European Journal of Risk Regulation (2026), **17**, 312–328
doi:10.1017/err.2025.10060

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Rethinking Cybersecurity Research Governance: Lessons from the Act on Digital Services?

Michal Rampášek and Matúš Mesarčík

Faculty of Law, Institute of Information Technology Law and Intellectual Property Law, Comenius University Bratislava, Bratislava, Slovakia
Corresponding author: Matúš Mesarčík; Email: matus.mesarcik@flaw.uniba.sk

Abstract

EU law lacks a coherent legal framework that adequately defines, protects, and empowers cybersecurity researchers, particularly those operating outside formal institutions. This paper examines how cybersecurity research fits within the evolving EU regulatory landscape, with a particular focus on the Digital Services Act (DSA), the Cyber Resilience Act (CRA), and the NIS2 Directive. It explores the legal ambiguity surrounding researcher status, the conditions for data access and auditing under the DSA, and the challenges posed by current vetting requirements. Drawing on doctrinal legal analysis and interdisciplinary insights from cybersecurity and platform governance, the paper argues that while the DSA provides novel tools such as vetted researcher access and auditing obligations for Very Large Online Platforms (VLOPs) its structure is better suited for systemic risk research than for adversarial, exploratory cybersecurity testing. The paper concludes that a sustainable model for cybersecurity research governance in the EU must go beyond DSA-style vetting, incorporating flexible mechanisms like coordinated vulnerability disclosure and bug bounty programs, as reflected more directly in the CRA.

Keywords: Cybersecurity research; Data access; Digital Services Act

I. Introduction

In the digital ecosystem governed by the Digital Services Act (DSA),[1] cybersecurity research has become indispensable for ensuring compliance, particularly for online platforms including Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). Major online platforms operate highly complex, interconnected systems that rely heavily on machine learning pipelines, recommender engines and complex software infrastructure, often built using third-party Machine Learning Operations (MLOps) platforms and open-source AI tools. Independent and academic security researchers have repeatedly demonstrated that these dependencies introduce severe vulnerabilities, ranging from hidden undocumented APIs in super apps like TikTok or WeChat discovered by U.S. university researchers,[2] to exploitable flaws in deep learning frameworks such as TensorFlow and PyTorch, as shown in recent Australian empirical study.[3]

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1.

[2] C Wang, Y Zhang and Z Lin, "Uncovering and exploiting hidden APIs in mobile super apps" in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (ACM 2023) <https://arxiv.org/pdf/2306.08134> (accessed 6 August 2025).

[3] Z Lai and others, "On security weaknesses and vulnerabilities in deep learning systems" (2024) IEEE Transactions on Dependable and Secure Computing. https://arxiv.org/abs/2406.08688 (accessed 6 August 2025).

© The Author(s), 2025. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

Concrete examples illustrate the critical role of vulnerability disclosure and independent security research. Over twenty critical supply chain vulnerabilities in widely used MLOps platforms were recently uncovered by independent teams, showing the susceptibility of AI infrastructure to exploitation.[4] Recent IBM research describes ways to abuse popular cloud-based and internally hosted platforms, including BigML, Azure Machine Learning, and Google Cloud Vertex AI. These findings are particularly relevant for enterprises relying on such platforms.[5] These findings directly impact online platforms relying on recommender systems,[6] moderation tools,[7] or fraud detection,[8] all powered via MLOps infrastructures,[9] being at risk from model poisoning, data leakage (extraction), and unauthorised access or manipulation of deployed models. Without the work of external researchers, many of these risks would remain undetected, leaving platforms and their users exposed to systemic harm.

These cases reflect that cybersecurity is increasingly dependent on the active participation of independent researchers to identify vulnerabilities, test the resilience of systems, and highlight risks before they are exploited. Despite their key role in the protection of information systems, the position of cybersecurity researchers in the European Union's (EU) legal frameworks remains unclear, incoherent and often only implicitly assumed. Researchers operate at the intersection of academic and informal technical practice, with many identifying themselves as ethical hackers or experts involved in community-based or commercial forms of security research. This nature poses challenges in their legal definition and regulation in the EU.

