Journal of Political Science, Law & Governance
ISSN: 3059-8303, Volume – 2, Issue – 2, 2026
DOI: https://doi.org/10.63456/jpslg-2-2-109

CO-CREATED LEGAL EDUCATION AND THE PREVENTIVE ARCHITECTURE OF EU CYBERCRIME GOVERNANCE

[1]ELEMEGIOUS MUGAMBA

Research Fellow Universitat Autònoma de Barcelona; https://orcid.org/0009-0002-0262-4098,

Email: elemegious.mugamba@autonoma.cat

Corresponding author: ELEMEGIOUS MUGAMBA

ABSTRACT

European Union cybercrime governance has achieved significant legislative and institutional sophistication through criminal law harmonisation, cybersecurity risk regulation, and transnational enforcement coordination. Nevertheless, prevailing regulatory and scholarly approaches remain disproportionately enforcement-centric, overlooking the epistemic infrastructures necessary for sustainable regulatory coherence and preventive compliance. This article identifies a critical lacuna in EU digital governance: the marginalisation of legal education as a structural regulatory instrument capable of enhancing cybercrime prevention, institutional resilience, and harmonised enforcement across Member States. Advancing an interdisciplinary analytical framework integrating preventive governance theory, regulatory pluralism scholarship, and co-creation governance models, the article argues that co-created legal education constitutes a novel form of preventive regulatory infrastructure within EU cybercrime governance. The study employs doctrinal analysis of EU cybercrime legal instruments, comparative evaluation of Member State educational governance across four analytically distinct jurisdictions, and normative regulatory modelling. Confronting the constitutional constraint of Article 165(4) TFEU — which expressly excludes legislative harmonisation of education — the article designs its normative model to operate through soft-law coordination, the Open Method of Coordination, and programmatic EU financing. It contributes original knowledge by reconceptualising legal education as a soft harmonisation mechanism that strengthens mutual trust, regulatory legitimacy, and interdisciplinary compliance ecosystems within multi-level digital governance. By proposing an institutionally grounded co-created legal education model, the study advances a preventive epistemic governance paradigm with transformative implications for EU cybersecurity policy, national regulatory capacity-building, and transnational cybercrime governance.

KEYWORDS: EU cybercrime governance; preventive governance; legal education harmonisation; regulatory pluralism; co-creation; epistemic governance; Article 165 TFEU; NIS2 Directive; Directive 2013/40/EU

1. INTRODUCTION

The exponential expansion of cybercrime across the European Union has catalysed profound regulatory and institutional challenges that transcend traditional criminal law enforcement paradigms. As digital infrastructures increasingly underpin economic, governmental, and social interactions, cyber threats have evolved into a systemic governance risk capable of destabilising democratic institutions, financial systems, and critical societal infrastructures. The European Commission has characterised cybercrime as among the most complex transnational threats confronting the Union, necessitating integrated regulatory, technological, and institutional responses that extend beyond reactive enforcement mechanisms.[1]

Despite significant legislative harmonisation through Directive 2013/40/EU on attacks against information systems and the NIS2 Directive, structural disparities persist across Member States in operational capacity, compliance culture, and preventive governance infrastructures.[2] These disparities are not incidental; they reflect a systemic failure to develop the epistemic infrastructures — coordinated legal education frameworks, shared interpretative methodologies, and harmonised compliance cultures — without which even well-designed legislative instruments cannot achieve their governance objectives. The jurisprudential recognition of this problem is implicit in landmark rulings such as *Digital Rights Ireland*[3] and *Schrems II*[4], where the Court of Justice of the European Union (CJEU) repeatedly underscored that effective digital governance requires regulatory actors to balance security imperatives with fundamental rights protections through sophisticated legal reasoning — a capacity that cannot be assumed absent coordinated legal education.

This article advances the thesis that co-created legal education constitutes an emergent and systematically neglected form of preventive governance capable of reinforcing regulatory harmonisation, enhancing compliance ecosystems, and strengthening institutional resilience against cybercrime threats. This claim is advanced with two important qualifications. First, harmonised legal education is presented as a necessary and critically undervalued regulatory lever, not a panacea; deep-rooted divergences arising from constitutional traditions, prosecutorial cultures, and resource asymmetries are independent sources of enforcement fragmentation that educational governance can mitigate but cannot eliminate.[5] Second, the article confronts directly the constitutional constraint of Article 165(4) TFEU, which expressly excludes harmonisation of national laws and regulations in the field of education, and designs the proposed model accordingly — through soft-law coordination, financial incentives, and the Open Method of Coordination rather than directive-based compulsion.[6]

The article makes four original contributions to EU digital governance scholarship. First, it reconceptualises legal education as preventive regulatory infrastructure rather than an auxiliary capacity-building tool — a paradigm shift with significant implications for how EU institutions approach digital skills policy. Second, it develops an integrated interdisciplinary framework linking preventive governance theory, regulatory pluralism, and co-creation scholarship not previously applied to cybercrime legal education. Third, it provides a critically evaluated comparative analysis of four Member State educational governance models. Fourth, it proposes a constitutionally grounded normative co-creation model with detailed institutional design, financing architecture, and accountability mechanisms.

The article proceeds as follows. Section II surveys existing scholarship and identifies the theoretical gaps underpinning the marginalisation of legal education in EU cybercrime governance discourse. Section III develops the interdisciplinary theoretical framework. Section IV undertakes a doctrinal analysis of EU cybercrime legal instruments. Section V provides the comparative governance analysis. Section VI proposes the normative co-created legal education model. Section VII concludes.

2. THE MARGINALISATION OF LEGAL EDUCATION IN EU CYBERCRIME GOVERNANCE SCHOLARSHIP

2.1 THE ENFORCEMENT-CENTRIC TRAJECTORY

European Union cybercrime governance has generated a substantial body of interdisciplinary scholarship spanning criminal law harmonisation, cybersecurity policy, digital governance, and transnational regulatory cooperation. Early scholarly engagement concentrated on harmonisation challenges arising from divergent national criminal justice traditions. Sieber's foundational analysis argued that cybercrime regulation demands transnational coordination capable of reconciling fragmented jurisdictional authority and differing enforcement standards.[7] This doctrinal orientation was reinforced by Directive 2013/40/EU, which aimed to standardise substantive criminal offences and enhance judicial cooperation. Carrapico and Trauner demonstrated how supranational coordination structures facilitate operational enforcement integration through Europol.[8] Mitsilegas's comprehensive treatment of EU criminal law after Lisbon examined the transformation of judicial cooperation through the European Arrest Warrant and European Investigation Order.[9] This literature has produced valuable insights into institutional cooperation mechanisms and their implications for Member State sovereignty, but its analytical scope remains predominantly enforcement-centric, treating capacity-building and education as technical rather than constitutive governance matters.

Parallel developments in cybersecurity scholarship have emphasised technological resilience and infrastructure protection. The emergence of the NIS2 Directive has stimulated extensive academic debate concerning regulatory compliance frameworks, risk management obligations, and public–private cybersecurity partnerships.[10] Yet, despite recognising the importance of skills development and awareness training, this scholarship rarely interrogates the normative dimensions of legal education as a regulatory instrument. The failure reflects a broader structural characteristic of EU digital governance scholarship: cybercrime is conceptualised primarily as a law enforcement and technical security challenge rather than as a knowledge governance phenomenon.

2.2 REGULATORY GOVERNANCE THEORY AND THE NEGLECT OF EPISTEMIC INFRASTRUCTURE

Black's theory of decentred regulation argues that modern regulatory systems increasingly rely upon networks of public and private actors engaged in collaborative governance processes.[11] Black and Baldwin's subsequent development of "really responsive regulation" emphasised that effective regulatory frameworks must be attentive to the behavioural, organisational, and normative contexts in which regulated actors operate.[12] These frameworks have significantly influenced EU digital governance scholarship but have rarely been applied to examine the epistemic foundations of regulatory compliance. Legal education is consistently conceptualised as an implementation support mechanism rather than as a constitutive element of regulatory governance architecture. Slaughter's concept of transnational epistemic communities provides the most analytically productive bridge between regulatory governance theory and the role of legal education.[13] Her argument that effective global governance depends upon networks of professionals sharing regulatory knowledge and normative standards directly implies that the absence of coordinated legal education frameworks undermines transnational governance effectiveness.

2.3 LEGAL PLURALISM, EPISTEMIC FRAGMENTATION, AND THE EDUCATIONAL GAP

Walker's analysis of global law, extended by Berman's global legal pluralism framework, conceptualises the EU as a regulatory environment characterised by overlapping supranational, national, and private normative orders.[14] Within cybercrime governance, this pluralistic environment creates interpretative divergences that complicate enforcement cooperation. The principle of mutual recognition presupposes mutual trust among national judicial systems.[15] As the CJEU demonstrated in *Minister for Justice and Equality v LM*, such trust cannot simply be presumed; it requires shared institutional standards and normative coherence.[16]

Empirical studies conducted by the European Judicial Training Network document significant disparities in cybercrime legal training across Member States, with standardised evaluation of training outcomes almost entirely absent.[17] These disparities represent what this article characterises as an *epistemic governance deficit* — a structural failure to invest in the knowledge production and dissemination infrastructures upon which regulatory effectiveness depends. This deficit has attracted limited scholarly attention precisely because it does not manifest in the legislative or institutional forms that mainstream EU cybercrime scholarship is equipped to analyse.

