Article

Securing Low-Energy Data Centres in Sustainable Cybersecurity Infrastructure

Sujal Chhajed*, Aman Kumar Jha and Tanishk Bhawsar

National Law Institute University, Kerwa Dam Road, Bhopal-462044, India; tanishkbhawsar.bscllb@nliu.ac.in (T.B); amankumarjha.bscllb@nliu.ac.in (A.K.J)

* Correspondence: sujalchhajed.bscllb@nliu.ac.in

Abstract: The global digital economy exists on a physical paradox: whilst the 'cloud' is an industrial physical infrastructure that uses a lot of electricity, water and other raw materials to operate. The emergence of this paradox has led to a significant doctrinal tension between a government's obligation for cyber security against its government's obligation for environmental sustainability as the European Union continues with its "twin transition" of digitization and decarbonization. In the paper, I will provide an analysis of the legal and technical implications of this conflict by examining how the NIS 2 Directive, GDPR and the recast Energy Efficiency Directive relate to each other. Finally, I will explain that the move towards using "low-energy" infrastructure will create new vulnerabilities that are not being addressed under current liability frameworks due to the adoption of liquid cooled systems; IoT-driven environmental controls; and lightweight cryptography. In addition, this write up discusses the "Sanitization Paradox", which is a situation where data protection absolutism requires functional devices to be physically destroyed (shredded), creating a break in the circular economy for Critical Raw Material (CRM) commodities such as Neodymium and Cobalt. This write up synthesizes technical information related to "Green AI" and cryptographic efficiency with legal information regarding tort liability and regulatory compliance in order to propose a standard for "eco-efficient resilience" that balances the demands of security against the demands of sustainability.

Keywords: data centres, NIS 2 directive, circular economy, green AI, lightweight cryptography, digital sovereignty, critical raw materials

Citation: Sujal Chhajed, Aman Kumar Jha, and Tanishk Bhawsar. 2025. Securing Low-Energy Data Centres in Sustainable Cybersecurity Infrastructure. *Digital Social Sciences 2(2),* 1-5. https://doi.org/10.69971/dss.2.2.2025.36

Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license https://creativecommons.org/licenses/by/4.0/.

1. Introduction

For a long time now, the term "cloud" has been used to hide the real way we engage with technology during this time known as 'the digital era.' The digital ecosystem is made up of data storage facilities across the globe that use significant amounts of electricity (up to about 340 terawatts). The amount of energy these facilities will use is likely to increase dramatically, reaching 800 terawatts by 2026 due to increased demand from both artificial intelligence and cryptocurrency mining. (International Energy Agency 2024). The data storage community finds itself in the middle of the 'twin transition' policy agenda being pursued by the EU. On one hand, the purpose of the 'twin transition' is to achieve carbon neutrality by 2050; on the other hand, it is also intended to speed up the development and use of digital technologies around the world (Commins and Kristina 2025). While both doctrine and operations are currently undergoing a major change, the fundamental legal foundations supporting these two areas are contradictory. The laws that define cybersecurity's operation (i.e., the GDPR, the NIS2 Directive) are based upon creating redundant systems to reduce risk to consumers and, as a result, have created a paradigm in which "security by design" has been about exhausting the computing system's processing capability for example, extensive data back-up systems, the use of more electricity for encrypted data than unencrypted data, and rapid destruct-time[s] of computing hardware in order to decrease the possibility of lost consumer data through data breaches. On the other hand, the sustainability standard legislated by the EED (recast) and the Circular Economy Action Plan requires diminishing returns and usage through decreased electricity consumption, universal use of hardware beyond three years, and the extended use of hardware components.

These different types of laws create a type of "unsafe security" and "secure but not sustainable" environment. In order to operate low-power data centers, you have to connect Industrial Internet of Things (IIoT.) sensors and liquid cooling systems, which increases the amount of possible cyber-physical attacks that could occur on those devices (The Cyber Express 2024). At the same time, fear of being sued under the

General Data Protection Regulation (GDPR) results in operators shredding millions of working hard drives that contain Critical Raw Materials (CRMs) used in the green transition (WeLOOP 2020).

