates in a regulatory environment that distinguishes strictly between civil/commercial applications and national security/defense applications. The AI Act explicitly excludes systems used exclusively for military, defense, or national security purposes from its scope. However, the CTI-balanced project, aiming for "sectorial and national collective cybersecurity," likely falls under the High-Risk classification of the AI Act when used for critical infrastructure or democratic processes.

The "Sharing" Mandate: The NIS2 Directive mandates that Member States ensure essential entities notify CSIRTs of significant incidents and encourages voluntary information sharing. Similarly, DORA requires financial entities to manage ICT third-party risk and allows voluntary cyber threat information sharing within trusted communities.

The "Privacy" Constraint: The ePrivacy Directive and GDPR restrict the processing of traffic and location data. The CJEU ruling in La Quadrature du Net[23] establishes that "mass and indiscriminate" retention of traffic data is prohibited for general crime-fighting and is only permissible in the face of a "genuine and present or foreseeable" threat to national security.

3.2. Implementation Scenarios and Opportunities

The following section contrasts two primary implementation scenarios: Scenario A (Civil/Commercial Compliance) and Scenario B (National Security/Defense Exemption).

3.2.1. Encryption

Legal Context: DORA mandates policies on the use of cryptography and encryption for data at rest, in use, and in transit. NIS2 promotes the use of end-to-end encryption to safeguard public electronic communications.

Scenario A (Civil): The CTI-balanced plug-in must implement state-of-the-art encryption. However, for threat detection, the system often requires visibility into traffic.

Opportunity: Use Privacy-Enhancing Technologies (PETs). The system can process encrypted traffic metadata (headers, flow size, timing) without decrypting the payload, complying with the ePrivacy Directive which protects confidentiality.

[18] NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
[19] Digital Operational Resilience Act: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
[20] General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
[21] Directive on privacy and electronic communications: https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng
[22] Artificial Intelligence Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689
[23] CJEU Case C-511/18 - La Quadrature du Net and Others, 2020. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18

Scenario B (Defense): Encryption standards may be dictated by national classified information acts rather than GDPR.

Opportunity: The Defence Readiness Omnibus aims to simplify intra-EU transfers of such defense-related technologies.

3.2.2. Data Minimization

Legal Context: GDPR Article 5 requires data to be "adequate, relevant and limited to what is necessary".

Scenario A (Civil): The "Quick Freeze" Approach.

Implementation: The system monitors traffic in real-time but does not commit data to storage by default. Storage is triggered only when a specific threat signature or anomaly is detected. This aligns with the La Quadrature du Net ruling, which prohibits general retention but allows targeted retention.

Advantage: Drastically reduces GDPR liability and storage costs.

Scenario B (Defense): Broader data collection is permitted under the "national security" exception of GDPR Art. 2(2) and ePrivacy Art. 15.

Pitfall: Mixing civil and defense data streams can contaminate the dataset, making the entire system subject to stricter civil liability if not strictly segregated.

3.2.3. Procedural Aspects

Legal Context: NIS2 requires entities to notify competent authorities of significant incidents without undue delay (early warning within 24 hours). The AI Act requires a fundamental rights impact assessment for high-risk systems deployed by public bodies.

Scenario A (Civil): Automated Compliance.

Implementation: The CTI-balanced system should include a "Template DPIA" (Data Protection Impact Assessment) for its clients. It should automate the NIS2 reporting workflow to reduce the administrative burden on SMEs.

Scenario B (Defense): Focus is on interoperability with NATO standards (e.g., NATO's Data Centric Reference Architecture)[24] rather than civil reporting obligations.

3.2.4. Limiting Access to Data

Legal Context: DORA emphasises access control policies. The CJEU ruling EDPS v SRB[25] clarifies that pseudonymized data is only considered "non-personal" if the recipient cannot re-identify the subject.

Implementation:

The "Key" Separation: When the CTI-balanced system shares data between Member States (e.g., from a National Cybersecurity Center to a private sector entity), it must strip identifiers. Crucially, the "key" to re-identify the IP address must remain with the sender. If the recipient does not possess the means to re-identify, the data sharing is less burdened by GDPR.

