BIS HUMANITIES AND SOCIAL SCIENCE

Volume 4 2026 | DOI: 10.31603/bishss.495
7th Borobudur International Symposium on Humanities and Social Science (BIS-HSS) 2025

UNIMMA PRESS
Universitas Muhammadiyah Magelang

Criminal liability in the era of green technology and digital society: Towards a smart and sustainable legal system

Basri[1]* and Tsuroyyaa Maitsaa' Jaudah[1]

[1] Universitas Muhammadiyah Magelang, Magelang, Indonesia
*Corresponding author email: basri@unimma.ac.id

Abstract

The rapid convergence of green technology and digital society has fundamentally transformed environmental governance. While digital infrastructures such as automated emissions monitoring systems, AI-driven compliance tools, and blockchain-based carbon markets enhance regulatory efficiency, they simultaneously generate new forms of eco-digital risk. These risks challenge the foundational assumptions of classical criminal liability, which remain anchored in individualized intent, direct causation, and territorially bounded jurisdiction. Existing scholarship has examined environmental harm through green criminology and technological wrongdoing through cyberlaw, yet these fields remain largely disconnected. As a result, criminal law lacks an integrated framework capable of addressing technologically mediated environmental harm. This article argues that eco-digital harm represents a structurally distinct category of wrongdoing characterized by distributed agency, algorithmic causation, and transnational digital interconnectivity. Employing a normative and comparative legal methodology, the study evaluates the doctrinal adequacy of existing liability principles and identifies structural gaps in attribution and enforcement mechanisms. The article advances a Hybrid Eco-Digital Liability Model that integrates expanded supervisory responsibility, functional causation standards, and technologically informed smart enforcement strategies. This model recalibrates classical doctrines without abandoning their normative foundations. By bridging green criminology and cyberlaw within a sustainability-oriented governance framework, the study contributes a unified conceptual approach to criminal liability in the era of digital environmental regulation. The findings highlight the urgent need for doctrinal evolution to preserve environmental integrity and regulatory legitimacy in technologically mediated societies.

Keywords

Criminal liability, Eco-digital harm, Green technology, Digital governance, Environmental crime

Published:
May 04, 2026

Selection and Peer-review under the responsibility of the 7th BIS-HSS 2025 Committee

Introduction

The rapid convergence of green technology and digital society is reshaping environmental governance at an unprecedented scale. Renewable energy infrastructures, automated emissions monitoring systems, blockchain-based carbon trading platforms, and AI-driven regulatory mechanisms are increasingly embedded within digital ecosystems. While these technological innovations advance sustainability objectives, they simultaneously generate new forms of risk that challenge the foundational assumptions of criminal law.

These developments reflect what (Beck, 1992) conceptualizes as "manufactured risks" where technological progress produces systemic vulnerabilities that are difficult to localize within traditional accountability structures. In eco-digital environments, environmental harm may result not from direct human misconduct but from algorithmic processes, automated decision-making systems, or complex interactions between human operators and technological architectures. Consequently, the classical model of criminal liability grounded in individualized intent, direct causation, and territorially bounded jurisdiction faces significant doctrinal strain.

Existing scholarship has examined environmental harm through the lens of green criminology (Lynch, 2019) (White, 2020) and technological wrongdoing through cyberlaw and digital liability frameworks (Kerr, 2022) (Hildebrandt, 2015). However, these fields largely remain analytically separated. Green criminology tends to focus on corporate environmental harm and regulatory failure without fully engaging with digital infrastructures as mediators of environmental risk. Conversely, cyberlaw scholarship addresses attribution, jurisdiction, and algorithmic governance but rarely incorporates sustainability or ecological harm into its analytical framework.

This disciplinary fragmentation obscures a critical transformation: environmental harm is increasingly produced, monitored, and regulated through digital systems. As (Lessig, 2006) famously observed, "code is law" in eco-digital contexts, technological architecture itself structures compliance, risk, and accountability. Yet criminal law doctrine has not evolved at the same pace as technological integration. The result is a widening gap between regulatory reality and doctrinal design.

