The Jurisprudence of Thermodynamics: Doctrinal Conflicts Between High-Availability Cybersecurity and Environmental Finitude in Data Centre Regulation

Aman Kumar Jha

B.Sc. LL.B. (Hons.) [Cyber Security]

National Law Institute University, Bhopal

Tanishk Bhawsar

B.Sc. LL.B. (Hons.) [Cyber Security]

National Law Institute University, Bhopal

Sujal Chhajed

B.Sc. LL.B. (Hons.) [Cyber Security]

National Law Institute University, Bhopal

ABSTRACT

The worldwide digital economy is based on a significant physical contradiction: the exponential inelastic requirement for high-availability and low-latency computing power and the restricted limits of the planetary environment. As data center operators move next to sustainable low-energy hardware architectures driven by reducing operational costs as well as stringent environmental requirements, they face unbending and inflexible security regulations. This paper will analyze the technological-legal paradox found in the contrast between the EU's NIS 2 regulation, GDPR recommendations, and the Energy Efficiency Directive's limitation for sustainable computing. The study relies on a doctrinal research method. Specifically, Dynamic Voltage and Frequency Scaling (DVFS), approximate computing, and liquid immersion cooling significantly impact the high-availability and continuous monitoring obligations required by the law regulating critical infrastructure. Current legal doctrines governing the tort of negligence, the doctrine of proportionality, and the statutory definition of "appropriate technological measures" are based on a misconception of the unlimited availability of resources. Therefore, operators are in a situation where compliance with the law requires them to infringe upon their obligations to ensure safety. The article ends by putting forward a more sophisticated legal category of "Proportionate Resilience" and asserting that the standard of a "reasonable operator" needs to be updated to legally legitimize the necessary environmental trade-offs that are characteristic of the Anthropocene era.

Keywords: Critical Infrastructure Law, NIS 2 Directive, Energy Efficiency Directive, Cybersecurity Liability, Data Centre Governance.

I. INTRODUCTION: THE MYTH OF THE IMMATERIAL CLOUD AND THE VISIBILITY OF LAW

The scholarship regarding cyberspace has, for a long time, strongly reflected a "software bias." As a matter of fact, it has been only in the last few decades that privacy, freedom of speech, content moderation, algorithmic bias, and lack of jurisdictional sovereignty of legit internet content have been discussed for the most part by the internet scholars

completely in the immaterial level alone.[1] The physical layer of cyberspace, the massive hyperscale data centers, the submarine fiber-optic cables, the cooling towers, the silicon architectures, and the colossal electricity consumption that sustains them, has mostly been treated by legal theorists as an inert utility footprint, a mere waste, a resource on which the digital rights drama is performed.

This advocate's blindness to things is not sustainable anymore. Today, the modern data center is known as the most significant infrastructural site and it has been officially and unequivocally proclaimed as "critical infrastructure" and an "essential entity" in three major legal formulations emanating from Europe.[2] Ineluctably, hardware and the human systems on which they operate create the non-human regulation of our physical environments; as Mireille Hildebrandt has also pointed out, "code is law," but hardware is the physics that constrains the code.[3]

Now, this physical infrastructure hangs in the balance of a significant regulatory and physical collision. One of the sides is the continuous rise of state-sponsored cyber threats, ransomware cartels, and supply-chain attacks that have resulted in the lawmakers queuing for the "state-of-the-art" security measures.[4] The laws stipulated here demand high availability, redundant architectures, and continuous, compute-intensive algorithmic monitoring, as the infrastructure should not be assumed to go down ever. On the flip side, the energy consumption limits of our planet have necessitated a paradigm shift in data centers. Following guidelines established by the international community, such as the UN Sustainable Development Goals (specifically SDG 9 and 13)[5], and the binding law of the European environmental law, the tech sector is in a rapid shift towards "low-energy" computing, which focuses on thermal efficiency instead of a higher performance avenue.