3.2.5. Red Lines, Privacy Impact, and Automated Decisions

Legal Context:

Red Lines: The AI Act prohibits AI systems that create facial recognition databases through untargeted scraping or use biometric categorization to infer political opinions.

[24] Data Centric Reference Architecture for the Alliance: https://nhqc3s.hq.nato.int/apps/DCRA_Report/index.html

[25] CJEU Case C-413/23 - EDPS v SRB, 2025. https://curia.europa.eu/juris/document/document.jsf?text=&docid=305584&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8121207

Automated Decision-Making (ADM): GDPR Article 22 protects individuals from solely automated decisions. The CJEU SCHUFA ruling[26] confirms that a "risk score" leading to a decision constitutes ADM. The Dun & Bradstreet ruling[27] mandates that users have a right to know the "logic involved" in such scores; trade secrets cannot block this transparency.

Implementation Strategy:

No Black Boxes: The CTI-balanced system cannot simply label an IP as "Malicious" using a proprietary "black box" algorithm. It must display the "key parameters" (e.g., "high frequency of port scanning") to the operator to satisfy the transparency requirement.

Human-in-the-Loop: To avoid the strict prohibition on solely automated decisions, the system should propose a block, requiring human confirmation, or provide a robust mechanism for contesting the decision.

FIMI Distinction: The system must be calibrated to detect "inauthentic behavior patterns" (bot farms) rather than profiling individuals' political views, avoiding the AI Act's prohibition on biometric categorization.

3.3. Conclusion for EU legal framework

The most viable path for the CTI-balanced project is to architect the system as a High-Risk AI System under the AI Act, incorporating "Security by Design" and "Privacy by Design." It should utilize "Quick Freeze" protocols to satisfy the strict data retention limits imposed by the CJEU on civil entities, while maintaining a technical capability for broader retention that can only be unlocked by a certified "National Security" user under specific legal authorization. This hybrid model captures the market opportunity of the NIS2 compliance wave while respecting the "red lines" of the AI Act.

[26] CJEU Case C-634/21 - SCHUFA Holding AG, 2023. https://curia.europa.eu/juris/liste.jsf?num=C-634/21
[27] CJEU Case C-203/22 - Dun & Bradstreet Austria GmbH, 2025. https://curia.europa.eu/juris/liste.jsf?num=C-203/22

4. Comparative analysis from the national legal perspective of the Republic of Lithuania

This comparative analysis evaluates implementation scenarios for the CTI-balanced project within the regulatory framework of the Republic of Lithuania. The analysis is based on the transposition of the EU NIS2 Directive into national law (Law on Cybersecurity[28]), specific government resolutions detailing technical requirements[29], and the Law on Legal Protection of Personal Data in Law Enforcement and National Security[30].

4.1. Analysis of the Regulatory Environment

The Lithuanian regulatory environment is defined by a rigid segmentation between Civil/Commercial Cybersecurity (governed by the Law on Cybersecurity and GDPR) and National Security/Defense (governed by specific exemptions and the Law on Personal Data for Law Enforcement).

The "NIS2" Transposition: The new version of the Law on Cybersecurity (CS Law) serves as the primary framework. It categorizes organizations into Essential (esminiai) and Important (svarbūs) entities. This law explicitly mandates compliance with specific risk management measures and reporting obligations, creating a "compliance market" for the CTI-balanced project.

The "State" Network: A unique feature of the Lithuanian framework is the Secure State Data Transfer Network (Saugusis tinklas). Specified state institutions and critical entities must use this network for internet access and data exchange, effectively creating a "walled garden" for high-value targets.

The "Law Enforcement" Exception: Processing personal data for national security or defense is governed by a separate law (Law on Personal Data in Law Enforcement/National Security), which allows for broader data collection and processing than GDPR, provided it is necessary and proportionate.

4.2. Implementation Scenarios and Opportunities

The following section contrasts Scenario A (Civil/Commercial Implementation) under the Law on Cybersecurity and Scenario B (National Security/Defense Implementation) under the Law on Personal Data in Law Enforcement.

4.2.1. Encryption

Legal Context: The Cybersecurity Requirements Description mandates specific technical standards for encryption.