In the context of increasing AI integration and cybersecurity concerns, regulating risks to citizens' health, safety, privacy, and the environment requires not only systemic oversight by digital platforms but also active engagement with the broader security research community. In times of uncertainty and societal contestation, such as during the rollout of disruptive AI systems or digital platforms (e.g., content moderation, deepfakes and synthetic content) regulators often turn to flexible, adaptive tools like regulatory sandboxes, public consultations, and soft law instruments (e.g., guidelines, codes of conduct). These mechanisms allow space for innovation while addressing public concerns and emerging harms. A growing trend is the integration of multi-stakeholder governance, including civil society, industry, and independent experts (such as cybersecurity researchers), to ensure more democratic, transparent, and responsive regulation across domains.[10]

[4] R Lakchmaan, "Researchers identify over 20 supply chain vulnerabilities in MLOps platforms" (*The Hacker News*, 24 August 2024) https://thehackernews.com/2024/08/researchers-identify-over-20-supply.html (accessed 6 August 2025).

[5] B Hawkins and C Thompson, "Disrupting the model: abusing MLOps platforms to compromise ML models and enterprise data lakes" (IBM X-Force Red, v 1.0, n.d.) <https://www.ibm.com/downloads/documents/us-en/11630e2cbc302316> (accessed 6 August 2025).

[6] See, e.g., A Saputra and others, "Secure and scalable LLM-based recommendation systems: an MLOps and security-by-design" in 2024 IEEE International Symposium on Consumer Technology (ISCT) (IEEE 2024) 623–629. https://doi.org/10.1109/ISCT62336.2024.10791207 (accessed 6 August 2025); P Narendra Patil, *Optimizing Movie Recommendations with MLOps in AWS* (Master's thesis, National College of Ireland 2024) <https://norma.ncirl.ie/8047/> (accessed 22 July 2025).

[7] P Winder, L Marsden and E Rotundo, "Automated content classification (ACC) systems: an investigation into how social media platforms use MLOps software, systems, and processes to manage user-generated content" (Winder.AI 2023) <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/other/acc-phase-2-report.pdf?v=329106> (accessed 22 July 2025).

[8] A Roy and others, "Deep learning detecting fraud in credit card transactions" in *Proceedings of the Systems and Information Engineering Design Symposium (SIEDS)* (IEEE April 2018) 129–134 https://doi.org/10.1109/SIEDS.2018.8374722 (accessed 6 August 2025).

[9] M Testi and others, "MLOps: a taxonomy and a methodology" (2022) 10 *IEEE Access* 63606–63618 https://doi.org/10.1109/ACCESS.2022.3181730 (accessed 6 August 2025).

[10] W Kleinwächter, "Cybersecurity, Internet governance, and the multistakeholder approach: the role of non-state actors in Internet policy making" (Cyberstability Paper Series: *New Conditions and Constellations in Cyber*, The

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

Cybersecurity research encompasses diverse dimensions, including technical vulnerability discovery, social implications, and evolving legal frameworks. One strand of literature explores rigorous research methodologies suited to the dynamic and adversarial cybersecurity landscape, covering empirical, observational, and applied approaches.[11] Another focuses on thematic priorities in cybersecurity innovation, such as artificial intelligence, complex systems, and biotechnology.[12] Ethical analysis highlights the lack of unified oversight mechanisms in both academic and corporate research practices.[13] Legal scholarship increasingly argues that cybersecurity research supports democratic values and should be protected as part of fundamental rights.[14] Finally, practitioner-oriented sources stress the importance of collaboration between researchers and system operators.[15] Role-definition frameworks outline the formal role with the skills and competences of cybersecurity researchers.[16]

The role of researchers has been particularly explored by the academic researchers under the DSA[17] generally[18] or under specific conditions.[19] Specific

Hague Centre for Strategic Studies and the Global Commission on the Stability of Cyberspace, December 2021) <https://hcss.nl/wp-content/uploads/2021/12/Kleinwaechter.pdf> (accessed 6 August 2025).

[11] TW Edgar and DO Manz, *Research Methods for Cyber Security* (Elsevier 2017) <www.sciencedirect.com/book/9780128053492/research-methods-for-cyber-security#book-description> (accessed 6 August 2025).