This analysis proceeds in four substantive parts. Section I examines the physical architecture of sustainable computing, analyzing how liquid cooling and IoT integration challenge the 'appropriate technical measures' standard of the NIS 2 Directive. Section II dissects the 'Data Lifecycle Paradox,' exploring the conflict between GDPR data sanitization requirements and the Waste Electrical and Electronic Equipment (WEEE) Directive's reuse targets. Section III evaluates the environmental cost of cyber defense itself, utilizing recent data on 'Green AI' to argue for an 'Eco-Efficiency Index' in legal standards of care. Finally, Section IV addresses the 'Rebound Effect' and the legal vacuum surrounding 'dark data,' arguing that current reporting obligations under the EED must evolve into binding efficiency caps to prevent digitalization from cannibalizing decarbonization efforts.

2. The Architectures of Vulnerability: Legal Risks in Low-Energy Infrastructure

The transition to 'planet-proof computing' necessitates a fundamental re-engineering of data centre infrastructure.[1] To meet the stringent Power Usage Effectiveness (PUE) targets mandated by the EED and the Climate Delegated Act of the EU Taxonomy Regulation[2], operators are moving away from traditional air cooling toward liquid cooling and extensive IoT automation. While environmentally necessary, these technologies introduce specific legal and technical vulnerabilities.

2.1 Liquid Cooling and the IoT Attack Surface

Data centres rely on their cooling systems to operate correctly; without proper cooling, data centres shut down due to high temperatures. Modern data centres are adopting liquid cooling rather than air-based cooling to improve efficiency in managing heat generated by equipment; however, this change has created a very complex infrastructure of pumps, coolants and sensors. Like many operational technologies (OT), the majority of liquid cooled infrastructure is connected to Internet of Things (IoT) devices. This allows for real-time, AI-enabled optimization of energy and water usage at a data centre.[3]

A successful cyber-attack that manipulates the thermal control systems can lead to the catastrophic destruction of hardware and/or service outages, popularly referred to as "cyber-physical" attacks. A cyberattack manipulating thermal controls could cause catastrophic overheating, hardware destruction, and service outages, a 'cyber-physical' attack (Elsa and Hassan 2024).

Legally, this implicates the NIS 2 Directive, which classifies data centre service providers as 'essential entities.[4] Article 21 mandates that these entities implement 'appropriate and proportionate technical, operational and organisational measures' to manage risk.[5] The crucial legal question is whether the adoption of novel, complex cooling technologies for the sake of sustainability constitutes a failure to minimise complexity, a core tenet of security. If an operator integrates a third-party liquid cooling solution with weak firmware security, they face liability under NIS 2 Article 21(2)(d) for supply chain negligence.[6]

Furthermore, the sensors required for these green technologies are often resource-constrained devices, unable to run standard, energy-intensive encryption protocols like AES (Advanced Encryption Standard) (Vishal, Mohammad and Muhammad 2021). This necessitates the use of Lightweight Cryptography (LWC).

2.2 The Legal Sufficiency of Lightweight Cryptography

The deployment of billions of IoT devices for energy monitoring in smart infrastructures creates a demand for cryptographic algorithms that balance security with low power consumption and small physical footprint (Gate Equivalents or GEs).[7] Standard block ciphers like AES, while secure, may be too heavy for the microcontroller units (MCUs) embedded in pumps and valve sensors.[8]

Research identifies several LWC algorithms, such as PRESENT, CLEFIA, and SIMON, designed specifically for these constrained environments.[9] For instance, PRESENT requires approximately 1570 GEs for implementation, significantly less than the 2400 GEs required for a compact AES implementation, making it highly attractive for sustainable hardware design.[10] However, the legal standard for data protection, 'state of the art' measures under GDPR Article 32 is fluid.

If a data centre operator deploys sensors using an ultralight cipher like KTANTAN (which has known vulnerabilities to related-key attacks)[11] to save energy, and a breach occurs, the operator could be found liable for negligence. The pursuit of energy efficiency (low GEs and latency) cannot legally supersede the obligation of confidentiality and integrity (Davronbekovich 2024).