2.4 IDENTIFYING THE THEORETICAL GAP

The preceding analysis reveals four interrelated gaps. First, the enforcement-centric orientation of EU criminal law scholarship has obscured the preventive regulatory potential of legal education. Second, cybersecurity capacity-building literature has prioritised technical training while neglecting doctrinal legal literacy. Third, regulatory governance theory has insufficiently examined the epistemic infrastructures underpinning compliance mechanisms. Fourth, legal pluralism scholarship has identified regulatory fragmentation without exploring educational harmonisation — pursued through constitutionally appropriate soft-law mechanisms — as a mechanism for addressing it. These gaps collectively sustain a scholarly paradigm in which legal education is treated as ancillary to cybercrime governance. The article addresses this paradigmatic failure by developing an interdisciplinary theoretical framework that reconceptualises legal education as preventive regulatory infrastructure.

3. THEORETICAL FRAMEWORK: PREVENTIVE GOVERNANCE, REGULATORY PLURALISM, AND CO-CREATION

3.1 PREVENTIVE GOVERNANCE AND ANTICIPATORY REGULATORY STRATEGY

The regulatory transformation of cyberspace within the European Union demands theoretical frameworks capable of addressing the anticipatory, transnational, and technologically adaptive nature of cybercrime. Traditional criminal law paradigms, rooted in deterrence and post-factum enforcement, are structurally ill-equipped to address cyber threats that evolve faster than legislative and institutional responses. Preventive governance has therefore emerged as a critical theoretical paradigm for reconceptualising regulatory strategies in complex risk societies.[18]

Zedner's influential articulation of preventive criminal justice emphasises that contemporary governance increasingly prioritises risk management, behavioural regulation, and knowledge dissemination as mechanisms for crime prevention.[19] Ashworth and Zedner's analysis of *Preventive Justice* demonstrates that anticipatory regulatory strategies require not merely technical risk assessment but normative judgement about the proportionality and legitimacy of pre-emptive intervention.[20] Within EU cybercrime governance, these normative demands underscore the necessity of legal education: regulatory actors cannot exercise proportionate and rights-compatible judgement without sophisticated legal literacy. The CJEU's reasoning in *H.K. v Prokuratuur*[21] — extending proportionality requirements to law enforcement access to electronic communications data in cybercrime investigations — illustrates the interpretative demands placed upon regulatory actors and the structural importance of legal education as a governance prerequisite.

Preventive governance scholarship also highlights the risk that anticipatory regulatory strategies may generate governance pathologies. Harcourt's critique of actuarial approaches to crime control warns that preventive frameworks can undermine civil liberties if not subject to robust normative constraints.[22] This reinforces the article's insistence that co-created legal education must integrate fundamental rights literacy as a non-negotiable component of its curriculum design.

3.2 REGULATORY PLURALISM AND THE MULTI-LEVEL GOVERNANCE CHALLENGE

Walker's pluralist analysis of global law, extended by Krisch's account of the pluralist structure of postnational law, provides the analytical framework for understanding the regulatory complexity that EU cybercrime governance must navigate.[23] The EU operates within a multi-layered regulatory environment. Cybercrime governance exemplifies this pluralistic architecture: EU legislative instruments, national criminal law systems, private cybersecurity standards, and international frameworks such as the Budapest Convention and its Second Additional Protocol[24] interact within shared regulatory spaces, generating both coordination opportunities and interpretative divergences.

The principle of mutual recognition since Tampere[25] presupposes mutual trust among national judicial systems. However, as the CJEU's reasoning in *LM*[26] and *Aranyosi and Căldăraru*[27] demonstrates, such trust is structurally dependent upon shared institutional standards and normative coherence among Member States. Interpretative fragmentation and institutional asymmetries — precisely the governance deficits that differential legal education standards produce — directly undermine the mutual trust upon which enforcement cooperation depends. This article advances the theoretical proposition that epistemic harmonisation through legal education represents a necessary complement — alongside institutional coordination and legislative harmonisation — to effective management of regulatory pluralism in EU cybercrime governance.

Journal of Political Science, Law & Governance
ISSN: 3059-8303, Volume – 2, Issue – 2, 2026
DOI: https://doi.org/10.63456/jpslg-2-2-109

3.3 CO-CREATION THEORY: FROM HIERARCHICAL REGULATION TO COLLABORATIVE GOVERNANCE

Co-creation theory represents a transformative governance paradigm that challenges hierarchical regulatory models by promoting collaborative policy design involving public authorities, private actors, academia, and civil society. Originating within Ostrom's analysis of collective action in commons governance[28] and developed within public administration scholarship, co-creation emphasises that complex governance challenges require participatory knowledge production and shared regulatory responsibility. Black's decentred regulation theory provides the most direct bridge between co-creation scholarship and EU digital governance.[29] By demonstrating that contemporary regulatory environments rely upon distributed networks integrating public and private actors in rulemaking and implementation, Black's framework explains why co-created legal education is not merely an innovative governance option but a structural necessity in the cybercrime domain. Slaughter's transnational epistemic communities and Haas's foundational analysis of international knowledge governance[30] further demonstrate that effective regulatory coordination across jurisdictions depends critically upon professional communities sharing interpretative standards — communities that can only be sustained through systematic co-created educational investment.

Co-creation principles are already embedded in the EU's Digital Education Action Plan[31] and ENISA's cross-sectoral training initiatives.[32] However, these initiatives remain fragmented, lack theoretical grounding in preventive governance and regulatory pluralism, and have not been designed to address the specific epistemic governance deficit identified in EU cybercrime legal education. This article provides the theoretical architecture to address these deficiencies.

3.4 CONSTITUTIONAL CONSTRAINTS: ARTICLE 165 TFEU AND THE SUBSIDIARITY PRINCIPLE

Any governance model proposing educational coordination at the EU level must confront the fundamental constitutional constraint of Article 165(4) TFEU, which expressly provides that, in the field of education, the European Parliament and Council shall adopt "incentive measures, excluding any harmonisation of the laws and regulations of the Member States."[33] This provision reflects a deliberate constitutional choice to preserve national sovereignty over educational systems. The principle of subsidiarity in Article 5(3) TEU reinforces this constraint by requiring EU-level action only where objectives cannot be sufficiently achieved by Member States individually.

This constitutional framework does not preclude EU-level coordination of cybercrime legal education; it defines the permissible instruments through which such coordination may lawfully occur. The Open Method of Coordination — a soft governance mechanism promoting convergence through peer review, benchmarking, and voluntary standard-setting — has demonstrated effectiveness in analogous EU policy domains including employment policy and social inclusion.[34] Davies's critique of subsidiarity as sometimes deployed to obstruct legitimate EU regulatory action notwithstanding,[35] the constitutional constraint in Article 165 TFEU reflects a genuine policy rationale that the normative model proposed in this article respects and accommodates. The proposed model operates through: voluntary minimum training standards developed through consensus-based governance; financial incentive structures using existing EU financing instruments; programmatic governance through the Open Method of Coordination; and soft-law benchmarking and peer review mechanisms.

3.5 TOWARD AN INTEGRATED PREVENTIVE EPISTEMIC GOVERNANCE ARCHITECTURE

The integration of preventive governance, regulatory pluralism, co-creation theory, and constitutional constraint analysis provides a comprehensive interdisciplinary framework for reconceptualising EU cybercrime governance. The theoretical synthesis advances three interrelated propositions. First, legal education functions as a preventive regulatory instrument capable of reducing enforcement burdens by fostering compliance-oriented legal cultures and anticipatory institutional behaviour. Second, co-created educational frameworks enhance governance legitimacy by integrating diverse regulatory stakeholders within knowledge production processes, while institutional safeguards prevent regulatory capture. Third, harmonised legal education — pursued through constitutionally appropriate soft-law mechanisms — facilitates transnational cooperation by standardising interpretative methodologies and enforcement practices across Member States, strengthening the mutual trust upon which EU criminal cooperation depends.

4. DOCTRINAL ANALYSIS OF EU CYBERCRIME LEGAL INSTRUMENTS: STRUCTURAL TRAINING DEFICIENCIES

4.1 THE ARCHITECTURE OF EU CYBERCRIME LEGAL REGULATION

The European Union's cybercrime regulatory regime has evolved into a sophisticated multilayered legal architecture combining criminal law harmonisation, cybersecurity risk governance, data protection regulation, and digital market oversight. Notwithstanding its legislative sophistication, the framework is characterised by structural training deficiencies that undermine regulatory harmonisation and enforcement effectiveness. These deficiencies stem from three interrelated sources: the fragmented distribution of competence across Member States; the rapid technological evolution of cyber threats; and the absence of integrated epistemic infrastructures capable of sustaining regulatory coherence.