[12] European Union Agency for Cybersecurity (ENISA), "Research and Innovation Brief: Annual report on cybersecurity research and innovation needs and priorities" (May 2022) <www.enisa.europa.eu/sites/default/files/publications/RIT%20Annual%20Report%202021.pdf> (accessed 6 August 2025); ENISA, "Artificial intelligence and cybersecurity research" (June 2023) <www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research> (accessed 6 August 2025).

[13] K Macnish and J van der Ham, "Ethics in cybersecurity research and practice" (2020) 63 Technology in Society 101382 https://doi.org/10.1016/j.techsoc.2020.101382 accessed 6 August 2025.

M Christen, B Gordijn and M Loi (eds), *The Ethics of Cybersecurity* (Springer 2020) https://doi.org/10.1007/978-3-030-29053-5_4 (accessed 6 August 2025).

[14] O van Daalen, "In defence of offence: information security research under the right to science" (2022) 46 Computer Law & Security Review 105706 https://doi.org/10.1016/j.clsr.2022.105706 (accessed 6 August 2025).

[15] T Beardsley and D Larson, "Engaging with security researchers: embracing a 'see something, say something' culture" (CISA, 23 October 2024) <www.cisa.gov/news-events/news/engaging-security-researchers-embracing-see-something-say-something-culture> (accessed 6 August 2025).

[16] European Union Agency for Cybersecurity (ENISA), "European Cybersecurity Skills Framework (ECSF)" (September 2022) <www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20Role%20Profiles.pdf> (accessed 6 August 2025).

[17] M Husovec, "How to facilitate data access under the Digital Services Act" (19 May 2023) https://ssrn.com/abstract=4452940 (accessed 22 July 2025); A Liesenfeld, "The legal significance of independent research based on Article 40 DSA for the management of systemic risks in the Digital Services Act" (2025) 16(1) European Journal of Risk Regulation 184–96 https://doi.org/10.1017/err.2024.61 (accessed 22 July 2025); J Jaursch, "Researcher access to platform data under the DSA: questions and answers" (Stiftung Neue Verantwortung/Max-Planck-Institut für Bildungsforschung, 28 July 2023) https://reclaimingautonomyonline.notion.site/Researcher-access-to-platform-data-under-the-DSA-Questions-and-answers-8f7390f3ae6b4aa7ad53d53158ed257c (accessed 22 July 2025); A Turillazzi and others, "The Digital Services Act: an analysis of its ethical, legal, and social implications" (2023) 15(1) Law, Innovation and Technology 83–106 https://doi.org/10.1080/17579961.2023.2184136 (accessed 22 July 2025).

[18] G Frosio and F Obafemi, "Augmented accountability: data access in the metaverse" https://doi.org/10.2139/ssrn.5246393 (accessed 22 July 2025).

[19] J Laux and others, "Taming the few: platform regulation, independent audits, and the risks of capture created by the DMA and DSA" (2021) 43 Computer Law & Security Review 105613 https://doi.org/10.1016/j.clsr.2021.105613 (accessed 22 July 2025); P Terzis and others, "Law and the emerging political economy of algorithmic audits" in *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (FAccT '24)* (ACM 2024) 1255–1267 https://doi.org/10.1145/3630106.3658970 (accessed 22 July 2025); A-K Meßmer and M Degeling, "Auditing recommender systems – putting the DSA into practice with a risk-scenario-based approach" (2023) *arXiv preprint* arXiv:2302.04556 https://doi.org/10.48550/arXiv.2302.04556 (accessed 22 July 2025); M-T Sekwenz, "Doing audits right? The role of sampling and legal content analysis in systemic risk assessments and independent

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

attention is paid to AI auditing ecosystems[20] and algorithmic auditing in the literature.[21]

The aim of this paper is to examine the legal status and role of cybersecurity researchers in light of current EU regulations. This paper contributes to the interdisciplinary risk governance discourse by analysing the regulatory treatment of cybersecurity research, a critical yet underexamined component of Europe's broader strategy for mitigating digital risks to privacy, public security and systemic societal resilience. It addresses how EU law conceptualises and integrates cybersecurity researchers into legal frameworks designed to manage the risks posed by digital infrastructures and platform ecosystems.