Thus, the legal definition of 'state of the art' must evolve to explicitly recognize and validate specific LWC standards (such as ISO/IEC 29192) as sufficient for environmental monitoring systems, distinguishing them from the higher standards required for personal data storage.

3. The Data Lifecycle Paradox: GDPR vs. Circular Economy

1 Commins and Irion (n 2) 3.

2 Directive (EU) 2023/1791 of the European Parliament and of the Council of 13 September 2023 on energy efficiency (recast) OJ L231/1 (EED); Commission Delegated Regulation (EU) 2021/2139 (Climate Delegated Act).

3 The Cyber Express (n 3).

4 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) OJ L333/80, Annex I.

5 *Ibid* art 21(1).

6 *Ibid* art 21(2)(d).

7 *Ibid* 357.

8 *Ibid.*

9 *Ibid* 411.

10 *Ibid* 411 (Table 3).

11 *Ibid* 403.

Perhaps the most acute conflict between legal regimes occurs at the end-of-life (EoL) stage of IT equipment. The EU's Circular Economy Action Plan prioritizes the reuse and repair of products to extend their lifespan and recover materials.[12] However, the data centre industry is characterized by rapid hardware refresh cycles often every 3 to 5 years, driven by the demand for higher performance and reliability.[13]

3.1 The Material Reality of the Cloud

To understand the legal stakes, one must understand the materiality of the equipment. A single enterprise server contains over 27 kg of materials, including steel, aluminum, and copper, alongside Critical Raw Materials (CRMs) such as Cobalt in backup batteries, and Neodymium (Nd) and Dysprosium (Dy) in the magnets of Hard Disk Drives (HDDs).[14] Under the WEEE Directive, the recovery of these materials is a priority. Yet, the recovery rate for CRMs from e-waste in Europe remains approximately 1%, a failure attributed largely to destructive recycling processes.[15]

3.2 Sanitization Standards: Shredding vs. Wiping

The bottleneck preventing reuse is the legal interpretation of 'secure disposal.' Data centre operators, acting as data controllers or processors under the GDPR, bear the burden of ensuring that personal data is irretrievable from retired storage media.[16] The industry's default response to this liability is physical destruction: shredding HDDs into 1-2 cm fragments.[17]

Shredding is legally 'safe' because a shredded drive cannot leak data. Ecologically, however, it is disastrous. Shredding mixes high-purity magnets with aluminum and steel scrap. During the subsequent smelting process, the Rare Earth Elements (REEs) are lost into the slag, rendering them unrecoverable.[18] The WeLOOP report on circularity in the data centre industry highlights that while steel and aluminum are recovered, the specific thermodynamics of smelting make the separation of mixed shredded materials technically and economically unviable for CRMs.[19]

A viable technical alternative exists software-based data sanitization (data wiping). Standards such as NIST 800-88 (Purge/Clear) involve overwriting data to render it unrecoverable while leaving the hardware intact for reuse.[20] According to the waste hierarchy, reusing materials is preferred over, recycling[21], but operators remain cautious due to the possibility of being found liable under GDPR for up to 4% of global turnover.[22]

Backed by the Waste able Hierarchy, the Data Centre Industry cannot be classified as "Taxonomy aligned" under the EU Taxonomy Regulation because shredding functionally valid hardware would not contribute substantially to the transition to a Circular Economy.[23] To provide accountability, this inconsistency must be addressed by the EDPB issuing a new guidance document confirming validated overwrite standards will be considered "safe harbours" and therefore support the reuse of data storage devices.

4. The Carbon Cost of Cyber Defence: Towards Green AI

With cyber threats becoming ever more advanced, the industry is increasingly using artificial intelligence (AI) and machine learning (ML) to detect anomalies and prevent intrusion (K. C., Md Zakir, and Md Shafiqul et al. 2025). However, AI is also an energy intensive technology. In fact, training deep learning models has a significant carbon footprint as research shows that training a single large natural language processing (NLP) model can generate the same amount of CO2 emissions as five cars over their lifetimes.[24]