The authors arguing in this paper propose that there exists a fundamental doctrinal incoherence currently between the legal duty to secure and the technical duty to conserve. Nevertheless, the operational resilience that is stipulated by the directive must be tended absolutely, the state of mind which low-energy computing requires is bringing some exceptions like latency, computational throttling, and algorithmic approximation. The law, however, is devoid of the jurisdiction's language to authorize them.[6]

The fundamental research issue driving this doctrinal analysis is: Is the adoption of energy-saving techniques in critical digital infrastructure the implementation of the violation of the statutory duty of care if those techniques themselves lower the security threshold? Through careful assessment of the interdependence of the physical laws of modern computing and the EU cybersecurity and tort law regulations, this paper demonstrates the way in which the current legal environment sometimes can lead to the punishment of the necessary transition to environmentally friendly digital structures.

II. The Legal Framework for Cybersecurity in the European Union

Appropriately to deal with this problem, one should first identify the baseline of the law. The regulation of data center security is no longer of merely private Service Level Agreements (SLAs) or voluntary industry standards but has been taken out of this scope and into the realm of public administrative law and strict statutory liability.

[1] Andrew Murray, *Information Technology Law: The Law and Society* (4th edn, OUP 2019) 112.
[2] Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities (CER Directive) [2022] OJ L333/164.
[3] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar 2015) 175.
[4] Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) [2022] OJ L333/80, art 21(1).
[5] UN General Assembly Resolution 70/1 (2015) 'Transforming our world: the 2030 Agenda for Sustainable Development' (SDG 9, SDG 13).
[6] NIS 2 Directive, art 21(2)(c).

2.1. NIS 2 Directive and the Mandate for Absolute Resilience

The NIS 2 Directive is a landmark shift in how European cybersecurity operates. It transitions from the disjointed, retrospective reporting framework of its predecessor (NIS 1) into the harmonized, prescriptive risk-management regime.[7] What is more, Annex I distinctly outlines "data center service providers" and "cloud computing service providers" as highly critical essential entities.[8] Hence, this categorization is the key to the firm exit from private enterprise, subjecting these entities to equally stringent liability under public law that is expected of supercritical nuclear plants or national electricity grids.

Article 21 is the kicker in the whole regulatory framework. It obliges essential entities to adopt "appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems."[9] Nevertheless, Article 21(1) cares a little about this obligation, which is conditional: the mentioned measures should be adopted "having regard to the state of the art."[10]

In the realm of legal science and reading of laws, "state of the art" (from the German concept of administrative law that is dealt with technical condition) is a rather figurative and exceptional standard that is dynamic and tough to achieve.[11] While "standard industry practice," which allows for a legal defense based on peer behavior ("everybody else is doing it"), "state of the art" means the use of the best available technology that has the backing of scientific results irrespective of the popularity in the market.[12]

In the age of cybersecurity infrastructure, the "state of the art" is delineated by the ethos of additive security. It is a do-or-die condition for maximum firewall throughput, triple-layer hardware redundancy (like 2N+1 architecture), dense cryptographic rounds, and continuous, AI-log driven log analysis. A state-of-the-art facility is designed to handle the primary power grid catastrophic failure without any computational downtime at all. This degree of robustness demands huge, constant electrical expenses to keep the redundant systems in a "hot standby" state, using incredible power while not running active computational tasks.[13]

2.2. The GDPR and the Strict Construction of Integrity

. NIS 2 is not the only piece of legislation that has an infrastructure-related emphasis. The General Data Protection Regulation (GDPR) runs a parallel to it since it contains the ethical requirements concerning the processing of personal data located on premises, these data centers are also known as.[14] In Article 32, data controllers and processors are required to set appropriate measures that protect the systems and services of the "confidentiality, integrity, availability and resilience of processing."[15]

Enforcement agencies and courts have interpreted these principles rigorously. The disciplinary measures that the UK Information Commissioner's Office (ICO) has undertaken against British Airways and Marriott International should be a clear signal that the effective security measures must equally combat both recognized security weaknesses and foreseeable ones.[16] The legal perspective assumes that the primary concern of the data controller is the security of the