4.2 DIRECTIVE 2013/40/EU: THE LIMITS OF SUBSTANTIVE HARMONISATION

Directive 2013/40/EU represents the cornerstone of EU cybercrime criminal law harmonisation, establishing minimum standards for criminalising cyber offences and strengthening cross-border enforcement cooperation.[36] The Directive aligns EU cybercrime law with the Council of Europe's Budapest Convention and its Second Additional Protocol on Enhanced Co-operation and Disclosure of Electronic Evidence,[37] thereby facilitating transnational legal cooperation. Nevertheless, the Directive's harmonisation model remains predominantly substantive and procedural, focusing on offence definition and investigative cooperation rather than institutional knowledge development. The Directive's reliance on minimum harmonisation reflects the EU's constrained competence in criminal law under Article 83(1) TFEU.[38] As the CJEU confirmed in *M.A.S. and M.B. (Taricco II)*, EU criminal law harmonisation operates within constitutional limits that preserve national criminal law traditions and procedural safeguards.[39]

Article 12 of the Directive obliges Member States to ensure adequate training for law enforcement and judicial authorities,[40] yet it provides no harmonised framework for implementing or evaluating such training. The European Commission's 2018 evaluation confirmed that Article 12 obligations are aspirational rather than binding, contributing to widely divergent training standards across Member States.[41] This doctrinal analysis reveals a structural tension at the heart of the Directive's design: the instrument seeks to harmonise enforcement outcomes while leaving the epistemic infrastructures necessary to achieve those outcomes entirely to Member State discretion. Legal education emerges as the critical and systematically neglected link between legislative harmonisation and enforcement effectiveness.

4.3 THE NIS2 DIRECTIVE: PREVENTIVE GOVERNANCE WITHOUT LEGAL LITERACY

The NIS2 Directive represents a significant evolution in EU cybercrime governance by shifting regulatory emphasis toward preventive cybersecurity risk management.[42] NIS2 imposes comprehensive security obligations on essential and important entities, requiring risk management measures, incident reporting procedures, supply chain security mechanisms, and cybersecurity competence development. Recitals 80–84 explicitly recognise that effective cybersecurity governance requires ongoing investment in skills and awareness, and Article 20 mandates training obligations for management bodies of regulated entities.[43]

However, NIS2's training provisions predominantly emphasise technical and operational competencies, implicitly assuming that cybersecurity compliance can be achieved without addressing the complex legal and governance dimensions of cybercrime regulation. As the CJEU demonstrated in *Schrems II*, effective cybersecurity governance requires regulatory actors to possess sophisticated understanding of transnational legal frameworks and fundamental rights jurisprudence — competencies that technical cybersecurity training alone cannot deliver.[44] ENISA's comparative assessments confirm that several Member States lack institutional mechanisms for integrating legal governance training across regulatory, prosecutorial, and judicial sectors.[45] This structural deficiency — the disaggregation of technical cybersecurity competence from legal governance literacy — constitutes the most significant normative gap in NIS2's preventive governance framework.

4.4 DATA PROTECTION REGULATION AS CYBERCRIME GOVERNANCE INSTRUMENT

The General Data Protection Regulation constitutes an indispensable component of EU cybercrime governance by establishing security obligations on data controllers and processors.[46] Article 32 requires organisations to implement technical and organisational measures to ensure data security appropriate to the risk — a standard requiring sophisticated legal and technical judgement. The European Data Protection Board plays a central role in facilitating regulatory harmonisation through interpretative guidance and coordinated enforcement actions,[47] yet empirical studies document that data protection authorities across Member States exhibit varying levels of legal and technical expertise, producing inconsistent enforcement practices.[48]

The CJEU's landmark ruling in *Google Spain v AEPD*[49] establishing the right to erasure illustrates the interpretative demands that evolving digital governance jurisprudence places upon regulatory actors. The consistent application of such jurisprudence across Member States requires harmonised interpretative frameworks that only coordinated legal education can provide. The GDPR further exemplifies the intersection between cybercrime governance and fundamental rights protection: cybersecurity measures often involve intrusive data monitoring and surveillance mechanisms raising significant Article 7 and Article 8 Charter concerns, making legal education programmes integrating cybersecurity compliance with fundamental rights literacy essential for maintaining normative legitimacy.

4.5 INSTITUTIONAL GOVERNANCE INSTRUMENTS AND SECTORAL FRAGMENTATION

Beyond legislative instruments, EU cybercrime governance relies upon institutional coordination through Europol's European Cybercrime Centre (EC3),[50] Eurojust's judicial cooperation function,[51] and ENISA's cybersecurity training and capacity-building mandates. While these institutions significantly enhance operational cooperation, their training initiatives remain fragmented within sectoral silos. Europol training targets law enforcement officers; ENISA focuses on technical

cybersecurity professionals; judicial and prosecutorial training is administered through national judicial academies with inconsistent curricula.[52] The European Commission's Digital Education Action Plan recognises the necessity of cross-sectoral digital competence development, yet its implementation in the cybercrime legal education domain remains embryonic.[53] This institutional fragmentation constitutes the organisational expression of the epistemic governance deficit identified at the legislative level.

4.6 MUTUAL RECOGNITION, ENFORCEMENT HARMONISATION, AND THE KNOWLEDGE DEFICIT

Mutual recognition, underpinning instruments such as the European Arrest Warrant and the European Investigation Order,[54] relies upon mutual trust among Member State judicial systems — trust presupposing shared legal standards and interpretative methodologies. Mitsilegas's analysis demonstrates that cybercrime investigations frequently encounter procedural and evidentiary inconsistencies resulting from divergent national legal traditions.[55] The CJEU's holdings in *Aranyosi and Căldăraru*[56] — that enforcement cooperation must be suspended where systemic fundamental rights violations exist — and in *LM*[57] — extending this logic to rule-of-law deficits — illustrate the structural dependency of mutual recognition on shared normative and institutional standards. Furthermore, in *Privacy International*[97] and *CNIL*[98], the Court extended the proportionality framework to law enforcement access to data in cybercrime contexts, placing interpretative demands upon regulatory actors that reinforce the centrality of legal education to enforcement effectiveness. Legal education plays a critical role in sustaining these shared normative standards by fostering compliance culture and interpretative convergence among the enforcement authorities upon whom mutual recognition depends.

5. COMPARATIVE GOVERNANCE ANALYSIS: LEGAL EDUCATION IN MEMBER STATE CYBERCRIME GOVERNANCE

5.1 METHODOLOGY, JURISDICTION SELECTION, AND SCOPE LIMITATIONS

This section undertakes a comparative governance analysis of cybercrime legal education initiatives in Spain, Estonia, Germany, and the Netherlands. These jurisdictions were selected to provide analytical diversity across four dimensions: legal system type (continental civil law variants); constitutional structure (unitary and federal); digital governance maturity; and cybersecurity policy architecture. The comparative methodology integrates doctrinal legal evaluation, institutional policy assessment, and empirical training programme analysis, consistent with regulatory governance scholarship's recognition that compliance effectiveness is shaped by institutional knowledge production and epistemic coordination.[58]

Methodological transparency requires two candid acknowledgements. First, the four-jurisdiction sample is deliberately bounded; it does not encompass Eastern European, Southern European, or Nordic Member States, each of which would likely reveal substantially different governance challenges, particularly those arising from weaker institutional capacities or different democratic consolidation trajectories.[59] The comparative analysis is offered as an empirically grounded but necessarily limited foundation for the normative model, not as a comprehensive mapping of EU-wide governance conditions. Second, outcome data is incorporated where available from institutional sources; where programme descriptions must substitute for impact evidence, this limitation is explicitly acknowledged consistent with standards of scholarly transparency.

5.2 SPAIN: INTEGRATED LEGAL EDUCATION WITHIN NATIONAL CYBERSECURITY STRATEGY

Spain represents an instructive case study in the deliberate integration of legal education within national cybersecurity governance. The Spanish National Cybersecurity Strategy 2019 explicitly mandates interdisciplinary training as a foundational element of national cyber resilience, recognising that effective cybercrime prevention requires coordinated legal, technical, and institutional competencies.[60] The Strategy's governance model is particularly significant because it conceptualises legal education not as an auxiliary training exercise but as a strategic governance instrument — directly aligned with the preventive governance theory advanced in Section III. The *Centro de Estudios Jurídicos* under the Ministry of Justice provides specialised cybercrime training programmes for judges and prosecutors, addressing digital evidence admissibility, cross-border data cooperation mechanisms, and cybersecurity regulatory compliance.[61] These programmes incorporate CJEU jurisprudence from *Schrems II* and *Digital Rights Ireland*[62] — promoting interpretative harmonisation with EU fundamental rights standards. INCIBE's empirical assessments report that interdisciplinary training programmes have enhanced institutional cooperation between law enforcement agencies and private-sector cybersecurity actors.[63]

Critical evaluation reveals, however, structural fragmentation across institutional sectors: judicial education programmes operate independently from law enforcement training academies, limiting the cross-sectoral knowledge exchange that effective cybercrime governance requires. Regional decentralisation has produced disparities in training accessibility across autonomous communities. Evaluation metrics measuring the actual impact of training on enforcement consistency are largely absent — a limitation constraining the strength of causal claims about training effectiveness. These asymmetries demonstrate that constitutional and structural factors constrain what educational governance can achieve independently of wider legislative and institutional reform.