This article argues that eco-digital risks expose structural inadequacies within traditional criminal liability frameworks. The problem is not merely the emergence of new categories of crime, but the transformation of how harm is generated, distributed, and attributed in technologically mediated systems. Accordingly, this study addresses the following research question:

How should criminal liability be reformulated to effectively respond to eco-digital risks arising from the integration of green technology and digital society?

This article makes three principal contributions. First, it conceptualizes eco-digital crime as a distinct category of technologically mediated environmental harm characterized by distributed agency and algorithmic causation. Second, it integrates insights from green

criminology and cyberlaw to develop a unified analytical framework for assessing criminal responsibility in digital environmental governance. Third, it proposes a model of smart and sustainable criminal regulation that recalibrates classical doctrines of culpability, attribution, and enforcement while preserving their normative coherence.

Methodologically, the study adopts a normative and comparative legal approach to evaluate doctrinal adequacy and identify emerging regulatory models. By bridging environmental sustainability principles with digital liability doctrines, this research advances a conceptual foundation for criminal law reform in the era of green technology and digital society.

Theoretical framework

Eco-digital harm and the risk society paradigm

The transformation of environmental governance through digital technology can be situated within the broader theoretical framework of the "risk society" (Beck, 1992) argues that modernity increasingly produces "manufactured risks" generated by technological advancement rather than natural forces. These risks are systemic, complex, and often invisible until harm materializes. Eco-digital crime exemplifies this phenomenon: environmental harm may emerge from algorithmic miscalculations, automated compliance failures, or digital manipulation of sustainability infrastructures.

Unlike traditional environmental crime often involving direct pollution or illegal extraction eco-digital harm operates through technologically mediated processes. The locus of risk shifts from visible physical acts to embedded digital architectures. This transformation complicates criminal liability because harm is no longer easily attributable to a single identifiable actor. Instead, responsibility may be diffused across networks of developers, operators, corporations, and regulatory systems.

Thus, the risk society paradigm highlights a structural misalignment between technologically generated environmental harm and legal frameworks grounded in individualized fault.

Green criminology and the expansion of environmental harm

Green criminology broadens the scope of criminal law analysis by focusing on environmental harm beyond conventional statutory definitions (Lynch, 2019); (White, 2020). It emphasizes ecological damage, corporate misconduct, and regulatory failures, often advocating for expanded accountability mechanisms.

However, while green criminology successfully reframes environmental harm as a matter of justice and sustainability, it traditionally concentrates on industrial pollution, extractive industries, and corporate negligence. Less attention has been devoted to the digital infrastructures that now govern environmental compliance, emissions monitoring, and renewable energy systems.

In eco-digital contexts, environmental harm may arise from data manipulation, cybersecurity breaches targeting renewable grids, or algorithmic bias within automated regulatory systems. These developments demand not only broader definitions of harm but also doctrinal adaptation in criminal liability theory.

Therefore, green criminology provides the normative foundation for recognizing environmental harm but requires integration with digital liability theory to address technologically mediated risk.

Cyberlaw, algorithmic governance, and attribution

Cyberlaw scholarship examines how digital environments reshape legal doctrines of jurisdiction, attribution, and responsibility. (Brenner, 2010) and (Kerr, 2022) demonstrate that cybercrime challenges traditional territorial assumptions and complicates proof of intent. Similarly, (Hildebrandt, 2015) argues that smart technologies embed normative decision-making within algorithmic systems, thereby transforming the epistemic structure of law.

A central insight from cyberlaw is that digital environments destabilize causal linearity. Actions are mediated through code, distributed servers, and transnational infrastructures. In eco-digital systems such as blockchain-based carbon markets or AI-driven environmental compliance tools harm may result from automated processes operating beyond direct human oversight (Wagner, W., & Steinzor, 2022).