4.1 Benchmarking Eco-Efficiency

A recent experiment utilizing the 'Carbon-Aware Cybersecurity Traffic Dataset' has evaluated multiple machine learning model performances for detecting network anomalies, revealing a stark trade-off between performance (accuracy) and energy consumption.[25] Complex ensemble models such as Random Forest and Support Vector Machine (SVM) obtained high F1 Scores (approximately 0.74) but used much greater amounts of energy while generating significant emissions (e.g., Random Forest the, found to generate 0.0553 gCO2eq in emissions during training).[26] In contrast, logistic regression and XGBoost models had much greater 'Eco-Efficiency' based on its definition of an F1 Score per kWh consumed.[27]

---

12 Commins and Irion (n 2) 18.
13 WeLOOP (n 4) 31.
14 *Ibid* 37-39.
15 *Ibid* 2 (Abstract).
16 Regulation (EU) 2016/679 (GDPR) art 32.
17 WeLOOP (n 4) 45.
18 *Ibid* 48.
19 *Ibid*.
20 *Ibid* 47.
21 *Ibid* 12 (Figure 1).
22 Commins and Irion (n 2) 19.
23 Regulation (EU) 2020/852 (Taxonomy Regulation).
24 *Ibid* 516.
25 *Ibid* 511.
26 *Ibid* 590.
27 *Ibid* 576.

The study introduced the 'Eco-Efficiency Index' (EEI) to quantify this trade-off.[28] Notably, applying Principal Component Analysis (PCA) to reduce feature dimensionality allowed a Random Forest model to maintain an accuracy of 76.96% while reducing carbon emissions by an order of magnitude.[29]

4.2 Liability for Energy Waste?

This technical reality challenges the legal concept of 'reasonableness' in tort law. In a negligence claim following a data breach, courts assess whether the defendant failed to exercise reasonable care.[30] If an operator utilizes a hyper-complex, energy-wasteful AI model when a lighter, eco-efficient model would have provided statistically similar protection, could this be considered a violation of emerging environmental due diligence obligations, such as those under the Corporate Sustainability Due Diligence Directive (CSDDD)?[31]

While current liability regimes focus on the *outcome* of security (i.e., was the breach prevented?), the integration of sustainability reporting (CSRD) suggests a shift towards evaluating the *cost* of security. Scope 3 emissions reporting will force transparency regarding the carbon footprint of purchased cloud services.[32] Consequently, 'appropriate technical measures' should arguably be interpreted to mean measures that are effective *and* energy-proportionate.

5. Regulatory Friction: The Rebound Effect and Dark Data

The European legal framework attempts to manage data centre sustainability through transparency. The EED requires data centres with an installed IT power demand of at least 500 kW to report performance indicators such as PUE and water usage.[33] However, efficiency metrics do not cap absolute consumption.

5.1 The Rebound Effect (Jevons' Paradox)

History demonstrates that increases in energy efficiency often lead to increased consumption, the 'rebound effect.'[34] As computing becomes more energy-efficient per bit, the cost of processing drops, stimulating demand for data-intensive applications like generative AI. The Commission's own studies admit that efficiency gains in servers have been outpaced by the exponential growth in demand for computing power.[35]

Current EU policy relies on the 'Energy Efficiency First' principle[36] but lacks a mechanism to limit the *utility* of the data being processed. A data centre mining cryptocurrency or training a redundant AI model may be highly energy-efficient (low PUE) while wasting vast amounts of renewable energy on socially widely regarded as 'frivolous' tasks.[37] The law remains neutral on the content of the computation, regulating only the efficiency of the machine.

5.2 The Legal Status of 'Dark Data'

A significant portion of this energy is spent storing 'dark data', information assets organizations collect but never use.[38] Estimates suggest 40-90% of stored data is dark.[39] Storing this data incurs continuous electricity costs for spinning disks and cooling.

Here, the GDPR offers an underutilized sustainability tool: the principle of '**data minimization**' (Article 5(1)(c)) and '**storage limitation**' (Article 5(1)(e)).[40] These articles mandate that data must be limited to what is necessary and kept for no longer than necessary. Regulatory agencies may aggressively enforce these rules both for privacy and as a dual-use measure to decrease the environmental impact of storing data.[41] According to legal scholarship, the guiding principle of 'data sufficiency' should align compliance with data protection to reduce energy used by data storage.[42]

5. Conclusion

The data centre market is at a critical junction. The path we are currently taking due to the rapidly increasing need for Artificial Intelligence, plus the lack of action (inertia) from organizations that are too cautious about taking risks related to compliance with regulations could ultimately lead us to a point where the digital transition and green transitions collide or converge. The NIS 2 Directive requires that data center's build resiliency through redundancy; whereas, the Circular Economy Action Plan requires an efficient operation to include re-use of their product. The GDPR requires that data be completely destroyed while the Critical Raw Materials Act requires material be recovered.