Scenario A (Civil/Commercial):

Mandatory Standards: The system must ensure that wireless connections use WPA2/WPA3 (or newer) encryption. Data transmitted via mobile devices or public networks must be encrypted via VPN or TLS/SSL.

Website Security: Public-facing elements must use HTTPS (TLS 1.3 or newer) and Web Application Firewalls (WAF).

Opportunity: The CTI-balanced project can market its compliance with these specific Lithuanian technical standards (e.g., failing securely for cryptographic modules).

Scenario B (Defense/State):

[28] Law of the Republic of Lithuania on Cybersecurity https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr

[29] National Cyber Incident Management Plan of the Republic of Lithuania. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr

[30] Law on Legal Protection of Personal Data in Law Enforcement and National Security of the Republic of Lithuania. https://e-tar.lt/portal/lt/legalAct/TAR.299D835159BE/asr

Implementation: Entities on the Secure Network receive collective protection and encryption services managed centrally by the network operator.

Constraint: The CTI-balanced project would need to integrate with this closed state network infrastructure rather than operating over the open internet for these clients.

4.2.2. Data Minimization and Retention

Legal Context: There is a conflict between "minimization" principles and "logging" mandates.

Scenario A (Civil/Commercial):

The "90-Day" Mandate: Unlike the general "Quick Freeze" preference in EU case law, Lithuanian regulations require Essential and Important entities to retain log records for at least 90 days.

Data Collection: The logs must capture specific data points: event date/time, event type, user/administrator ID, and device ID.

Opportunity: The CTI-balanced system can automate this mandatory 90-day retention cycle, ensuring logs are stored in specialized hardware/software as required.

Scenario B (Defense/State):

Broad Scope: Data processing is lawful if necessary for the prevention or investigation of criminal offenses or threats to public security.

Categorization: The system must distinguish between different categories of data subjects (e.g., suspects, victims, witnesses) to comply with the requirement to separate these data flows "as far as possible".

4.2.3. Procedural Aspects and Reporting

Legal Context: The National Cyber Incident Management Plan establishes strict timelines.

Scenario A (Civil/Commercial):

Reporting Windows: The system must automate reporting to the National Cyber Security Centre (NKSC).

24 Hours: Early warning of a significant incident.

72 Hours: Incident notification.

1 Month: Final report.

Automation Mandate: New regulations require entities to adapt their systems within 12 months to register incidents automatically via the National Cyber Incident Management Platform.

Opportunity: The CTI-balanced project provides immense value if it includes an API for automatic submission to the NKSC Platform, satisfying the 12-month upgrade mandate.

Scenario B (Defense/State):

Crisis Management: In the event of a large-scale incident, the NKSC coordinates with the National Crisis Management Centre (NKVC). The system must be capable of generating aggregated, anonymized situational reports for these high-level bodies.

4.2.4. Limiting Access to Data

Legal Context: Strict access control is mandated by the Cybersecurity Requirements Description.

Implementation:

MFA Mandate: The system must enforce Multi-Factor Authentication (MFA) for all users and administrators.

Segmentation: The network must be segmented (e.g., separate subnets for management, printers, third parties).

Administrator Control: Administrator rights must be reviewed annually, and separate accounts must be used for administrative vs. daily tasks. The system should automatically lock accounts after 5 failed attempts.

4.2.5. Red Lines and Automated Decisions

Legal Context:

Automated Decisions: The Law on Personal Data in Law Enforcement strictly prohibits decisions based solely on automated processing (including profiling) if they produce adverse legal effects, unless explicitly authorized by law with human intervention safeguards.

Profiling: Profiling that leads to discrimination based on special categories of data (race, politics, etc.) is prohibited.

NCSC Powers: The NCSC has the power to issue binding instructions to disconnect clients (up to 48 hours without court order) or block domains.

Implementation Strategy:

Human-in-the-Loop: The CTI-balanced system should generate "recommendations for blocking" rather than auto-blocking, to keep the decision-making human (the administrator) liable, complying with the prohibition on solely automated decisions.

Vulnerability Disclosure: The system must respect the 90-day embargo on disclosing vulnerabilities to third parties (unless the NCSC allows a shorter term).