Journal of Political Science, Law & Governance
ISSN: 3059-8303, Volume – 2, Issue – 2, 2026
DOI: https://doi.org/10.63456/jpslg-2-2-109

5.3 ESTONIA: DIGITAL GOVERNANCE LEADERSHIP AND THE TECHNICAL–LEGAL DIVIDE

Estonia is internationally recognised as a leader in digital governance and cybersecurity policy innovation, a position substantially shaped by its proactive regulatory and institutional response to the 2007 cyberattacks targeting government and financial institutions.[64] Estonia's cybersecurity governance model integrates legal education within broader digital literacy and public administration training programmes. The Estonian Information System Authority collaborates with academic institutions and judicial training bodies to deliver interdisciplinary cybercrime education programmes incorporating EU cybercrime directives and Budapest Convention standards.[65] ENISA assessments confirm that Estonia's integrated training approach has generated measurable improvements in institutional cyber resilience and enforcement efficiency.[66]

Estonia's model exhibits two analytically significant vulnerabilities. First, its small population and highly centralised governance structure enable rapid policy implementation but substantially limit the model's replicability in larger, constitutionally more complex Member States. Germany or Poland cannot adopt Estonian governance structures without fundamental constitutional transformation — a point limiting the direct transferability of Estonian best practices. Second, and more substantively, Estonia's internationally recognised e-governance expertise risks conflating technical cybersecurity proficiency with legal interpretative competence. The emphasis on digital literacy and technical incident management occasionally overshadows the doctrinal legal education that cybercrime prosecution, regulatory compliance, and fundamental rights adjudication require. This technical–legal divide is precisely the governance gap that co-created legal education frameworks are designed to bridge, and its presence in one of the EU's most advanced digital governance jurisdictions underscores the systemic nature of the epistemic governance deficit.

5.4 GERMANY: FEDERAL GOVERNANCE AND THE COORDINATION CHALLENGE

Germany's cybercrime education governance model is analytically valuable because it reproduces, at the national level, the same multi-level coordination challenges the EU faces supranationally. The Federal Criminal Police Office (Bundeskriminalamt) provides specialised cybercrime training for law enforcement authorities,[67] while the Federal Office for Information Security (BSI) delivers cybersecurity awareness and compliance training regarding NIS2 obligations.[68] Judicial and prosecutorial education is administered through federal and Länder judicial academies — creating a distributed governance structure that mirrors the EU's own multi-level architecture.

European Judicial Training Network comparative studies document divergent cybercrime legal training curricula across German federal states,[69] producing interpretative inconsistencies that complicate enforcement harmonisation within a single Member State. This finding provides empirical support — at the sub-national level — for the central theoretical proposition that decentralised training governance without coordinated baseline standards generates measurable enforcement asymmetries. Germany's experience demonstrates that achieving epistemic harmonisation through directive-based compulsion would be constitutionally inappropriate (as Article 165(4) TFEU confirms) and practically unnecessary if well-designed soft-law coordination mechanisms are deployed.

5.5 THE NETHERLANDS: COLLABORATIVE GOVERNANCE AND STRUCTURAL VULNERABILITIES

The Netherlands provides the comparative analysis's most developed example of co-creation principles applied to cybercrime legal education governance. The Dutch National Cyber Security Centre (NCSC) coordinates training involving law enforcement agencies, academic institutions, and private-sector cybersecurity organisations.[70] The Netherlands Institute for Judicial Training (SSR) provides specialised courses addressing cybercrime prosecution, digital evidence regulation, and EU cybersecurity legal frameworks. Empirical studies document that interdisciplinary training programmes enhance investigative coordination and regulatory compliance among enforcement authorities.[71]

The Netherlands has further developed innovative co-creation training initiatives involving technology companies and financial institutions, facilitating real-time knowledge exchange regarding emerging cyber threats — an approach explicitly aligned with EU public–private cybersecurity partnership policy.[72] Critical evaluation reveals, however, two structural governance vulnerabilities that the normative model in Section VI must address. First, many interdisciplinary training programmes operate on project-based funding models, producing governance discontinuity when funding cycles conclude — a structural instability antithetical to sustained preventive governance. Second, private-sector participation raises regulatory capture concerns: without robust oversight mechanisms, technology industry actors may acquire disproportionate influence over curriculum design and governance priorities. The Netherlands model demonstrates both the potential and the structural limitations of co-creation in legal education governance.

5.6 COMPARATIVE SYNTHESIS: GOVERNANCE LESSONS FOR THE NORMATIVE MODEL

Four cross-jurisdictional findings emerge with direct relevance to the normative model. First, all four Member States reflect the same foundational structural tension: strong co-creation principles at the policy design level are systematically undermined by fragmented implementation across institutional sectors, with judicial education, law enforcement training, and regulatory compliance training operating as disconnected silos. Second, jurisdictions demonstrating stronger cross-sectoral educational coordination — Estonia and the Netherlands — exhibit stronger enforcement outcomes as measured by ENISA capacity assessments and national evaluation studies, providing suggestive (though not conclusively causal) evidence supporting the article's central proposition. Third, sustainable funding is consistently identified as a critical governance vulnerability: project-based financing produces the institutional discontinuity antithetical to sustained preventive governance. Fourth, the German case provides a powerful sub-national analogy for the EU's supranational coordination challenge, demonstrating that decentralised educational governance without coordinated standards generates documented enforcement asymmetries tractable through soft governance rather than constitutionally impermissible harmonisation.

The comparative analysis confirms the geographic representativeness limitation noted in Section 5.A. Member States with weaker institutional capacities or different democratic consolidation trajectories would likely exhibit more acute governance deficits and greater resistance to epistemic harmonisation initiatives.[73] Future comparative research extending this framework to Eastern European, Southern European, and Nordic Member States would substantially enrich the empirical foundation of the normative model.

6. A NORMATIVE CO-CREATED LEGAL EDUCATION MODEL FOR EU CYBERCRIME PREVENTIVE GOVERNANCE

6.1 MODEL ARCHITECTURE: DESIGN PRINCIPLES AND CONSTITUTIONAL GROUNDING

The normative co-created legal education model proposed in this section addresses the structural deficiencies identified in the doctrinal analysis and validated by the comparative evidence. The model is built upon four design principles reflecting the theoretical framework developed in Section III and the constitutional constraints established by Article 165(4) TFEU. First, the model is preventively oriented: designed to mitigate cybercrime risks through anticipatory regulatory compliance rather than reactive enforcement. Second, it pursues harmonisation through epistemic convergence — promoting shared interpretative methodologies and regulatory knowledge through soft-law mechanisms rather than binding legislative compulsion. Third, it embeds co-creation as a governance mechanism enhancing regulatory legitimacy while incorporating robust accountability safeguards against regulatory capture. Fourth, it maintains fundamental rights compliance as a non-negotiable design constraint, integrating Charter jurisprudence and CJEU interpretative standards throughout its curriculum architecture.

6.2 INSTITUTIONAL ARCHITECTURE: THREE INTERCONNECTED PILLARS

(I) EU CYBERCRIME LEGAL EDUCATION COORDINATION PLATFORM

The first institutional pillar proposes the creation of an EU Cybercrime Legal Education Coordination Platform under the joint operational supervision of ENISA, Europol, and the European Judicial Training Network. Constitutionally, this platform operates without directive-making authority — which Article 165(4) TFEU renders impermissible — and instead develops voluntary minimum training standards, harmonised curriculum frameworks, and benchmark evaluation methodologies. The platform's curriculum architecture would incorporate: the substantive criminal law framework of Directive 2013/40/EU and its relationship to the Budapest Convention and Second Additional Protocol;[74] the risk management and training obligations of NIS2; the data protection and security obligations of the GDPR; relevant CJEU jurisprudence including *Digital Rights Ireland*, *Schrems II*, *Tele2 Sverige*, *Aranyosi and Căldăraru*, *H.K. v Prokuratuur*, *M.A.S. and M.B. (Taricco II)*, *Privacy International*, *CNIL*; and fundamental rights standards under the Charter.[75]

Participation by Member States would be incentivised through preferential access to the Digital Europe Programme, Horizon Europe, and the European Social Fund Plus — EU financing instruments providing the financial architecture for supporting co-created training initiatives without constitutionally impermissible legislative compulsion.[76] This financing strategy follows the model demonstrated in EU employment and social policy coordination, where financial incentives have successfully driven voluntary convergence toward EU-level benchmarks without directive-based harmonisation. The Open Method of Coordination would provide the governance mechanism: annual peer review cycles, comparative benchmarking against agreed minimum standards, and national action plans committing Member States to incremental convergence objectives within their own constitutional frameworks.[77]

(II) NATIONAL CO-CREATION EDUCATIONAL HUBS

The second institutional pillar proposes national co-creation educational hubs integrating law enforcement agencies, judicial training academies, academic institutions, and private-sector cybersecurity organisations within each Member State. These hubs would design and implement interdisciplinary training programmes tailored to national regulatory contexts while adhering to the voluntary EU standards developed by the Coordination Platform. The Dutch governance model provides empirical validation that cross-sectoral collaboration enhances investigative coordination and regulatory compliance;[78] the German case demonstrates the enforcement asymmetries that emerge when sub-national educational governance lacks coordinated baseline standards. National hubs would operate under multi-annual programme funding frameworks — addressing the structural discontinuity identified as a critical vulnerability in project-based funding models — supported by Digital Europe Programme and European Social Fund Plus allocations.