(Lessig, 2006) proposition that "code is law" is particularly relevant in this context. If technological architecture regulates behavior, then criminal law must engage with code as a regulatory instrument rather than treat it as an external technical domain. This insight reinforces the need to reconsider doctrines of intent (mens rea), causation, and corporate liability in eco-digital contexts.

Recent scholarship further emphasizes the regulatory implications of algorithmic governance. (Yeung, 2018) argues that algorithmic systems increasingly perform regulatory functions traditionally exercised by legal institutions. Similarly, (Wagner, W., & Steinzor, 2022) demonstrate that administrative law structures are being recalibrated to address algorithmic decision-making within regulatory agencies. These developments confirm that digital infrastructures are no longer peripheral to governance but constitutive of regulatory authority itself.

Moreover, (Veale, M., 2021) highlight the emerging European regulatory approach toward artificial intelligence, underscoring the necessity of risk-based legal frameworks capable of addressing systemic technological harm. In eco-digital contexts, such risk-based models may offer guidance for recalibrating criminal liability standards.

Smart regulation and sustainable legal governance

The concept of smart regulation emphasizes adaptive, technology-integrated governance models capable of responding to complex regulatory challenges (Schartum, 2021). Rather than relying solely on punitive enforcement, smart regulation

incorporates digital monitoring tools, automated compliance systems, and collaborative governance mechanisms.

From a sustainability perspective, (Bosselmann, 2017) argues that legal systems must internalize ecological limits as foundational normative principles. A sustainable legal order therefore requires more than environmental protection statutes; it demands structural alignment between legal doctrine and long-term ecological integrity.

Integrating smart regulation with sustainability theory suggests that criminal law reform should not merely expand liability but also embed technological competence and ecological responsibility into enforcement frameworks. In eco-digital contexts, this integration becomes essential to preserve both accountability and regulatory legitimacy (Eubanks, 2022).

Toward an integrated analytical framework

Taken together, these theoretical strands reveal a common insight: environmental harm in the digital era is structurally different from traditional forms of crime. Risk society theory explains the systemic nature of technological harm. Green criminology foregrounds environmental justice and accountability. Cyberlaw exposes doctrinal challenges in digital attribution (Black, 2008). Smart regulation and sustainability theory provide governance-oriented solutions.

Table 1. Comparative literature mapping on environmental and digital liability

Author(s)	Focus Area	Approach	Limitation	Relevance to Eco-Digital Liability
Beck (1992)	Risk society	Sociological theory	No criminal liability analysis	Explains systemic technological risk
Lynch & Stretesky (2019)	Green criminology	Environmental harm	Limited digital integration	Expands environmental harm
Kerr (2022)	Cybercrime law	Doctrinal	No sustainability focus	Explains digital attribution
Yeung (2018)	Algorithmic regulation	Governance theory	Not environmental-specific	Shows regulatory automation
Bosselmann (2017)	Sustainability law	Normative theory	No digital liability	Provides sustainability principle
This Article	Eco-digital harm	Hybrid liability model	—	Integrates sustainability + digital liability

However, existing scholarship rarely synthesizes these perspectives into a unified criminal liability framework. This study bridges these domains by developing an integrated analytical model that conceptualizes eco-digital crime as technologically mediated environmental harm requiring doctrinal recalibration and regulatory innovation. This integrated framework serves as the conceptual foundation for the subsequent doctrinal and comparative analysis.

To clarify the analytical gap identified above, Table 1 provides a comparative mapping of the principal theoretical traditions and their respective limitations in addressing

technologically mediated environmental harm. As the comparison indicates, no single framework sufficiently captures the doctrinal complexity of eco-digital harm.