4.3. Conclusion for Lithuania

Unlike the broader EU context where "Quick Freeze" is the dominant privacy paradigm, Lithuania explicitly mandates a 90-day retention period for logs for regulated entities. Therefore, the CTI-balanced project must technically support this retention duration to be viable. Furthermore, the mandatory automation of incident reporting to the NCSC offers a distinct competitive advantage for a tool that can handle this API integration natively. The project should "fork" a specific module dedicated to Essential Subjects (Esminiai subjektai) that enforces the strict technical controls (MFA, Segmentation, 90-day logs) outlined in the Government Resolution, while offering a lighter version for non-regulated entities.

5. Comparative analysis of selected cases outside the scope of the EU legal framework

This comparative analysis evaluates the regulatory environments of the United Kingdom and the United States for the CTI-balanced project. Unlike the EU's comprehensive statutory framework (AI Act), both the UK and US have adopted distinct, sovereignty-focused approaches that prioritize innovation and geopolitical dominance over precautionary regulation, though they achieve this through radically different legal mechanisms.

5.1. United Kingdom: "Regulated Flexibility" & Sectoral Oversight

The UK has explicitly rejected a monolithic "AI Law" in favor of a "context-based" framework. The regulatory environment is defined by the empowerment of existing regulators to apply cross-sectoral principles, backed by targeted legislation to reform digital markets and data protection.

The "Pro-Innovation" Framework: The UK's approach relies on five non-statutory principles (Safety, Transparency, Fairness, Accountability, Redress) which regulators (like the CMA, ICO, and Ofcom) interpret for their specific sectors.

Legislative Pillars:

Data (Use and Access) Act 2025 (DUAA)[31]: A major reform of the UK GDPR designed to reduce compliance burdens. It introduces "recognised legitimate interests" and relaxes rules on automated decision-making.

Digital Markets, Competition and Consumers Act 2024 (DMCCA)[32]: Establishes the "Strategic Market Status" (SMS) regime to regulate big tech firms (like Google and Apple) with tailored codes of conduct.

AI Opportunities Action Plan (Jan 2025)[33]: Focuses on building "sovereign AI" capabilities, creating AI growth zones, and mobilizing public data.

Implementation Scenarios (UK)

5.1.1. Encryption

Scenario: The CTI-balanced project can leverage the UK's strong cybersecurity focus. The Online Safety Act 2023[34] and PECR (amended by DUAA) emphasize security but also align with law enforcement needs.

Opportunity: The DUAA facilitates data sharing for "national security" and "crime prevention" under "recognised legitimate interests," potentially simplifying the legal basis for sharing encrypted threat intelligence without complex balancing tests.

5.1.2. Data Minimization

Scenario: The DUAA loosens the strict "purpose limitation" of the EU GDPR. It allows further processing for "scientific research" or "compatible purposes" without seeking fresh consent.

Opportunity: The project can reuse collected threat data for research and model training more easily than in the EU, provided it falls under the broad definition of "commercial scientific research" now codified in law.

[31] Data (Use and Access) Act 2025. https://www.legislation.gov.uk/ukpga/2025/18/contents
[32] Digital Markets, Competition and Consumers Act 2024. https://www.legislation.gov.uk/ukpga/2024/13/contents
[33] AI Opportunities Action Plan. https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan
[34] Online Safety Act 2023. https://www.legislation.gov.uk/ukpga/2023/50

5.1.3. Procedural Aspects

Scenario: Compliance is regulator-led. The Information Commission (formerly ICO)[35] and Regulatory Innovation Office (RIO)[36] coordinate approvals.

Opportunity: The DRCF AI and Digital Hub offers a "multi-agency advisory service," allowing the project to get regulatory advice from multiple regulators (ICO, CMA, Ofcom) simultaneously, streamlining the launch process.

5.1.4. Limiting Access to Data

Scenario: The DMCCA mandates interoperability and data access for firms with "Strategic Market Status" (SMS).

Opportunity: If the project requires threat data from major platforms (e.g., cloud providers), the CMA's new powers could theoretically force these "gatekeepers" to share data with smaller players to ensure fair competition.