To resolve these conflicts will require a change in doctrine towards 'sustainable cybersecurity.' Toward that end, there are three specific legal-technical reconciliations necessary to affect that transition. First, it will be necessary for both the European

---

28 *Ibid* 512.
29 *Ibid* 597.
30 Allakuliev (n 18) 338.
31 Directive (EU) 2024/1760 (CSDDD); Commins and Irion (n 2) 22.
32 Directive (EU) 2022/2464 (CSRD); Commins and Irion (n 2) 21.
33 Commins and Irion (n 2) 30.
34 *Ibid* 25.
35 *Ibid* 24.
36 *Ibid* 25.
37 *Ibid* 29.
38 *Ibid* 28.
39 *Ibid*.
40 GDPR art 5.
41 Commins and Irion (n 2) 28.
42 *Ibid* 28-29.

Commission and EDPB to standardize and approve use of software-based data sanitization methods so as to eliminate the practice of shredding hardware, thus opening up the circular economy for CRMs. Next, to enable compliance with NIS 2 and GDPR, definitions under those instruments regarding 'state-of-the-art' security must include measures of energy efficiency to promote the use of lightweight cryptographic and eco-efficient AI models when appropriate. And lastly, the regulatory frame must not only focus on hardware efficiency (PUE) but also shift to include data sufficiency and therefore employ the principles of minimization set forth in the GDPR as a means of preventing future accumulation of dark data. If these changes do not occur, the current legal structure will continue to prescribe an environmentally costly and physically unsustainable form of cybersecurity, undermining the very future it seeks to secure.

References

Commins, Jessica and Kristina Irion. 2025. Towards Planet Proof Computing: Law and Policy of Data Centre Sustainability in the European Union. *Technology and Regulation*. https://pure.uva.nl/ws/files/226700880/TechReg2025.001_Commins.pdf

Davronbekovich, Allakuliev Mirdjalol. 2024. Legal regulation of liability for cyber attacks and data breaches. *International Journal of Law* 10: 111-113. https://www.lawjournals.org/assets/archives/2024/vol10issue5/10234.pdf

Editorial, 'Challenges Faced By Data Centers In Adopting Liquid Cooling' (The Cyber Express, 1 July 2024).

Elsa, Jane and Hassan Raza. 2024. Cyber Resilience for Sustainable Data Centers: Strengthening Security in Eco-Friendly Infrastructure. *EasyChair Preprint* 12217: 1-7. https://easychair.org/publications/preprint/h2jG/open

International Energy Agency. 2024. Electricity 2024 - Analysis and Forecast to 2026. *International Energy Agency*. https://iea.blob.core.windows.net/assets/6b2fd954-2017-408e-bf08-952fdd62118a/Electricity2024-Analysisandforecastto2026.pdf

K. C., Aashish, Md Zakir Hossain Zamil, and Md Shafiqul Islam Mridul et al. 2025. Towards Eco-Friendly Cybersecurity: Machine Learning-Based Anomaly Detection with Carbon and Energy Metrics. *International Journal of Applied Mathematics* 38: 765- 515. https://arxiv.org/pdf/2601.00893

Thakor, Vishal A, Mohammad Abdur Razzaque and Muhammad R. A. Khandaker. 2021. Lightweight Cryptography for IoT: A State-of-the-Art. *Arxiv*. https://arxiv.org/abs/2006.13813

WeLOOP. 2020. A Situational Analysis of a Circular Economy in the Data Centre Industry. *Circular Economy for the Data Centre Industry*. https://www.weloop.org/wp-content/uploads/2021/09/2020_04_16_CEDaCI_situation_analysis_circular_economy_report_VF.pdf