Method

This study employs a normative legal research method combined with a comparative legal approach. Normative legal research, as defined by (Van Hoecke, 2011), focuses on the systematic analysis of legal norms, doctrines, and principles to evaluate coherence, consistency, and adequacy within a legal system. Unlike empirical socio-legal research, normative research examines law as a normative system, emphasizing doctrinal interpretation and conceptual analysis.

The normative method is particularly appropriate for this study because the central research question concerns the adequacy and reformulation of criminal liability doctrines in response to eco-digital risks. As (McConville, M., & Chul, 2007) explain, doctrinal legal research is suitable when the objective is to clarify legal principles, identify doctrinal gaps, and propose normative reforms. Accordingly, this study analyzes primary legal materials, including criminal codes, environmental protection statutes, and cybercrime regulations, alongside secondary sources such as scholarly works and international legal instruments.

The analytical procedure consists of three stages. First, doctrinal analysis is conducted to assess the conceptual structure of criminal liability particularly attribution, intent (*mens rea*), and causation within environmental and digital contexts. Second, conceptual analysis is applied to evaluate the challenges posed by AI-mediated harm and distributed agency in green technology systems. Third, normative evaluation is undertaken to determine whether existing doctrines remain adequate in addressing eco-digital criminal risks.

In addition, a comparative legal approach is employed following the functional method described by (Zweigert, K., & Kotz, 1998). This method compares how different legal systems address similar regulatory problems rather than merely comparing statutory texts. Selected jurisdictions, including the European Union and Southeast Asian regulatory frameworks, are examined to identify emerging models of environmental cybercrime regulation and digital evidence governance.

Through this combined doctrinal and functional comparative analysis, the study formulates a proposed model of smart and sustainable criminal regulation capable of responding to technological transformation while maintaining doctrinal coherence.

Results and discussion

The structural inadequacy of classical criminal liability

1. Individualized culpability and distributed agency
   Classical criminal law is premised on the attribution of blame to identifiable individuals acting with intention or negligence. However, eco-digital harm often emerges from distributed systems in which multiple actor software developers, corporate managers, system operators, and automated algorithms interact within complex technological architectures. The fragmentation of agency complicates the attribution of personal fault and weakens the traditional focus on singular perpetrators (Duff, 2007; H. L. A. Hart, 1968).

2. Linear causation in non-linear digital systems
   Conventional doctrines of causation rely on direct, traceable links between conduct and harm. Yet in digitally mediated environmental governance, harm may result from layered algorithmic processes, automated feedback mechanisms, or transnational data flows (Wagner, W., & Steinzor, 2022; Yeung, 2018). Causation becomes probabilistic and systemic rather than linear. Under such conditions, strict adherence to traditional causation tests risks excluding technologically mediated harms from criminal accountability.

3. Territorial jurisdiction in transnational digital infrastructures
   Criminal law traditionally operates within territorially bounded jurisdictional frameworks (Brenner, 2010). Digital environmental systems, however, operate across borders. Cloud-based data storage, cross-border carbon trading platforms, and globally integrated renewable energy networks challenge territorial assumptions (Kerr, 2022). This jurisdictional diffusion undermines enforcement consistency and complicates prosecution.

4. Doctrinal consequences
   Taken together, distributed agency, algorithmic causation, and jurisdictional fluidity expose structural tensions within classical criminal liability (Frisch, 2020) (Roxin, 2016). The issue is not merely evidentiary complexity but doctrinal misalignment. Criminal law, designed for direct physical misconduct, must confront technologically mediated harm that operates through systemic digital infrastructures.

These structural inadequacies provide the doctrinal justification for reconstructing liability within a hybrid eco-digital framework.

Reconstructing criminal liability: A hybrid eco-digital model

1. The structural inadequacy of classical liability
   Classical criminal liability rests on three foundational pillars: individual culpability, direct causation, and territorial jurisdiction (Duff, 2007; H. L. A. Hart, 1968). These pillars presuppose that harm results from identifiable human action within a

clearly bounded legal system. However, eco-digital harm disrupts each of these assumptions in structurally significant ways.