This paper employs a doctrinal and analytical legal methodology, supported by interdisciplinary references from cybersecurity studies and platform governance literature. It draws on primary legal sources, including EU legislation, delegated acts, and policy documents, complemented by academic commentary and case studies of researcher practices. Through a combined analysis of normative frameworks and institutional arrangements, the paper aims to identify interpretative challenges, regulatory gaps, and opportunities for integrating cybersecurity research into existing oversight mechanisms. The contribution of this paper lies in clarifying the fragmented legal positioning of cybersecurity researchers in EU law and in evaluating whether the DSA provides a workable model for their structured involvement in risk identification and mitigation.

In the first part, we address the question of who falls under the term cybersecurity researcher. We examine the extent to which current practice relies on academic or non-academic research, paying particular attention to informal and community-based forms of research, including ethical hacking. Subsequently, we examine the role of cybersecurity research through the lens of the relevant EU cybersecurity legislation, namely in the context of the NIS2 Directive (NIS2)[22] and the Cyber Resilience Act (CRA),[23] which recognises the importance of security researchers by requiring manufacturers to establish and maintain coordinated vulnerability disclosure (CVD) policies and procedures to process and remediate vulnerabilities reported from both internal and external sources.[24] In the second part, we analyse the emerging concept of the "vetted researcher" and general explorative research under the DSA and the Delegated Act on Data Access[25] to regulate the conditions for researchers' access to VLOPs and VLOSEs data. This model of researcher authentication is intended to ensure responsible access to sensitive data while

audits in the Digital Services Act" (2025) *arXiv preprint* arXiv:2505.03601 https://doi.org/10.48550/arXiv.2505.03601 (accessed 22 July 2025).

[20] D Hartmann, "Addressing the regulatory gap: moving towards an EU AI audit ecosystem beyond the AI Act by including civil society" (2025) 5(4) AI and Ethics 3617–38 https://doi.org/10.1007/s43681-024-00595-3 (accessed 22 July 2025).

[21] EP Goodman and J Trehu, "Algorithmic auditing: chasing AI accountability" (2023) 39(3) Santa Clara Computer and High Technology Law Journal 289–337.

[22] 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333/80.

[23] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [2024] OJ L (20 November 2024).

[24] Regulation (EU) 2024/2847 (Cyber Resilience Act), Art 13(8) and Annex I pt II(5).– Requires manufacturers to have appropriate procedures, including CVD policies, for handling vulnerability reports from internal or external sources.

[25] European Commission, *Draft Delegated Act on data access* C(2025) 4340 (2 July 2025), 'Commission Delegated Regulation (EU) .../... of 1.7.2025 supplementing Regulation (EU) 2022/2065 ...' https://digital-strategy.ec.europa.eu/en/library/delegated-act-data-access-under-digital-services-act-dsa (accessed 6 August 2025).

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

supporting external oversight of the platforms. Specific focus is also on the requirements for auditing of VLOPs and VLOSEs. The third part of the paper synthetises previous sections and offers our views on rethinking cybersecurity research under the EU legal landscape and whether the model provided by the DSA is suitable for cybersecurity researchers.

The paper therefore contributes to the debate on how cybersecurity research could be systematically and sustainably legally embedded in the regulatory frameworks of the EU. The aim is not only to identify gaps, but also to outline possible pathways towards the legal recognition and promotion of this type of research as an integral part of digital security in the EU.

II. Concept of Cybersecurity Research

Security researchers use their skills and knowledge to improve the cybersecurity resilience of products, services and information systems. They play a crucial role in strengthening cybersecurity resilience by identifying and reporting vulnerabilities in products, services and information systems.[26] Exposing vulnerabilities in good faith by researchers makes complex technologies more transparent and helps companies design safer products.[27] Cybersecurity research is inherently probing. Researchers simulate the actions of attackers, scanning for open ports, testing for injection vulnerabilities or attempting buffer overflows, etc. The value of this research lies precisely in its independence and unpredictability.