To address the regulatory capture risks inherent in multi-stakeholder co-creation, national hub governance structures would incorporate: mandatory public-interest representation including civil society and consumer advocacy organisations; transparent curriculum development processes subject to public consultation; independent academic peer review of training content to ensure doctrinal accuracy and fundamental rights compliance; and annual performance reporting to the EU Coordination Platform and relevant national parliamentary oversight bodies. These safeguards are essential design requirements consistent with the democratic accountability principles of the Charter[79] and the accountability norms established in the Cybersecurity Act.[80]

(III) TRANSNATIONAL KNOWLEDGE EXCHANGE NETWORKS

The third institutional pillar proposes transnational knowledge exchange networks facilitating cross-border training programmes, research collaboration, regulatory best-practice dissemination, and professional mobility for prosecutors, regulators, and cybersecurity professionals. These networks operationalise Slaughter's concept of transnational epistemic communities[81] and Haas's account of international knowledge governance,[82] creating the professional infrastructure through which shared interpretative methodologies and regulatory norms are sustained across jurisdictional boundaries. Holzinger and Knill's analysis of cross-national policy convergence demonstrates that transnational communication — precisely the function these networks serve — is among the most effective mechanisms of regulatory convergence in multi-level governance systems.[83] Knowledge exchange networks would build upon existing EU governance infrastructure: the European Judicial Training Network's judicial exchange programmes; ENISA's professional community platforms; and Europol's operational training partnerships.

6.3 IMPLEMENTATION PATHWAY AND CONSTITUTIONAL COMPLIANCE

The implementation of the normative model operates through three sequential phases. Phase one — voluntary coordination — involves the establishment of the EU Cybercrime Legal Education Coordination Platform through a Commission Communication and joint ENISA–EJTN–Europol memorandum of understanding, initiating voluntary curriculum benchmarking and best-practice exchange (indicative timeframe: 12–18 months). Phase two — programmatic integration — involves the integration of cybercrime legal education standards within Digital Europe Programme and European Social Fund Plus funding conditions, creating financial incentive structures for national hub development and multi-annual curriculum investment (indicative timeframe: 18–36 months from Phase one initiation). Phase three — systematic evaluation — involves the establishment of an independent evaluation framework measuring training outcomes against agreed benchmarks, informing iterative refinement of voluntary standards and identifying jurisdictions requiring targeted capacity-building support (ongoing from month 36).

NIS2 provides an existing legislative foundation for integrating enhanced training obligations within cybersecurity risk management frameworks[84] — and a forthcoming Commission review of NIS2 implementation could incorporate cybercrime legal education standards as recommended practice within the Directive's Article 20 compliance framework without requiring legislative amendment. The Digital Education Action Plan provides the broader policy architecture within which cybercrime legal education governance would sit.[85]

6.4 ANTICIPATED GOVERNANCE IMPACTS

The normative co-created legal education model is designed to generate four interrelated governance impacts. First, enhanced enforcement harmonisation: by promoting interpretative convergence and shared regulatory knowledge, the model addresses the documented enforcement asymmetries identified across the comparative analysis, strengthening the mutual trust upon which EU criminal cooperation depends. Second, strengthened compliance culture: by integrating legal literacy within cybersecurity training programmes, the model addresses the technical–legal divide identified in all four comparative jurisdictions, fostering the compliance-oriented institutional behaviour that preventive governance theory identifies as central to effective cybercrime prevention. Third, enhanced institutional resilience: by facilitating sustained interdisciplinary collaboration and continuous knowledge adaptation, the model builds the regulatory learning capacity necessary to respond to the rapid technological evolution of cybercrime threats. Fourth, reinforced fundamental rights compliance: by embedding Charter jurisprudence and CJEU interpretative standards within training curricula, the model strengthens the normative accountability of cybercrime governance — addressing the democratic legitimacy concern that Harcourt's critique of preventive governance raises.[86]

Journal of Political Science, Law & Governance
ISSN: 3059-8303, Volume – 2, Issue – 2, 2026
DOI: https://doi.org/10.63456/jpslg-2-2-109

7. CONCLUSION: EPISTEMIC GOVERNANCE AND THE FUTURE OF EU DIGITAL REGULATION

7.1 FROM ENFORCEMENT-CENTRIC TO PREVENTIVE EPISTEMIC GOVERNANCE

This article has advanced, developed, and defended the proposition that legal education should be reconceptualised as a foundational regulatory infrastructure within European Union cybercrime governance. The argument has been developed across four interconnected analytical registers. Theoretically, the article has integrated preventive governance scholarship, regulatory pluralism theory, co-creation governance models, and constitutional constraint analysis to construct a novel interdisciplinary framework for understanding EU cybercrime governance. Doctrinally, it has demonstrated that existing EU legal instruments — Directive 2013/40/EU, NIS2, and the GDPR — each exhibit structural training deficiencies that legislative harmonisation alone cannot remedy. Comparatively, it has provided critically evaluated evidence from four Member State jurisdictions that validates the theoretical propositions about epistemic governance deficits and their governance consequences. Normatively, it has proposed an institutionally detailed co-created legal education model that is theoretically grounded, empirically informed, constitutionally compliant, and practically implementable.

The CJEU's jurisprudential trajectory provides implicit but powerful endorsement of this analytical framework. *Digital Rights Ireland*[87] established that digital security measures must be balanced against fundamental rights through sophisticated legal reasoning. *Schrems II*[88] reinforced that transnational digital governance depends upon institutional safeguards requiring interpretative competence. *Tele2 Sverige*[89] extended proportionality requirements to cybersecurity data retention, placing interpretative demands upon regulatory actors that legal education must address. *H.K. v Prokuratuur*[90] further extended these requirements to law enforcement access to communications data in cybercrime investigations. Taken together, this jurisprudential trajectory implicitly recognises that effective EU digital governance is constitutively dependent upon coordinated legal literacy — precisely the governance infrastructure that this article's normative model is designed to develop.

7.2 STRUCTURAL CONSTRAINTS AND REALISTIC GOVERNANCE AMBITION

The article has been consistently attentive to two categories of structural constraint that temper but do not undermine its normative ambitions. First, the constitutional constraint of Article 165(4) TFEU is real and consequential: the proposed model does not circumvent it but operates through constitutionally appropriate channels — soft-law coordination, financial programming, and the Open Method of Coordination. This constitutional grounding is not a concession to political pragmatism but an expression of the model's analytical integrity. Second, the article explicitly acknowledges that harmonised legal education cannot alone resolve deep-rooted structural divergences arising from constitutional traditions, prosecutorial cultures, resource asymmetries, and differing conceptions of the privacy–security balance across Member States.[91] The model advances legal education as a necessary and systematically neglected regulatory lever, not as a governance panacea.

Herlin-Karnell's analysis of the constitutional dimension of European criminal law[92] and Baker's examination of how prosecutorial cultures resist supranational harmonisation[93] both underscore that the governance challenges confronting EU cybercrime regulation are deeply embedded in constitutional and institutional structures that transcend educational intervention. The normative model is designed to work with these structural constraints — respecting national constitutional autonomy while creating meaningful incentive structures for epistemic convergence — rather than against them.