[7] NIS 2 Directive, recital 76.
[8] NIS 2 Directive, Annex I, Sector 8 (Digital Infrastructure).
[9] NIS 2 Directive, art 21(1).
[10] ibid.
[11] Alexander Roßnagel, 'Das IT-Grundrecht' (2008) 61 *Neue Juristische Wochenschrift* 1113.
[12] *Commission v Germany* Case C-418/04 [2007] ECR I-10947.
[13] Ian Sommerville, *Software Engineering* (10th edn, Pearson 2016) 302.
[14] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons about the processing of personal data (GDPR) [2016] OJ L119/1.
[15] GDPR, art 32(1)(b).
[16] *British Airways plc* ICO Penalty Notice COM0783547 (2020); *Marriott International Inc* ICO Penalty Notice COM0804337 (2020).

data, renouncing all other operational, financial, or environmental metrics. Should the data controller's choice to remove server redundancy to reduce power as per prolonged reliability and environmental concerns cause a systematic security flaw, they may present the case for their legal negligence in a much stronger manner. The jurisprudence of the Court of Justice of the European Union, especially in cases related to the fundamental right under Article 8 of the Charter of Fundamental Rights of the European Union, allows not much operational looseness that would put the data subjects at risk.[17]

The previous paragraph outlines the reasons behind management accountability and the transformation of disclosing the corporate veil as the discussion. Article 20 of the NIS 2 Act is contributing to this huge risk because it imposes personal responsibility on the management bodies of crucial entities for the non-compliance of the risks established by Article 21.[18] In this way, the law also serves to tear down the corporate veil, which has the effect of preventing executives from wanting to be behind the corporate policy in general.

If a CISO or a board of directors chooses to authorize a "green" data center architecture that was directly calculated to incur an increase in threat response latency to save energy, they would be the one accepting that risk. In case of a huge data breach, the reason for staying "environmentally friendly" will not bring any statutory protection against the business consequences such as the administrative fines up to 10 million EUR or 2% of their total global annual turnover. That accused stance of environmental sustenance is not a shield against litigations from shareholders concerning the violation of fiduciary duty.[19]

III.3. The Ancillary Constraint: Environmental Law is a Competing Mandate

Aside from the primary focus on the technological and liability aspects of cybersecurity, this doctrinal analysis needs to recognize the growing environmental regulatory pressure on data center operators, which forces them to face legal challenges. Environmental administrative law must be considered along with the law of cyberspace.

The first major piece of legislation on this matter is the recasted Energy Efficiency Directive (EED) which will be responsible for the majority of environmental pressure on the data centers.[20] Article 12 of the EED mandates data centers with an IT power demand of at least 500kW to publicly report their energy performance, water usage and waste heat recovery metrics to a European database.[21] This obligation is further implemented through the regulation of the Commission, which establishes a common Union rating scheme for data centers.[22]

The operation of this transparency regime is also a "name and shame" tool of tremendous strength. High energy consumption is a barrier to corporate governance driven by ESG; it violates the reporting framework of the Corporate Sustainability Reporting Directive (CSRD) and causes the company to be under strict regulatory investigation.[23]

But the trouble not only is that there is a Safe Harbour provision that can bind these separate requirements but also a serious doctrinal gap. The NIS 2 Directive, GDPR, or CER Directive do not specify any provision that gives an entity immunity from civil liability or administrative penalties, resulting from a cybersecurity incident which was unavoidable and due to compliance with the EED. Consequently, the data center operator must comply with two independent

[17] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 8.
[18] NIS 2 Directive, art 20.
[19] NIS 2 Directive, art 34(4).
[20] Directive (EU) 2023/1791 of the European Parliament and of the Council on energy efficiency (EED recast) [2023] OJ L231/1.
[21] EED, art 12(1)(b).
[22] Commission Delegated Regulation (EU) 2024/1364 on the first phase of the establishment of a common Union rating scheme for data centres [2024] OJ L 2024/1364.
[23] Directive (EU) 2022/2464 of the European Parliament and of the Council amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting (CSRD) [2022] OJ L322/15.

authorities whose directives are contradictory: the cyber regulator calls for total, high-energy resiliency; the environmental regulator demands complete, low-energy efficacy.