The reporter is often a security researcher, but any individual or organisation can act as a reporter.[28] Professional researchers can act independently or as part of an organisation. Some researchers are affiliated with universities or other academic institutions.[29] Research organisations and departments includes business sector, the government sector, the higher education sector (colleges, universities, etc.), as well as private non-profit sector.[30] An empirical study analyzing vulnerability reports from major Free/Libre and Open Source Software (FLOSS) projects, found that vulnerability reporting is highly concentrated among a small core of dedicated security researchers, though a wider group of occasional contributors also plays a meaningful role.

Academic cybersecurity research is a critical driver of foundational innovation, systematic vulnerability discovery and long-term resilience across digital ecosystems. Unlike corporate or product-focused research, academic inquiry often operates with greater methodological openness, longer time horizons and interdisciplinary collaboration, allowing researchers to investigate underlying assumptions in hardware design, cryptographic protocols and system architectures.

The discovery of Spectre and Meltdown in 2018, which revealed fundamental design flaws in modern processor architectures, was discovered by interdisciplinary academic teams from institutions such as Graz University of Technology, the University of

[26] J Alex Halderman, "Long comment regarding a proposed exemption under 17 USC §1201" (US Copyright Office, n.d.) 8 <www.acm.org/binaries/content/assets/public-policy/ustpc-jt-long-comment-copyright-ofc-dmca.pdf> (accessed 6 August 2025).

[27] JL Hall and others, "The importance of security research: four case studies" (Center for Democracy & Technology, 15 December 2017) <https://cdt.org/insights/the-importance-of-security-research-four-case-studies/> (accessed 6 August 2025).

[28] ISO/IEC 29147:2018, *Information technology – Security techniques – Vulnerability disclosure*.

[29] ISO/IEC 29147:2018, *Information technology – Security techniques – Vulnerability disclosure*, cl 5.5.4.

[30] OECD, *Frascati Manual 2015: Guidelines for collecting and reporting data on research and experimental development* (OECD Publishing 2015) https://doi.org/10.1787/9789264239012-en (accessed 7 August 2025).

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

Pennsylvania and the University of Maryland, demonstrated how interdisciplinary teams can uncover flaws not just in software, but in the very architecture of modern CPUs, forcing a global re-evaluation of hardware and operating system design.[31] In 2015, a collaboration between researchers at Johns Hopkins University, INRIA and the University of Michigan exposed the Logjam attack[32] Similarly, the DROWN attack, disclosed in 2016 by researchers from institutions including the University of Münster, Ruhr-University Bochum and the University of Michigan. Both cases showcased how cryptographic weaknesses identified by university-led collaborations prompted industry-wide shifts in TLS configurations and security standards.[33]

In addition to academic cybersecurity research, non-academic researchers, whether affiliated with private initiatives or operating independently, play a vital role in the discovery and disclosure of critical security vulnerabilities. These researchers often work on the front lines of software and hardware ecosystems, engaging directly with real-world products and deployment environments. For instance, in 2023, Google researcher (affiliated with Project Zero) disclosed "Reptar," a buffer-processing vulnerability in Intel's Alder Lake, Raptor Lake and Sapphire Rapids CPUs. The bug caused privilege escalation or denial-of-service attacks, with both microcode patches and CVE assignment rolled out in November 2023.[34] Similarly, in February 2021, independent security researcher Alex Birsan demonstrated the "dependency confusion" exploit by uploading malicious packages to public repositories under names matching internal dependencies of major tech firms such as Apple, Microsoft, Tesla and Uber. These malicious packages were automatically installed by developers' build systems, granting him code execution on their internal systems. Birsan responsibly disclosed the issue.[35]

1. Vulnerability reporting as a research activity through the lens of the EU cybersecurity law

However, the act of vulnerability reporting carries the inherent risk of legal repercussions, including criminal prosecution. Various EU laws, such as the Cybersecurity Act (CSA),[36] the NIS2 and the CRA recognises the importance of security research and anticipate activity of the security researchers.

The CSA requires manufacturers and ICT service providers whose products have been certified under the EU cybersecurity certification framework to publicly disclose their contact information and accepted reporting methods for vulnerability disclosure.[37] The NIS2 mandates that essential and important entities implement or at least cooperate in

[31] Graz University of Technology, "Meltdown and Spectre" <https://meltdownattack.com> (accessed 6 August 2025).