First, technologically mediated environmental harm frequently arises from algorithmic processes or automated system interactions rather than direct human conduct (Hildebrandt, 2015; Yeung, 2018). Second, causation becomes diffuse in digitally networked infrastructures, where multiple actors and systems contribute to harmful outcomes, thereby challenging traditional doctrines of factual and legal causation (H. Hart, 2008). Third, jurisdictional boundaries are blurred in transnational digital ecosystems that transcend territorial sovereignty (Brenner, 2010; Kerr, 2022).

The result is not merely evidentiary difficulty but structural inadequacy. Traditional liability doctrine struggles to reconcile distributed agency with individualized blameworthiness (Latour, 2005). Therefore, incremental adaptation is insufficient; conceptual recalibration is required in order to preserve doctrinal coherence.

2. Conceptualizing eco-digital crime

This article proposes that eco-digital crime constitutes a distinct analytical category characterized by three defining features.

a. Technologically mediated harm

Environmental damage increasingly arises through digital infrastructures, such as automated monitoring systems, AI-driven compliance tools, and blockchain-based carbon registries. Such infrastructures embed regulatory norms within technological architecture (Hildebrandt, 2015), thereby transforming the site of legal risk production.

b. Distributed agency

Responsibility is dispersed across human actors (developers, operators, corporate executives) and technological systems. Actor-network theory demonstrates that agency within socio-technical systems is relational rather than purely individual (Latour, 2005), complicating conventional attribution models.

c. Algorithmic causation

Harm may result from code-based decision processes that operate beyond immediate human intention. Algorithmic regulation reshapes governance by embedding normativity into automated decision structures (Yeung, 2018), thereby challenging linear causation assumptions (Hart, H.L.A., 1985).

Recognizing eco-digital crime as a structurally distinct category allows criminal law to move beyond analogical reasoning toward doctrinal clarity.

3. *Hybrid* responsibility *framework*

To address eco-digital risks, this study proposes a Hybrid Responsibility Model consisting of three integrated dimensions.

a. Expanded attribution mechanisms

Criminal liability should incorporate structured corporate and supervisory liability where technological systems operate under organizational control. Contemporary regulatory theory acknowledges that complex risks require institutional rather than purely individual accountability (Ayres, I., & Braithwaite, 1992; Braithwaite, 2002).

Negligent design, failure to implement cybersecurity safeguards, or inadequate algorithmic oversight should therefore trigger enhanced responsibility standards. This approach preserves the moral core of criminal law while acknowledging systemic technological interdependence (Duff, 2007).

b. Functional causation doctrine

Instead of requiring strictly linear causation, courts should adopt a functional causation test that evaluates whether the actor exercised effective control over the risk-generating system. Such an approach aligns with modern understandings of risk regulation in complex technological societies (Beck, 1992).

Under this model:

1) Liability attaches to those who design, deploy, or negligently supervise high-risk eco-digital infrastructures.
2) Algorithmic mediation does not sever causation where foreseeable harm results from inadequate governance (Yeung, 2018).

This reconceptualization seeks to preserve doctrinal coherence while accommodating technological realities.

c. Integrated smart enforcement

Substantive reform must be complemented by procedural modernization. Smart enforcement mechanisms including AI-assisted compliance audits, blockchain-based environmental verification, and cross-border digital cooperation reflect the growing convergence between regulatory governance and technological oversight (Wagner, W., & Steinzor, 2022).

Importantly, technological integration should serve legal accountability, not replace normative judgment. Human oversight remains essential to preserve legality and proportionality principles (Hildebrandt, 2015).

4. *Normative justification*
   The hybrid eco-digital liability model is normatively justified on three grounds.
   a. Sustainability imperative
      Environmental integrity requires adaptive legal mechanisms capable of responding to systemic technological risk (Beck, 1992).
   b. Doctrinal coherence
      Criminal law must evolve to remain internally consistent when technological mediation alters causation and agency (Duff, 2007; H. L. A. Hart, 1968).
   c. Regulatory legitimacy
      Failure to address eco-digital risks undermines public confidence in environmental governance and weakens institutional legitimacy (Braithwaite, 2002).