IV.4. Finite Technical Architectures and Doctrinal Friction Points

The clash between cybersecurity and Eco sustainability targets is, indeed, not Just a theoretical exercise in statutory interpretation, because it also translates very well into the actual hardware operators' decisions they need to make. The leap to low energy technology brings in quite different and open legal liabilities against the existing doctrinal regime.

4.1. Advocacy of Dynamic Voltage and Frequency Swinging (DVFS) and Defense Latency

The main design approach of reducing energy consumption in a data center server through the facility of DVFS is Dynamic Voltage and Frequency Scaling. DVFS can change the power of the CPU dynamically by the real-time computational workload. The CPU enters lower voltage states when the demand is low, like C-states or P-states (normally referred to as).[24]

Technical Vulnerability: Connecting the server directly from a state of deep sleep to active state adds latency while serving a higher load--a phenomenon known as "wake-up latency" which is typically measured in milliseconds or microseconds. Security of systems relies on the ultimate measure of time. Off takers of Volumetric Distributed Denial also attack with speed as machines do. A micro-burst attack can fill a network interface card (NIC) with millions of malicious packets in the fraction of a second, that the processor has not "woken up" to analyze, filter and drop the traffic.[25] Besides, DVFS itself is a source of observable side-channels. The widely known "Hertzbleed" vulnerability (CVE-2022-24436) is a good example of the extent to which attackers can take advantage of these frequency changes that are triggered specifically by DVFS power adjustments to gain information and thus extract cryptographic keys from a CPU.[26]

The Doctrinal Conflict: Article 21(2)(c) of NIS 2 explicitly mandates "business continuity, such as backup management and disaster recovery, and crisis management" in connection with the company's statement.[27] If, as a result of an incident report, a DDoS attack is discovered as the cause of a long-term service interruption due to the fact that the perimeter defense systems (like hardware firewalls and intrusion detection systems) are set to a deep sleep state to hit EED energy targets, then the operator is faced with a nearly impossible legal challenge.

An affected party (or regulator) would argue that the operator had intentionally put the system into a latent mode thus compromising its security. Due to the continuous, instantaneous, and "always-on" sense of the legal definition of the "state of the art," it is clear that the aggressive DVFS policies are misinterpreted by a judge as a failure to implement "appropriate" technical measures and the operator is thus rendered legally liable for the out-time caused. In addition to that, the fact that the disabling of DVFS to mitigate the existing hardware vulnerabilities such as Hertzbleed is a direct breach of the duty of care, the act of disabling it will lead to the loss of the facility's hard-won energy efficiency.

4.2. Approximate Computing and the Erosion of Legal Integrity.

Computer architects are opting for "Approximate Computing" models increasingly frequently in their efforts to bypass the physical boundaries of silicon (the end of Moore's Law) and to cut energy consumption drastically. The idea behind

[24] EED, Annex VII (methodology for monitoring energy efficiency).
[25] Louise Bennett, 'The Green Data Centre: A Symbiotic Relationship Between Security and Sustainability' (2023) 14 *Journal of Law and Technology* 45.
[26] CVE-2022-24436 (Hertzbleed side-channel vulnerability).
[27] NIS 2 Directive, art 21(2)(c).

this computing model is that it purposefully loses the requirement of exactness in computations- for instance, in the case of big data analytics, video rendering, or AI model training, approximate computing can lead to considerable energy savings.[28]

Technical Vulnerability: Approximate computing rewrites the rules and thus creates an opportunity for the new "Dishonest Approximate Computing" (DHAC) attacks. Say a system is designed by its mathematics to accept a 5% margin of error in its processing output; an intruder could temporarily mislead the system by subtly injecting malicious data within that range of margin. The system, which is especially programmed for the sake of energy efficiency to be "tolerant" of errors, will authenticate the harmful data as genuine.[29]

The Doctrinal Conflict: This design choice leads to a direct and irreconcilable conflict with the GDPR Article 5(1)(d) (Accuracy) and Article 5(1)(f) (Integrity and Confidentiality). A plaintiff willing to initiate a class action suit against a data center can state without any doubts that the system was specifically designed to be inaccurate.