[32] "Weak Diffie-Hellman and the Logjam Attack" <https://weakdh.org> (accessed 7 August 2025).

[33] "The DROWN Attack" <https://drownattack.com> (accessed 7 August 2025).

[34] A Hashim, "Intel released urgent patch for Reptar vulnerability in its CPUs" (*Latest Hacking News*, 20 November 2023) <https://latesthackingnews.com/2023/11/20/intel-released-urgent-patch-for-reptar-vulnerability-in-its-cpus/> (accessed 6 August 2025).

[35] A Birsan, "Dependency confusion: how I hacked into Apple, Microsoft and dozens of other companies – the story of a novel supply chain attack" (*Medium*, 9 February 2021) <https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610> (accessed 7 August 2025).

[36] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151/15.

[37] Regulation (EU) 2019/881 (Cybersecurity Act), Art 55.

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

CVD processes. Commission Implementing Regulation (EU) 2024/2690 operationalises the NIS2 by requiring digital infrastructure entities to establish internal procedures for vulnerability handling, the CVD and to disclose vulnerabilities.[38] While the regulation formalises the procedural obligations of entities to receive and act on good-faith reports, it does not contain any vetting mechanism or procedural safeguards for security researchers nor grant legal protections to the researchers making those disclosures. Nor do the ENISA technical guidelines.[39] The CRA extends vulnerability reporting to products with digital elements. The CRA affirms the value of vulnerability research by requiring manufacturers to implement coordinated vulnerability disclosure procedures, encourages voluntary reporting to CSIRTs or ENISA, and mandates that users be informed of how to report vulnerabilities via a public contact point.

The CRA requires manufacturers to establish and maintain CVD policies and procedures to process and remediate vulnerabilities reported from both internal and external sources.[40] In addition, the CRA supports a culture of transparency and collaboration by allowing voluntary reporting of vulnerabilities, cyber threats, and near misses to CSIRTs or ENISA by manufacturers or third parties, including security researchers,[41] and mandates that manufacturers provide a public single point of contact for receiving such reports, along with access to their CVD policy.[42]

Many but not all CVDs give researchers express permission to probe a system, so long as they adhere to certain rules, including the rule of not publishing vulnerabilities until the developer or owner has a reasonable chance to fix it. A CVD program may include language intended to mitigate legal risk by authorising, or even inviting, independent security researchers to probe a system or product. Such policies will describe the products and assets that are covered, research techniques that are prohibited, how to submit vulnerability reports, and how long security researchers should wait before publicly disclosing vulnerabilities.[43]

Independent research isn't limited to public, external testers, private programs can include both **external specialists and internal security experts**. One model offers a compelling bridge between these two paradigms are **private bug bounty programs**. These programs rely on **pre-screened, externally sourced researchers** who are invited to participate based on a verified history of skill, trustworthiness, and sometimes identity or

[38] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers. Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 ... [2024] OJ L (18 October 2024).

[39] ENISA, "Technical implementation guidance on cybersecurity risk management measures" (v 1.0, June 2025) 103 <www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf> (accessed 7 August 2025).

[40] Regulation (EU) 2024/2847 (Cyber Resilience Act), art 13(8) and Annex I pt II(5) – Requires manufacturers to have appropriate procedures, including CVD policies, for handling vulnerability reports from internal or external sources.

[41] CRA, Article 15(1) (2Regulation (EU) 2024/2847 (Cyber Resilience Act), Art 15(1)–(2) - Allows voluntary reporting of vulnerabilities, cyber threats, and incidents to CSIRTs designated as coordinators or to ENISA by manufacturers and any natural or legal person.

[42] Regulation (EU) 2024/2847 (Cyber Resilience Act), Annex II pt 2.– Requires manufacturers to provide a single point of contact for vulnerability reporting and access to their coordinated vulnerability disclosure policy.

[43] AJ Grotto and J Dempsey, "Vulnerability disclosure and management for AI/ML systems: a working paper with policy recommendations" (16 November 2021) https://doi.org/10.2139/ssrn.3964084 (accessed 7 August 2025).