5.1.5. Red Lines & Automated Decisions

Scenario: The DUAA permits solely automated decision-making (ADM) for non-special category data, removing the human-in-the-loop requirement for many commercial decisions, provided safeguards (right to contest) are in place.

Opportunity: The CTI-balanced project can deploy fully automated threat blocking (ADM) more aggressively than in the EU, as long as it does not process sensitive personal data (e.g., biometrics) without consent.

5.2. United States: "Dominance-Led" Deregulation & Federal Preemption

The US regulatory environment in 2025/2026 is characterized by an aggressive Executive-led shift toward deregulation, infrastructure expansion ("Stargate"), and the dismantling of "precautionary" state-level rules.

The "America First" AI Doctrine: The Trump Administration revoked the Biden-era AI Executive Order (EO 14110) that focused on safety and equity. The new EO 14179[37] and AI Action Plan[38] prioritize "American AI Dominance," energy infrastructure, and removing "ideological bias" (DEI/safety constraints) from models.

Federal vs. State Conflict: A major dynamic is the federal government's active hostility toward state regulations (like California's SB 53[39] or Colorado's AI Act[40]). The DOJ has established an AI Litigation Task Force to sue states that enact "onerous" AI rules, arguing they interfere with interstate commerce.

Implementation Scenarios (USA)

5.2.1. Encryption

Scenario: Cybersecurity is framed as a national security imperative. The "Stargate" partnership ($500B infrastructure investment) focuses on building secure, high-power data centers.

[35] The Information Commission. https://ico.org.uk/
[36] Regulatory Innovation Office. https://www.gov.uk/government/organisations/regulatory-innovation-office
[37] Executive Order 14179 of January 23, 2025. Removing Barriers to American Leadership in Artificial Intelligence. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/
[38] America's AI Action Plan. https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf
[39] SB-53 Artificial intelligence models: large developers. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB53
[40] SB24-205 Consumer Protections for Artificial Intelligence. https://leg.colorado.gov/bills/sb24-205

Opportunity: High-level encryption standards are driven by national security requirements rather than consumer privacy. The project can position itself as a defense-adjacent tool to benefit from federal support for "secure" infrastructure.

5.2.2. Data Minimization

Scenario: The administration actively discourages data minimization if it hinders model training. The AI Action Plan seeks to "unlock" federal data and encourages the use of "high-quality data" as a strategic asset.

Opportunity: Extremely favorable environment for collecting vast datasets for training. The policy push is for more data access, not less, contrasting sharply with the EU's minimization principle.

5.2.3. Procedural Aspects

Scenario: Deregulation is the priority. Agencies are ordered to repeal regulations that hinder AI. However, this creates a "Wild West" where the rules are unclear because federal standards are being dismantled while state rules are being litigated.

Pitfall: Legal Uncertainty. The project faces a chaotic environment where complying with a state law (e.g., California's transparency act) might invite federal scrutiny or loss of federal funding.

5.2.4. Limiting Access to Data

Scenario: The focus is on National Security. Export controls are tightening to prevent "rivals" (China) from accessing US AI stacks or data.

Opportunity: If the project is US-aligned, it benefits from a protected market. If it involves cross-border data flows with non-allies, it faces severe friction.

5.2.5. Red Lines & Bias

Scenario: The administration defines "bias" differently - viewing DEI (Diversity, Equity, and Inclusion) guardrails as "ideological bias" that makes AI "deceptive".

Pitfall: The CTI-balanced project must be careful not to implement "equity" filters that the FTC might now deem "deceptive trade practices" under the new administration's interpretation. The mandate is for "truthful outputs" (unfiltered) rather than "safe" outputs.

5.3. Conclusion & Recommendation from non-EU cases

For the CTI-balanced project, the United Kingdom currently offers a superior operational environment due to legal certainty and alignment of interests:

Legal Certainty: The UK's DUAA 2025 provides a stable statutory basis for processing threat intelligence ("crime prevention" as a recognized legitimate interest) without the chaotic federal-state conflict seen in the US.

Automated Response: The UK's relaxation of Automated Decision-Making (ADM) rules for non-sensitive data allows the project to automate threat blocking legally, a critical capability for CTI systems.