In the field of law, "integrity" signifies a dichotomous condition: information is either precisely as it was meant to be recorded or it has been altered. The legal framework does not allow for partial truths in data processing. Approximate computing undoubtedly brings in the idea of the "probabilistic integrity" which the European data protection law altogether does not admit.[30] For instance, if a financial risk model or a medical diagnostic algorithm which is being run in a green data center produces a faulted output result because the machine was operating in an "approximate mode" for energy saving, the problem is that the operator is prejudicially processing data without the guaranteed proper integrity, therefore, the operator breaches core sections of the GDPR.[31]

4.3. Liquid Immersion Cooling and the Expansion of the IoT Attack Surface.

To attain PUE ratios that are close to 1.0 (the theoretical thermodynamic ideal of zero energy waste), some of the best green facilities have switched air conditioning HVAC systems with the traditional ones and have introduced liquid immersion cooling, where the server blades are completely soaked in a dielectric fluid.[32]

Technical Vulnerability: Immersion cooling not only requires many sensors but also that they are all interconnected to an Internet of Things (IoT) and Operational Technology (OT) network. This ensures that the sensors are used for monitoring the fluid flow, thermal dynamics, and pressure. The underlying fact is that these OT sensors mostly utilize lightweight, less secure communication protocols (for instance MQTT or Modbus) as opposed to the very strong security features of the servers they cool. Hence, in this regard, one does not need to penetrate through the main firewall or decrypt the database to obliterate the data center. All they have to do is to compromise the cooling controller, stop the dielectric fluid pump from working, and conduct a "thermal denial of service" attack, thereby, allowing the servers to melt by their own computational heat.[33]

The Doctrinal Conflict: Operators must provide both the "supply chain security" and stringent physical and environmental security as stated in the Critical Entities Resilience (CER) Directive and NIS 2 Article 21(2)(d).[34] In order to improve the benefits through sustainability, the operator generally switches to liquid cooling process and risks the digital thermal perimeter by losing the analogue secure physical perimeter.

[28] S Mittal, 'A Survey of Approximate Computing Techniques' (2016) 48 *ACM Computing Surveys* 1.
[29] GDPR, recital 74.
[30] GDPR, art 5(1)(d) and art 5(1)(f).
[31] GDPR, recital 83.
[32] EED, recital 45 (encouraging waste heat recovery and innovative cooling).
[33] NIS 2 Directive, art 21(2)(e) (security in network and information systems acquisition, development and maintenance).
[34] NIS 2 Directive, art 21(2)(d).

This IoT sensor provided by the third party is an unsecured device for tempering with. In OT supply chains, such settings are as common as Pvt. OPCO's staff, and the operator has breached their legislation. However, the initiative towards environmental sustainability is a complex addition to the facility's security by creating an exposure to risks that regulators and courts might challenge the proportionality of the added environmental benefits, only considering the issue through cybersecurity law.

V. Cryptographic Thermodynamics: The Energy Cost of Legal Secrecy

This legal predicament is not just about hardware choices but also about the mathematical aspect of cryptography. The law sees encryption as a strict, weightless, and absolute requirement, meaning it should just be thought of as a line of code. But in the real world, the data center sees encryption as a physical thermodynamic cost.