7.3 IMPLICATIONS FOR EU CYBERCRIME GOVERNANCE AND DIGITAL REGULATORY HARMONISATION

The reconceptualisation of legal education as regulatory infrastructure carries profound implications for EU cybercrime governance. It addresses structural enforcement asymmetries arising from divergent national training standards, fostering the interpretative convergence and compliance culture that legislative harmonisation alone cannot achieve. It strengthens mutual trust mechanisms through the development of shared institutional standards and normative competencies among enforcement authorities. It enhances regulatory adaptability by providing the continuous knowledge adaptation infrastructure that the technological dynamism of cybercrime demands. And it reinforces democratic accountability by embedding Charter jurisprudence and rights-based compliance standards at the centre of regulatory training design. At the EU level, harmonised co-created legal education governance supports the Digital Single Market by strengthening cybersecurity compliance among cross-border digital service providers and critical infrastructure operators.[94]

Globally, the proposed reconceptualisation contributes to transnational governance scholarship by demonstrating how legal education can function as a soft-law harmonisation mechanism within complex regulatory pluralist environments. The EU's development of co-created legal education frameworks within the constitutional constraints of Article 165 TFEU could serve as a normative governance model for international cybercrime regulatory cooperation — potentially informing the implementation of the Budapest Convention's Second Additional Protocol on Enhanced Co-operation and Disclosure of Electronic Evidence at the international level.[95]

7.4 FUTURE RESEARCH DIRECTIONS

This article opens several avenues for future research. First, empirical longitudinal studies should develop methodologies for establishing causal relationships between educational governance quality and enforcement consistency — moving beyond the suggestive correlation evidence available in existing ENISA and EJTN assessments. Second, the comparative analysis should be extended to Eastern European, Southern European, and Nordic Member States.[96] Third, the model's applicability beyond the EU — particularly in the context of Budapest Convention implementation and international cybercrime governance cooperation — merits systematic exploration. Fourth, the integration of artificial intelligence and machine learning tools into cybercrime investigation and prosecution creates new interpretative challenges that co-created legal education frameworks must be designed to address. The development of harmonised epistemic governance infrastructures represents a critical frontier in EU digital governance scholarship, offering significant opportunities for advancing regulatory innovation, institutional legitimacy, and societal resilience in an increasingly digitalised global governance environment.

TABLE OF CASES

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources EU:C:2014:238
2. Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II) EU:C:2020:559
3. Case C-362/14 Maximillian Schrems v Data Protection Commissioner (Schrems I) EU:C:2015:650
4. Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson and Others EU:C:2016:970
5. Case C-216/18 PPU Minister for Justice and Equality v LM EU:C:2018:586
6. Case C-220/18 PPU Generalstaatsanwaltschaft (Conditions of Detention in Hungary) EU:C:2018:589
7. Joined Cases C-404/15 and C-659/15 PPU Aranyosi and Căldăraru EU:C:2016:198
8. Case C-131/12 Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González EU:C: 2014:317
9. Case C-286/12 Commission v Hungary EU:C: 2012:687
10. Case C-490/10 Parliament v Council EU:C:2012:525
11. Case C-42/17 Criminal Proceedings against M.A.S. and M.B. (Taricco II) EU:C:2017:936
12. Case C-105/14 Criminal Proceedings against Ivo Taricco and Others EU:C:2015:555
13. Case C-746/18 H.K. v Prokuratuur EU:C:2021:152
14. Case C-623/17 Privacy International v Secretary of State for Foreign and Commonwealth Affairs EU:C:2020:790
15. Case C-507/17 Google Inc v Commission Nationale de l'Informatique et des Libertés (CNIL) EU:C:2019:772
16. Case C-237/15 PPU Francis Lanigan EU:C:2015:474

REFERENCES

1. PRIMARY SOURCES: EU LEGISLATION, TREATIES AND DOCUMENTS

[1] Charter of Fundamental Rights of the European Union [2012] OJ C326/391. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT
[2] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures between Member States [2002] OJ L190/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002F0584
[3] Council of Europe, Convention on Cybercrime (Budapest Convention) ETS 185 (Budapest, 23 November 2001). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
[4] Council of Europe, Second Additional Protocol to the Budapest Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence CETS 224 (Strasbourg, 12 May 2022). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224
[5] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems [2013] OJ L218/8. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040
[6] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the European Investigation Order in Criminal Matters [2014] OJ L130/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0041
[7] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (NIS1 Directive) [2016] OJ L194/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

[8] 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 (NIS2 Directive) [2022] OJ L333/80. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555
[9] European Commission, Evaluation of Directive 2013/40/EU COM(2018) 448 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0448
[10] European Commission, EU Cybersecurity Strategy for the Digital Decade JOIN(2020) 18 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018
[11] European Commission, EU Security Union Strategy COM(2020) 605 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605
[12] European Commission, Digital Education Action Plan 2021–2027 COM(2020) 624 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0624
[13] European Commission, 'Shaping Europe's Digital Future' COM(2020) 67 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0067
[14] European Council, Presidency Conclusions, Tampere European Council 15–16 October 1999. https://www.europarl.europa.eu/summits/tam_en.htm
[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR) [2016] OJ L119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[16] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol Regulation) [2016] OJ L135/53. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0794
[17] Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust Regulation) [2018] OJ L295/138. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1727
[18] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on Information and Communications Technology Cybersecurity Certification (Cybersecurity Act) [2019] OJ L151/15. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881
[19] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme [2021] OJ L166/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0694
[20] Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing the Framework Programme for Research and Innovation — Horizon Europe [2021] OJ L170/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0695
[21] Regulation (EU) 2021/1057 of the European Parliament and of the Council of 24 June 2021 establishing the European Social Fund Plus [2021] OJ L231/21. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1057
[22] Treaty on European Union [2012] OJ C326/13. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012M%2FTXT
[23] Treaty on the Functioning of the European Union [2012] OJ C326/47. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E%2FTXT

2. INSTITUTIONAL AND POLICY DOCUMENTS

[1] Bundeskriminalamt, *Cybercrime Training Programme Report* (BKA 2022). https://www.bka.de/EN/OurTasks/Cybercrime/cybercrime_node.html
[2] Dutch National Cyber Security Centre, *Cybersecurity Education Framework* (NCSC-NL 2022). https://www.ncsc.nl/english
[3] ENISA, *Cybersecurity Training Framework* (Publications Office of the EU 2022). https://www.enisa.europa.eu/publications/enisa-training-framework
[4] ENISA, *Cybersecurity Skills Development in the EU: The Certification of Cybersecurity Degrees and ENISA's Higher Education Database* (Publications Office of the EU 2023). https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[5] ENISA, *NIS Investment Report 2022* (Publications Office of the EU 2022). https://www.enisa.europa.eu/publications/nis-investments-2022
[6] Estonian Judicial Training Centre, *Cybercrime Training Curriculum* (EJTC 2021). https://www.kohus.ee/en/courts/judicial-training-centre
[7] European Data Protection Board, *Annual Report 2022* (Publications Office of the EU 2022). https://www.edpb.europa.eu/our-work-tools/our-documents/annual-report/annual-report-2022_en
[8] European Judicial Training Network, *Cybercrime Training Comparative Study* (EJTN 2021). https://www.ejtn.eu/Training/Training-offers/
[9] European Judicial Training Network, *Cybercrime Training Report 2021* (EJTN 2021). https://www.ejtn.eu/Training/Training-offers/

[10] European Judicial Training Network, *EU Judicial Training Strategy 2021–2027* (EJTN 2021). https://www.ejtn.eu/Training/Training-offers/
[11] Eurojust, *Annual Report 2022* (Eurojust 2022). https://www.eurojust.europa.eu/publications/annual-reports
[12] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023* (Publications Office of the EU 2023). DOI: https://doi.org/10.2813/587536
[13] Federal Office for Information Security (BSI), *Cybersecurity Awareness Strategy* (BSI 2021). https://www.bsi.bund.de/EN/TheBSI/bsi_node.html
[14] Government of Spain, *National Cybersecurity Strategy 2019* (Departamento de Seguridad Nacional 2019). https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-nacional-ciberseguridad-2019
[15] INCIBE, *Cybersecurity Education Impact Report 2022* (INCIBE 2022). https://www.incibe.es/en
[16] Netherlands Ministry of Justice, *Cybercrime Governance Evaluation* (Ministerie van Justitie en Veiligheid 2023). https://www.government.nl/ministries/ministry-of-justice-and-security
[17] Spanish Ministry of Justice, *Judicial Cybercrime Training Programme* (Ministerio de Justicia 2022). https://www.mjusticia.gob.es/es/AreaTematica/FormacionJuridica