Regulatory Support: The DRCF provides a clear mechanism to navigate overlap between competition, data, and communications regulators, whereas the US landscape is currently defined by litigation and inter-agency conflict.

Pitfall in the US: While the US offers vast infrastructure support and a pro-business rhetoric, the DOJ's war on state AI laws creates a compliance minefield. A tool compliant with California's transparency laws might be targeted by the Federal FTC for "ideological bias," putting the project in a "double bind".

Therefore, the UK's "Third Way" - diverging from the EU's rigidity but avoiding the US's volatility - is the most strategic launchpad for a collective cybersecurity system.

References

1. Artificial Intelligence Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689
2. General Data Protection Regulation: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
3. CJEU Case C-511/18 - La Quadrature du Net and Others, 2020. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18
4. CJEU Case C-634/21 - SCHUFA Holding AG, 2023. https://curia.europa.eu/juris/liste.jsf?num=C-634/21
5. CJEU Case C-203/22 - Dun & Bradstreet Austria GmbH, 2025. https://curia.europa.eu/juris/liste.jsf?num=C-203/22
6. NIS2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
7. Law of the Republic of Lithuania on Cybersecurity https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr
8. Directive on privacy and electronic communications: https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng
9. CJEU Case C-413/23 - EDPS v SRB, 2025. https://curia.europa.eu/juris/document/document.jsf?text=&docid=305584&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8121207
10. The Cyber Resilience Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847
11. Visions and recommendations for Denmark as a digital pioneer. Danish government digitization partnership. https://en.digst.dk/media/w4oft5kd/visions-and-recommendations-for-denmark-as-a-digital-pioneer-danish-government-digitisation-partnership.pdf
12. Dual-Use Regulation (2021/821): https://eur-lex.europa.eu/eli/reg/2021/821/2024-11-08/eng
13. CJEU Case C-807/21 - Deutsche Wohnen, 2023. https://curia.europa.eu/juris/document/document.jsf?text=&docid=282192&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8123480
14. Anomali. https://www.anomali.com/
15. Dataminr. https://www.dataminr.com/
16. EclecticIQ. https://www.eclecticiq.com/
17. Digital Operational Resilience Act: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
18. Union Rolling Work Programme for European cybersecurity certification. https://ec.europa.eu/newsroom/dae/redirection/document/102292
19. ISO/IEC 27034-1:2011 Information technology - Security techniques - Application security: https://www.iso.org/standard/44378.html#:~:text=Abstract,of%20the%20application%20is%20outsourced.
20. Apply AI Strategy (Communication from the Commission Artificial Intelligence for Europe) COM(2025) 723 final. https://eur-lex.europa.eu/resource.html?uri=cellar:194ae542-a421-11f0-97c8-01aa75ed71a1.0001.02/DOC_1&format=PDF
21. Law of the Republic of Lithuania on Cybersecurity. https://www.e-tar.lt/portal/it/legalAct/5468a25089ef11e4a98a9f2247652cf4/asr
22. National Cyber Incident Management Plan of the Republic of Lithuania. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr
23. Law on Legal Protection of Personal Data in Law Enforcement and National Security of the Republic of Lithuania. https://e-tar.lt/portal/lt/legalAct/TAR.299D835159BE/asr
24. Data (Use and Access) Act 2025. https://www.legislation.gov.uk/ukpga/2025/18/contents
25. Digital Markets, Competition and Consumers Act 2024. https://www.legislation.gov.uk/ukpga/2024/13/contents
26. AI Opportunities Action Plan. https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan

27. Online Safety Act 2023. https://www.legislation.gov.uk/ukpga/2023/50
28. The Information Commission. https://ico.org.uk/
29. Regulatory Innovation Office. https://www.gov.uk/government/organisations/regulatory-innovation-office
30. Executive Order 14179 of January 23, 2025. Removing Barriers to American Leadership in Artificial Intelligence. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/
31. America's AI Action Plan. https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf
32. SB-53 Artificial intelligence models: large developers. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB53
33. SB24-205 Consumer Protections for Artificial Intelligence. https://leg.colorado.gov/bills/sb24-205

Editor
<<Main Editor>>

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

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

Disclaimer