5.1. The Post-Quantum Dilemma and the Energy Spike

The coming of quantum computing, which is supposed to give the power to break current public-key cryptography through Shor's algorithm, has made it a must for the development of Post-Quantum Cryptography (PQC) on an urgent basis. Governments, such as those from ENISA and the US NIST have shown that they are seriously committed to protecting national security by making a tip for critical infrastructure operators to stop "carve now, decrypt later" attacks by advanced persistent threats (APTs) with the help of PQC algorithms.[35]

Energy Reality: PQC algorithms like CRYSTALS-Kyber or Dilithium are stated to be heavier SSD than RSA and ECC, respectively. They necessitate a key size of a certain number of bits which is higher than that of current algorithms, ciphertext which is larger, and more CPU cycles for the processes of encrypting, transmitting, and decrypting the data.[36] Enabling the transition to a massive hyperscale data processing facility that uses PQC across a hyper-scaler processing petabytes of data daily raises the "Base Load" energy consumption of the data center by a non-negligible percentage.

The Doctrinal Bind: A low-power data center operator entrapment in compliance issues immediately finds oneself. If they choose PQC instead of the state-of-the-art requirement evolving under NIS 2 and GDPR Article 32, they get an energy consumption spike, thus violating EED reporting quotas, municipal power agreements, or corporate ESG commitments.[37] On the other hand, if they decide to implement PQC at a later date without compromising their energy efficiency, they will be leaving the critical data susceptible to interception. In the future, the evidence that has been reported may not be "we wanted to save electricity" as the attorney for the infringing company and maybe even the court will not accept that as a legal justification for not implementing industry-standard cryptographic protection. The hierarchy of legal values in European law is such that the basic human rights like data privacy which is found in Article 8 of the Legal Charter of Basic Rights are far more important than energy efficiency, which is generally regarded by judges only as a socio-economic policy goal.[38]

5.2. Digital Operational Resilience and Immutability Tax

The likelihood of conflict increases with the financial sector's heavy dependence on data centers, which now brings digital operational resilience act (DORA) into the picture.[39] DORA Article 9, in particular, creates a tough task for the Information and Communication Technology risk management framework that is required to follow the guidelines of

[35] National Institute of Standards and Technology (NIST), 'Post-Quantum Cryptography Standardization' (NIST, 5 July 2022).
[36] GDPR, art 32(1)(a) (pseudonymisation and encryption of personal data).
[37] EED, art 12.
[38] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 8.
[39] Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector (DORA) [2022] OJ L333/1.

the regulatory authorities that are generally interpreted as mandating the use of append-only immutable logs to ensure the forensic auditability of the incidents that took place.[40]

The implementation of immutability through distributed ledger technologies (DLT) or dense, continuous cryptographic hashing necessarily means that such operations will entail huge amounts of power and vast quantities of computational resources working together for the validation of such transactions. Following the legal rule to maintain perfect operational resilience and forensic traceability as stipulated in the DORA by the “immutability tax"" on facility's power grid, it indeed is a direct and aggressive breach of the basic energy conservation rules of sustainable computing.

VI. Judicial Ideas on Risk, Liability, and the "Reasonable Operator"

How will the courts in Europe rule when a "green" data center incurs inevitable breach scenarios where the direct security leak is because of the energy saving measure used? In situations where there are no specific legal precedents pertaining to the sustainability of data centers, legal scholars can only depend on the extensive and well-known precedents in areas such as professional negligence, tortious liability, and statutory duty.

6.1. The Standard of Care: Bolam, Bolitho, and Cyber Negligence

When it comes to the ruling on common law negligence, most of the time, courts are reliant on the standard of the "reasonable professional." Bolam v Friern Hospital Management Committee, the outstanding medical negligence court ruling, has been the starting point of the standard legal test. The classical legal criterion weighs whether the professional acted in accordance with a practice that is agreed as proper by a responsible body of professional opinion.[41]

If a responsible body of hyperscale data center operators is consistently moving toward green architecture such as DVFS and approximate computing to meet ESG requirements, then a defense lawyer might firmly state that computational throttling has become the new "industry standard" in the context of the Bolam test.

But, in the case of Bolitho v City and Hackney Health Authority, the following ruling of the House of Lords presented an urgent and basic counterargument: the accepted professional practice must be examined from the perspective of logical analysis and courtroom scrutiny.[42] A judge cannot be forced to accept a certain professional practice if the practice is regarded as illogical or risky.