3. BOOKS AND BOOK CHAPTERS

[1] Ashworth A and Zedner L, *Preventive Justice* (Oxford University Press 2014). https://scholar.google.com/scholar?q=Ashworth+Zedner+Preventive+Justice+2014
[2] Beck U, *Risk Society: Towards a New Modernity* (Sage 1992). https://scholar.google.com/scholar?q=Beck+Risk+Society+New+Modernity+1992
[3] Bekkers V, Edelenbos J and Steijn B (eds), *Innovation in the Public Sector: Linking Capacity and Leadership* (Palgrave Macmillan 2011). https://scholar.google.com/scholar?q=Bekkers+Edelenbos+Steijn+Innovation+Public+Sector+2011
[4] Berman P S, *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders* (Cambridge University Press 2012). https://scholar.google.com/scholar?q=Berman+Global+Legal+Pluralism+2012
[5] Boehm F, *Information Sharing in the Area of Freedom, Security and Justice* (Cambridge University Press 2012). https://scholar.google.com/scholar?q=Boehm+Information+Sharing+Freedom+Security+Justice+2012
[6] Giddens A, *The Consequences of Modernity* (Polity Press 1990). https://scholar.google.com/scholar?q=Giddens+Consequences+Modernity+1990
[7] Harcourt B, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (University of Chicago Press 2007). https://scholar.google.com/scholar?q=Harcourt+Against+Prediction+2007
[8] Herlin-Karnell E, *The Constitutional Dimension of European Criminal Law* (Hart Publishing 2012). https://scholar.google.com/scholar?q=Herlin-Karnell+Constitutional+Dimension+European+Criminal+Law+2012
[9] Hooghe L and Marks G, *Multi-Level Governance and European Integration* (Rowman & Littlefield 2001). https://scholar.google.com/scholar?q=Hooghe+Marks+Multi-Level+Governance+European+Integration+2001
[10] Krisch N, *Beyond Constitutionalism: The Pluralist Structure of Postnational Law* (Oxford University Press 2010). https://scholar.google.com/scholar?q=Krisch+Beyond+Constitutionalism+Pluralist+Postnational+Law+2010
[11] Millard C (ed), *Cloud Computing Law* (2nd edn, Oxford University Press 2021). https://scholar.google.com/scholar?q=Millard+Cloud+Computing+Law+2021
[12] Mitsilegas V, *EU Criminal Law after Lisbon: Rights, Trust and the Transformation of Justice in Europe* (Hart Publishing 2016). https://scholar.google.com/scholar?q=Mitsilegas+EU+Criminal+Law+after+Lisbon+2016
[13] Morgan B and Yeung K, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press 2007). https://scholar.google.com/scholar?q=Morgan+Yeung+Introduction+Law+Regulation+2007
[14] Ostrom E, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge University Press 1990). https://scholar.google.com/scholar?q=Ostrom+Governing+Commons+1990
[15] Sieber U, 'Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study' (Council of Europe 2001). https://ccdcoe.org/uploads/2018/10/Sieber-1998_Legal-Aspects-of-Computer-Related-Crime-in-the-Information-Society.pdf
[16] Slaughter A-M, *A New World Order* (Princeton University Press 2004). https://scholar.google.com/scholar?q=Slaughter+New+World+Order+Princeton+2004
[17] Tikk E, *International Cyber Incidents: Legal Considerations* (NATO CCDCOE 2010). https://ccdcoe.org/library/publications/international-cyber-incidents-legal-considerations/
[18] Walker N, *Intimations of Global Law* (Cambridge University Press 2015). https://scholar.google.com/scholar?q=Walker+Intimations+Global+Law+Cambridge+2015
[19] Zeitlin J and Pochet P (eds), *The Open Method of Co-ordination in Action: The European Employment and Social Inclusion Strategies* (PIE Peter Lang 2005). https://scholar.google.com/scholar?q=Zeitlin+Pochet+Open+Method+Coordination+2005

4. JOURNAL ARTICLES

[1] Baker E, 'Governing through Crime — the Case of the European Union' (2010) 7 *European Journal of Criminology* 187. DOI: https://doi.org/10.1177/1477370810362836
[2] Black J, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (2001) 54 *Current Legal Problems* 103. DOI: https://doi.org/10.1093/clp/54.1.103
[3] Black J and Baldwin R, 'Really Responsive Regulation' (2008) 71 *Modern Law Review* 59. DOI: https://doi.org/10.1111/j.1468-2230.2008.00681.x
[4] Carrapico H and Trauner F, 'Europol and its Impact on EU Policymaking on Organised Crime: Analysing Governance Dynamics and Opportunities' (2013) 14 *Perspectives on European Politics and Society* 357. DOI: https://doi.org/10.1080/15705854.2013.817804
[5] Davies G, 'Subsidiarity: The Wrong Idea, in the Wrong Place, at the Wrong Time' (2006) 43 *Common Market Law Review* 63. https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/43.1/COLA2005083
[6] De Hert P and Papakonstantinou V, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 *Computer Law & Security Review* 179. DOI: https://doi.org/10.1016/j.clsr.2016.02.006
[7] Gherghina S and Mişcoiu S, 'The Failure of Coercive Europeanisation: The Roma Policy in the Czech Republic and Romania' (2013) 26 *Journal of Contemporary European Studies* 417. DOI: https://doi.org/10.1080/14782804.2013.849281
[8] Haas P, 'Introduction: Epistemic Communities and International Policy Coordination' (1992) 46 *International Organisation* 1. DOI: https://doi.org/10.1017/S0020818300001442
[9] Holzinger K and Knill C, 'Causes and Conditions of Cross-National Policy Convergence' (2005) 12 *Journal of European Public Policy* 775. DOI: https://doi.org/10.1080/13501760500161357
[10] Sedelmeier U, 'Europeanisation in New Member and Candidate States' (2011) 6 *Living Reviews in European Governance* 1. DOI: https://doi.org/10.12942/lreg-2011-1
[11] Thatcher M and Stone Sweet A, 'Theory and Practice of Delegation to Non-Majoritarian Institutions' (2002) 25 *West European Politics* 1. DOI: https://doi.org/10.1080/713601583
[12] Tikk E and Minárik T, 'The 2007 Cyber Attacks against Estonia: International Law Aspects' (2014) 13 *Baltic Yearbook of International Law* 163. https://scholar.google.com/scholar?q=Tikk+Minarik+2007+Cyber+Attacks+Estonia+Baltic+Yearbook
[13] Trauner F and Clifton J, 'A New Intergovernmentalism in Practice? EU Justice and Home Affairs in the Post-Lisbon Era' (2016) 9 *Journal of Common Market Studies* 54. DOI: https://doi.org/10.1111/jcms.12348
[14] Zedner L, 'Pre-Crime and Post-Criminology?' (2007) 11 *Theoretical Criminology* 261. DOI: https://doi.org/10.1177/1362480607075851

FOOTNOTES

[1] European Commission, EU Security Union Strategy COM(2020) 605 final; European Commission, 'Shaping Europe's Digital Future' COM(2020) 67 final.
[2] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems [2013] OJ L218/8; 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 (NIS2 Directive) [2022] OJ L333/80.
[3] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources EU:C:2014:238, paras 41–54.
[4] Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II) EU:C:2020:559, paras 94–105.
[5] V Mitsilegas, EU Criminal Law after Lisbon: Rights, Trust and the Transformation of Justice in Europe (Hart Publishing 2016) chs 2–3; E Baker, 'Governing through Crime — the Case of the European Union' (2010) 7 European Journal of Criminology 187, 190–95.
[6] Treaty on European Union [2012] OJ C326/13, Art 5(3); Treaty on the Functioning of the European Union [2012] OJ C326/47, Arts 165(1), (4).
[7] U Sieber, 'Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study' (Council of Europe 2001) 14–19.
[8] H Carrapico and F Trauner, 'Europol and its Impact on EU Policymaking on Organised Crime: Analysing Governance Dynamics and Opportunities' (2013) 14 Perspectives on European Politics and Society 357, 362–65; F Trauner and J Clifton, 'A New Intergovernmentalism in Practice? EU Justice and Home Affairs in the Post-Lisbon Era' (2016) 9 Journal of Common Market Studies 54.
[9] Mitsilegas (n 5) 89–97, 134–41.
[10] NIS2 Directive (n 2); Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (NIS1 Directive) [2016] OJ L194/1.