Thus, the model does not abandon classical principles of culpability but recalibrates them to remain operational in digitally mediated environments.

5. The *core* contribution
   The primary contribution of this study lies in shifting the analytical focus from isolated environmental or cyber offenses toward an integrated eco-digital liability paradigm. Rather than treating digital mediation as an external complication, this model recognizes technological architecture as structurally embedded within contemporary environmental harm (Hildebrandt, 2015).

   Accordingly, criminal liability must evolve from a purely individualistic paradigm toward a calibrated hybrid model capable of addressing systemic and algorithmically mediated harm while preserving foundational rule-of-law principles.

Illustrative regulatory developments in eco-digital contexts

1. Digital manipulation of environmental monitoring systems
   Recent enforcement trends demonstrate how environmental governance increasingly relies on digital infrastructures. Automated emissions monitoring systems (EMS), smart grids, and blockchain-based carbon registries are designed to enhance transparency and compliance. However, these systems have also become targets of digital manipulation.

   For example, regulatory investigations within the European Union have identified instances of falsified environmental data submissions facilitated through digital reporting systems. Such cases illustrate how environmental harm may occur not through physical pollution alone but through manipulation of data that structures regulatory oversight.

   These developments reinforce the argument that eco-digital harm is mediated through code-based infrastructures. The criminal conduct may involve data interference, cybersecurity breaches, or algorithmic manipulation rather than

direct physical acts. Consequently, traditional liability models focused solely on tangible environmental damage become insufficient.

2. Cybersecurity risks to renewable energy infrastructure
   Renewable energy systems particularly smart grids and digitally connected power distribution networks are increasingly vulnerable to cyber intrusion. Cyberattacks on energy infrastructures demonstrate how environmental sustainability initiatives themselves can generate new forms of criminal risk.

   Such vulnerabilities complicate criminal attribution. When a digitally connected renewable grid fails due to external interference or internal software malfunction, determining responsibility requires analysis beyond conventional negligence or intent-based frameworks. The harm is technologically mediated, transnational, and structurally complex.

   This illustrates the necessity of expanded attribution standards and supervisory responsibility within eco-digital infrastructures.

3. Algorithmic governance and automated compliance systems
   Governments increasingly employ AI-driven systems to monitor environmental compliance, detect regulatory anomalies, and automate reporting obligations. While these systems enhance efficiency, they also introduce risks of algorithmic bias, data corruption, or systemic oversight failure.

   In such cases, environmental harm may arise from flawed algorithmic design rather than deliberate misconduct. The question then becomes whether criminal liability should attach to programmers, deploying corporations, regulatory authorities, or a combination thereof.

   These scenarios concretely demonstrate the structural challenges outlined in the Hybrid Responsibility Model. They validate the need for functional causation standards and supervisory liability mechanisms.

Conclusion

The convergence of green technology and digital society marks a structural transformation in environmental governance. As sustainability infrastructures become increasingly embedded within algorithmic and digitally networked systems, environmental harm is no longer confined to direct physical misconduct. Instead, it emerges through technologically mediated processes characterized by distributed agency, algorithmic causation, and transnational interconnectivity.

This article has argued that such eco-digital risks expose fundamental inadequacies within classical criminal liability doctrines. Frameworks grounded exclusively in individualized intent, linear causation, and territorially bounded jurisdiction struggle to respond effectively to harms generated within complex technological ecosystems. The

challenge is therefore not merely the proliferation of new offenses, but the transformation of how responsibility itself must be conceptualized.