In the setting of a cyber breach, a claimant would use Bolitho to claim that it is irrational and thus negligent to prioritize energy conservation over the proper security of critical public infrastructure (for instance, electronic healthcare records, energy grids, or financial clearinghouses). It is probable that the court would reach a decision that predominantly, the NIS 2 data center’s primary statutory function is its availability and security, and conservation is just a mere secondary operational preference. Thus, with the Bolitho gloss, any technical measure that offends the primary statutory function for a secondary ESG aim is legally unreasonable and is an act of breach of the duty of care.

6.2. The Negligence Calculus: Hand Formula and Environmental Burden

When reviewing a breach of duty, courts frequently presuppose an economic calculus that is similar to the "Hand Formula," which was originally expressed by Judge Learned Hand in United States v Carroll Towing Co.[43] Liability

[40] DORA, art 9 (Protection and prevention).
[41] *Bolam v Friern Hospital Management Committee* [1957] 1 WLR 582.
[42] *Bolitho v City and Hackney Health Authority* [1998] AC 232.
[43] *United States v Carroll Towing Co* 159 F.2d 169 (2d Cir 1947).

will be set when the cost of precautions (B) is less than the probability of injury (P) times the severity of loss (L) (B < PL).

In the scenario of a data center operator who utilizes energy-efficient infrastructure, he/she will go for a newly invented, eye-catching, and turnaround legal argument which states that the Burden (B) should not be evaluated exclusively in financial terms but is to be assessed with the intrinsic environmental cost to the planet as well. They would say that the high carbon footprint of running continuous 2N redundancy is an environmental Burden that can legally be offset by the acceptance of a slightly higher Probability (P) of cyber risk.

It is with great respect that I beg to differ as to why this argument would categorically fail under the existing European and common law principles. The sheer catastrophic magnitude (L) of the possible cyberattack on critical infrastructure, which could result directly in lives being endangered, such as the shutting down of critical care servers in a hospital, or indirectly in a huge economic debacle, would push the court to almost inevitably acknowledge that the risk of human safety and privacy are far more significant than the abstract environmental savings brought by the reduction of kilowatt-hours. In the legal profession, the data subject's imminent and clearly foreseeable harm gets more preference than diffuse environmental harm. Now, saving the environment is just not a legitimate legal defense for data breach.

The concept of proportionality has its limitations in the area of EU administrative law, as seen in article 21(1) of NIS 2, which expects organizations to adopt "proportionate" measures.[44] According to EU law, the proportionality principle is a precondition for taking action the measures must be appropriate and indispensable to the effect, they are achieving but not more than what is strictly necessary.[45]

In major data protection cases such as the landmark CJEU ruling in Schrems II (the international data transfer question) and in Digital Rights Ireland regarding data retention, the Court of Justice of the EU displayed very rigorous adherence to the principle of proportionality concerning the protection of personal data.[46]

For example, within the context of the data center, if a provider presents the lame argument of the disabling security features being "proportionate" to their energy quota under the EED, regulators will counter that energy quotas do not permit the removal of fundamental rights to privacy and security. The Court of Justice of the European Union's rulings on "the best available techniques," like the one seen in the environmental Commission v Germany case, affirm that cost (along with energy cost) is seldom enough of a justification for underperforming on the most efficient safety measures which have public viability at risk.[47]

VII. Crafting a New Judiciary: The Principle of Proportionate Resilience

As one is made to think, digital infrastructure currently seems to be battling on two fronts: "security" and "sustainability," which are like two parallel lines that will never meet. This legal provision is asking for total digital resilience (NIS 2 and GDPR) at the same time while also demanding total physical efficiency (EED and CSRD). The situation could not get more entangled, thus, it has led to the creation of undefined legal elements and has caused conflicts for the concerned professionals such as subject matter experts, CISOs, and corporate legal counsels who have had to go through a wrongful course between an irreconcilable liability and a wrong matrix.