[11] J Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (2001) 54 Current Legal Problems 103, 113–17.
[12] J Black and R Baldwin, 'Really Responsive Regulation' (2008) 71 Modern Law Review 59, 61–63.
[13] A-M Slaughter, A New World Order (Princeton University Press 2004) 36–44, 168–72.
[14] N Walker, Intimations of Global Law (Cambridge University Press 2015) 12–15, 89–97; P S Berman, Global Legal Pluralism: A Jurisprudence of Law Beyond Borders (Cambridge University Press 2012) 3–8.
[15] European Council, Presidency Conclusions, Tampere European Council 15–16 October 1999, para 33; Mitsilegas (n 5) 97–108.
[16] Case C-216/18 PPU Minister for Justice and Equality v LM EU:C:2018:586, paras 48–68.
[17] ENISA, Cybersecurity Skills Development in the EU (Publications Office of the EU 2023) 41–43; European Judicial Training Network, EU Judicial Training Strategy 2021–2027 (EJTN 2021) 22–25.
[18] U Beck, Risk Society: Towards a New Modernity (Sage 1992) 19–23; A Giddens, The Consequences of Modernity (Polity Press 1990) 124–27.
[19] L Zedner, 'Pre-Crime and Post-Criminology?' (2007) 11 Theoretical Criminology 261, 265–70.
[20] A Ashworth and L Zedner, Preventive Justice (Oxford University Press 2014) ch 1.
[21] Case C-746/18 H K v Prokuratuur EU:C:2021:152, paras 48–60.
[22] B Harcourt, Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age (University of Chicago Press 2007) ch 7.
[23] Walker (n 14) 89–97; N Krisch, Beyond Constitutionalism: The Pluralist Structure of Postnational Law (Oxford University Press 2010) ch 2.
[24] Council of Europe, Convention on Cybercrime (Budapest Convention) ETS 185 (Budapest, 23 November 2001); Council of Europe, Second Additional Protocol to the Budapest Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence CETS 224 (Strasbourg, 12 May 2022).
[25] Tampere European Council (n 15) para 33.
[26] LM (n 16) paras 48–68.
[27] Joined Cases C-404/15 and C-659/15 PPU Aranyosi and Căldăraru EU:C:2016:198, paras 83–104; Case C-237/15 PPU Francis Lanigan EU:C:2015:474, paras 36–47.
[28] E Ostrom, Governing the Commons: The Evolution of Institutions for Collective Action (Cambridge University Press 1990) 88–102; V Bekkers, J Edelenbos and B Steijn (eds), Innovation in the Public Sector: Linking Capacity and Leadership (Palgrave Macmillan 2011) ch 1.
[29] Black (n 11) 142–46.
[30] Slaughter (n 13) 168–72; P Haas, 'Introduction: Epistemic Communities and International Policy Coordination' (1992) 46 International Organisation 1, 3–6.
[31] European Commission, Digital Education Action Plan 2021–2027 COM(2020) 624 final, 8–11.
[32] ENISA, Cybersecurity Training Framework (Publications Office of the EU 2022) 14–18.
[33] TFEU (n 6) Art 165(4); Case C-490/10 Parliament v Council EU:C:2012:525, para 83.
[34] J Zeitlin and P Pochet (eds), The Open Method of Co-ordination in Action: The European Employment and Social Inclusion Strategies (PIE Peter Lang 2005) ch 1; G Davies, 'Subsidiarity: The Wrong Idea, in the Wrong Place, at the Wrong Time' (2006) 43 Common Market Law Review 63, 74.
[35] Davies (n 34) 74–78.
[36] Directive 2013/40/EU (n 2) recitals 1–6, Arts 1–12.
[37] Budapest Convention (n 24); Second Additional Protocol (n 24).
[38] TFEU (n 6) Art 83(1).
[39] Case C-42/17 Criminal Proceedings against M A S and M B (Taricco II) EU:C:2017:936, paras 51–58; Case C-105/14 Criminal Proceedings against Ivo Taricco and Others EU:C:2015:555, paras 37–58.
[40] Directive 2013/40/EU (n 2) Art 12; European Commission, Evaluation of Directive 2013/40/EU COM(2018) 448 final, 27–30.
[41] European Commission, Evaluation of Directive 2013/40/EU COM(2018) 448 final, 22–31; ENISA (n 17) 38.
[42] NIS2 Directive (n 2); C Millard (ed), Cloud Computing Law (2nd edn, Oxford University Press 2021) ch 12.
[43] NIS2 Directive (n 2) Art 20(1)–(2); recitals 80–84.
[44] Schrems II (n 4) paras 94–105.
[45] ENISA (n 17) 41–45; ENISA, NIS Investment Report 2022 (Publications Office of the EU 2022) 24–28.
[46] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR) [2016] OJ L119/1.
[47] European Data Protection Board, Annual Report 2022 (Publications Office of the EU 2022) 14–18; GDPR (n 46) Art 68.
[48] P De Hert and V Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179, 186–89; F Boehm, Information Sharing in the Area of Freedom, Security and Justice (Cambridge University Press 2012) ch 3.
[49] Case C-131/12 Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González EU:C:2014:317, paras 80–99.

[50] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023 (Europol 2023) 8–12; Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol Regulation) [2016] OJ L135/53.
[51] Eurojust, Annual Report 2022 (Eurojust 2022) 22–26; Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust Regulation) [2018] OJ L295/138.
[52] European Judicial Training Network, Cybercrime Training Report 2021 (EJTN 2021) 8–12.
[53] European Commission, Digital Education Action Plan (n 31) 12–15.
[54] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures between Member States [2002] OJ L190/1; Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 on the European Investigation Order in Criminal Matters [2014] OJ L130/1.
[55] Mitsilegas (n 5) 89–97.
[56] Aranyosi and Căldăraru (n 27) paras 83–104.
[57] LM (n 16) paras 48–68.
[58] Black (n 11) 113; B Morgan and K Yeung, An Introduction to Law and Regulation: Text and Materials (Cambridge University Press 2007) ch 3.
[59] U Sedelmeier, 'Europeanisation in New Member and Candidate States' (2011) 6 Living Reviews in European Governance 1, 8–12.
[60] Government of Spain, National Cybersecurity Strategy 2019 (Departamento de Seguridad Nacional 2019) 33–37.
[61] Spanish Ministry of Justice, Judicial Cybercrime Training Programme (Ministerio de Justicia 2022) 7–11.
[62] Schrems II (n 4); Digital Rights Ireland (n 3).
[63] INCIBE, Cybersecurity Education Impact Report 2022 (INCIBE 2022) 11–13.
[64] E Tikk, International Cyber Incidents: Legal Considerations (NATO CCDCOE 2010) 14–18; E Tikk and T Minárik, 'The 2007 Cyber Attacks against Estonia: International Law Aspects' (2014) 13 Baltic Yearbook of International Law 163.
[65] Estonian Judicial Training Centre, Cybercrime Training Curriculum (EJTC 2021) 6–10.
[66] ENISA (n 17) 44.
[67] Bundeskriminalamt, Cybercrime Training Programme Report (BKA 2022) 9–13.
[68] Federal Office for Information Security (BSI), Cybersecurity Awareness Strategy (BSI 2021) 14–17.
[69] European Judicial Training Network, Cybercrime Training Comparative Study (EJTN 2021) 18–23.
[70] Dutch National Cyber Security Centre, Cybersecurity Education Framework (NCSC-NL 2022) 8–11.
[71] Netherlands Ministry of Justice, Cybercrime Governance Evaluation (Ministerie van Justitie en Veiligheid 2023) 21–25.
[72] European Commission, EU Cybersecurity Strategy for the Digital Decade JOIN(2020) 18 final, 18–20.
[73] Sedelmeier (n 59) 8–12; S Gherghina and S Mișcoiu, 'The Failure of Coercive Europeanisation: The Roma Policy in the Czech Republic and Romania' (2013) 26 Journal of Contemporary European Studies 417.
[74] Budapest Convention (n 24); Second Additional Protocol (n 24).
[75] TFEU (n 6) Art 165(4); Parliament v Council (n 33) para 83; Zeitlin and Pochet (n 34) ch 1.
[76] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme [2021] OJ L166/1; Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing the Framework Programme for Research and Innovation — Horizon Europe [2021] OJ L170/1; Regulation (EU) 2021/1057 of the European Parliament and of the Council of 24 June 2021 establishing the European Social Fund Plus [2021] OJ L231/21; L Hooghe and G Marks, Multi-Level Governance and European Integration (Rowman & Littlefield 2001) 78–84.
[77] Zeitlin and Pochet (n 34) ch 1; M Thatcher and A Stone Sweet, 'Theory and Practice of Delegation to Non-Majoritarian Institutions' (2002) 25 West European Politics 1, 11–15.
[78] Netherlands Ministry of Justice (n 71) 21–25.
[79] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, Arts 7, 8, 47, 48.
[80] Thatcher and Stone Sweet (n 77) 17–21; Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on Information and Communications Technology Cybersecurity Certification (Cybersecurity Act) [2019] OJ L151/15, Art 20.
[81] Slaughter (n 13) 168–72.
[82] Haas (n 30) 3–6.
[83] K Holzinger and C Knill, 'Causes and Conditions of Cross-National Policy Convergence' (2005) 12 Journal of European Public Policy 775, 783.
[84] NIS2 Directive (n 2) Arts 20–21.
[85] European Commission, Digital Education Action Plan (n 31) 12–15.
[86] Harcourt (n 22) ch 7; Charter (n 79) Arts 47–48.
[87] Digital Rights Ireland (n 3) paras 47–54.
[88] Schrems II (n 4) paras 94–105.
[89] Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson and Others EU:C:2016:970, paras 115–25.

[90] H K v Prokuratuur (n 21) paras 48–60.
[91] Mitsilegas (n 5) chs 2–3; Baker (n 5) 190–95.
[92] E Herlin-Karnell, The Constitutional Dimension of European Criminal Law (Hart Publishing 2012) 88–95.
[93] Baker (n 5) 190–95.
[94] European Commission, EU Cybersecurity Strategy (n 72) 2–4.
[95] Budapest Convention (n 24); Second Additional Protocol (n 24).
[96] Sedelmeier (n 59) 8–12.
[97] Case C-623/17 Privacy International v Secretary of State for Foreign and Commonwealth Affairs EU:C:2020:790, paras 64–82.
[98] Case C-507/17 Google Inc v Commission Nationale de l'Informatique et des Libertés (CNIL) EU:C:2019:772, paras 44–60.