By integrating insights from green criminology, cyberlaw, risk society theory, and smart regulation, this study advances a hybrid eco-digital liability model. This model recalibrates traditional doctrines of culpability and attribution without abandoning their normative foundations. It proposes expanded supervisory responsibility, functional causation standards, and technologically informed enforcement mechanisms as necessary components of a smart and sustainable criminal law system.

The broader implication is clear: criminal law must evolve alongside technological transformation to preserve both environmental integrity and regulatory legitimacy. A failure to adapt risks rendering environmental criminal enforcement normatively obsolete in the face of digitally mediated harm.

Future research should explore empirical enforcement practices, algorithmic accountability mechanisms, and transnational cooperation frameworks to further operationalize eco-digital criminal liability. As environmental sustainability increasingly depends on digital infrastructures, the relationship between code, governance, and criminal responsibility will become a defining issue of twenty-first century legal scholarship.

References

1. Ayres, I., & Braithwaite, J. (1992). *Responsive Regulation: Trancending the Deregulation Debate*. Oxford University Press.
2. Beck, U. (1992). *Risk Society: Toward a New Modernity*. Sage Publications.
3. Black, J. (2008). Contructing and Contesting Legitimacy and Accountability in Policentric Regulatory Regime. *Regulation & Govermance*, *2*(2), 137–164.
4. Bosselmann, K. (2017). *The Principle of Sustainability: Transforming Law and Governance (2nd ed.)*. Routledge.
5. Braithwaite, J. (2002). *Restorative Justice and Responsive Regulation*. Oxford University Press.
6. Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.
7. Duff, R. A. (2007). *Answering for Crime: Responsibility and Liability in the Criminal Law*. Hart Publishing.
8. Eubanks, V. (2022). Automating Inequality in the Gital Administrative State. *Science, Technology & Human Values*, *47*(2), 215–240.
9. Frisch, W. (2020). *Strafrecht und Strafprozessrecht im Rechtsstaat*. C.H. Beck.
10. Hart, H.L.A., & H. (1985). *Causation in the Law (2nd ed.)*. Oxford University Press.
11. Hart, H. (2008). *Punishment and Politics*. Oxford University Press.
12. Hart, H. L. A. (1968). *Punishment and Responsibility: Essays in the Philosophy of Law*. Oxford University Press.
13. Hildebrandt, M. (2015). *Smart Technologies and the End(s) of Law*. Edward Elgar Publishing.
14. Kerr, O. S. (2022). *Computer Crime Law (4th ed.)*. West Academic Publishing.
15. Latour, B. (2005). *Reassembling the Social: An Indtroduction to Actor-Network Theory*. Oxford University Press.
16. Lessig, L. (2006). *Code: Version 2.0.* Basic Books.
17. Lynch, M.J., & S. (2019). *Green Criminology: Crime, Justice, and the Environment (2nd ed)*. University of California Press.
18. McConville, M., & Chul, W. H. (eds. . (2007). *Research Methods for Law*. Edinburgh University Press.
19. Roxin, C. (2016). *Strafrecht: Allgemeiner Teil*. C.H. Beck.
20. Schartum, D. . (2021). Digital Transformation o Public Administration and the Role of Law. *Artificial Intelligence and Law*, *29*(1), 1–25.

21. Van Hoecke, M. (2011). Methodology of Comparative Legal Research. *Law and Methode*, *1*, 1–35.
22. Veale, M., & B. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, *22*(4), 97–112.
23. Wagner, W., & Steinzor, R. (2022). Recalibrating Regulation in the Digital Age: Administrative Law and Algorithmic Governance. *Administratif Law Review*, *74*(3), 567–612.
24. White, R. (2020). *Climate Change Criminology*. Bristol University Press.
25. Yeung, K. (2018). Algorithma Regulation: A Critical Interrogation. *Regulation & Govermance*, *12*(4), 505–523.
26. Zweigert, K., & Kotz, H. (1998). *An Introduction to Comparative Law (3rd re.ed.,T. Weir, Trans*. Oxford University Press.