[44] NIS 2 Directive, art 21(1).
[45] Consolidated Version of the Treaty on European Union [2012] OJ C326/13, art 5(4).
[46] *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (Schrems II) Case C-311/18 [2020] ECLI:EU:C: 2020:559; *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* Joined Cases C-293/12 and C-594/12 [2014] ECLI:EU:C:2014:238.
[47] *Commission v Germany* Case C-418/04 [2007] ECR I-10947.

The Doctrine of Proportionate Resilience is the immediate new jurisprudential model that technology law must create; it will be a tool by means of which stagnation of sustainable infrastructure will be avoided, and operators who act in good faith will be protected.

7.1. Legislative Redefinition of "State of the Art"

National parliaments and organizations in charge of setting norms (for instance, ENISA and national cybersecurity centers) must issue legally binding guidelines that expressly redefine "the state of the art" in Article 21 of NIS 2 to include "energy proportionality." The legal benchmark must admit the fact that a security measure that ensures no possibility of data exposure but at the same time asks for increasing the power supply to the environment is actually "defective." The decision of "appropriate and proportionate measures" should consider the heat caused by computation as a valid mitigating factor in carrying out the risks assessment.[48]

7.2. A "Green Security" Safe Harbour will be established

Defining "Green Security" Safe Harbour will be the implementation of a law that will allow companies to apply and adopt security measures based on carbon footprint evaluation.

A cross-directive Safe Harbour provision, which is a part of European legislation, is necessary for dealing with the intersection of cyber and environmental law. If the essential entity has a convincing case through an independent audit that a certain security weakness was the direct, unavoidable result of a real technical measure that was previously required by the binding energy efficiency targets of the EED, then it should be given a rebuttable against gross negligence.

This Safe Harbour would not fully exempt the entity from liability, but rather it would require consideration of the damages to victims, while also protecting the executive management from very high personal administrative charges included in Article 20 of NIS 2[49], as long as they acted in good faith and implemented alternative, low-energy mitigating controls.

7.3. Integrated Regulatory Auditing Models

Now, data centers are being audited in silos: by data protection authority (for GDPR compliance), cybersecurity agency (for NIS 2 resilience) and environmental regulatory (for EED reporting). This torn, confrontational approach induces the compliance trap further. The EU should make the shift to the integrated "Digital Sustainability Impact Assessments" (DSIA) whereby an operator's technological structure is assessed thoroughly by a singular body, drawing a balance between cyber risk and carbon discharges in a legally acknowledged matrix.[50]

VIII. CONCLUSION

The digital era brings to the foreground the need for securing data against the onslaught of incredibly sophisticated, persistent adversaries, but the physical reality in the Anthropocene brings to us the need of healing our planet from staggering resource depletion. At the moment, the European law stands between these two existential issuances opposing each other in a zero-sum game manifested at the data center walls.

[48] Proposal for a Regulation laying down harmonised rules on artificial intelligence (AI Act) COM/2021/206 final (illustrating the shift toward risk-proportionate technology regulation).
[49] NIS 2 Directive, art 20(1).
[50] UN General Assembly, 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace' (2015) UN Doc A/70/174.

The insistence on "absolute" resilience along with the maximum-security measures in the continuity, which don't count on the cost of thermodynamics, current cybersecurity regulations practically enforce the loss of energy on a large scale. On the opposite side, the basic system requirements to be achieved of true sustainability through methods like dynamic throttling, latency acceptance, and algorithmic approximation, cause the security measures to become lax from the initial rigid demand of law, exposing the operators to stringent legal liability, hefty fines, and irreparable reputational harm.

Legal scholarship should move beyond its dystopic perspective of software and engage actively with the reality of finite hardware in cyberspace. The extremely secure and low-energy data center is a technical challenge to be overcome, however, under the current legal paradigms, it is fraught with peril. Until the legislative measures and judicial thinking i.e. the hard and fast laws of energy provision and boundless firewalls, data center managers will stay galleyed in the friction of finitude forced to choose between the well-being of the server and the health of the planet.