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

background checks. The use of a vetted, customised group of researchers – tailored to the system or domain in question – allows organisations to "harness the power of the crowd" while preserving operational and legal control.[44] These mechanisms are not only tools for improving cybersecurity but also serve strategic organisational functions. Some entities utilise their CVD programmes as informal recruitment pipelines for independent penetration testers or future in-house red team members, leveraging familiarity and proven capabilities at lower cost. Moreover, private programmes operated on platforms enable more refined governance, allowing organisations to vet participants, authenticate access, and retain control over credentials, thereby mitigating concerns about rogue actors or unprofessional conduct. By requiring authentication and facilitating activity monitoring, these programmes also generate valuable metrics on researcher engagement, which can inform broader risk management strategies and the overall efficacy of disclosure initiatives.[45] Greater governmental involvement in vulnerability disclosure should include the promotion or mandatory implementation of bug bounty programs and coordinated vulnerability disclosure platforms, as these are seen as effective, low-barrier mechanisms for engaging external researchers.[46]

In other words, private programs allow for **independent testing** within a framework of **contractual and technical safeguards**, thereby addressing concerns about researcher accountability, data protection and regulatory compliance.

Pre-screened researchers operating within private bug bounty environments demonstrate that **independence and trust can coexist**, especially when access is structured, scoped and monitored. These researchers are often more effective when it comes to uncovering novel or context-specific vulnerabilities, particularly in pre-release or complex digital ecosystems.

2. *Research and Auditing under the Act on Digital Services*

The DSA represents a comprehensive regulatory framework aimed at ensuring a safer and more transparent online environment within the European Union. Its rationale lies in addressing the growing societal and economic impact of digital platforms, particularly very large online platforms and search engines. Its scope includes safeguards for fundamental rights, accountability mechanisms for recommender systems, rules for mitigation of deceptive design and systemic risk mitigation.

DSA establishes a layered and structured framework of due diligence duties for online platforms, organised in a pyramid-like hierarchy. At the top are the specific obligations applicable exclusively to Very Large Online Platforms (VLOPs), designed to tackle systemic risks. These are built upon a foundation of universal, basic, and advanced duties, forming an interconnected set of regulatory responsibilities for intermediary services, hosting service and online platforms.[47]

[44] J Haddix, "Private, public, or hybrid? Finding the right fit in a bug bounty program" (*Dark Reading*, 5 October 2017) <www.darkreading.com/vulnerabilities-threats/private-public-or-hybrid-finding-the-right-fit-in-a-bug-bounty-program> (accessed 7 August 2025); M Al-Banna and others, "Software security professionals: expertise indicators" in *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)* (IEEE 2016) 139–148; J Wachs, "Making markets for information security: the role of online platforms in bug bounty programs" (2022) *arXiv preprint* arXiv:2204.06905 https://arxiv.org/abs/2204.06905 (accessed 7 August 2025).

[45] T Walshe and A Simpson, "Coordinated vulnerability disclosure programme effectiveness: issues and recommendations" (2022) 123 Computers & Security 102936. https://doi.org/10.1016/j.cose.2022.102936 (accessed 7 August 2025).

[46] A Zrahia, "Navigating vulnerability markets and bug bounty programs: a public policy perspective" (2024) 13(1) Internet Policy Review https://doi.org/10.14763/2024.1.1740 (accessed 7 August 2025).

[47] See more M Husovec and IR Laguna, "Digital Services Act: a short primer" (5 July 2022) https://doi.org/10.2139/ssrn.4153796; P de Miguel Asensio, "Due diligence obligations and liability of intermediary services: the

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

When it comes to requirements for the biggest actors within the scope of the regulation – VLOPs (and VLOSEs), there are at least two mechanisms that may be utilised by researchers: (i) data access and (ii) auditing. Both may provide insights how different risks including cybersecurity risks are mitigated by VLOPs and VLOSEs.

a. Data Access for researchers

The DSA differentiates between narrow research-questions-driven research and exploratory research[48] or in other words research with non-public data and publicly available data.[49] Researchers investigating specific threats such as coordinated inauthentic behaviour facilitated by platform vulnerabilities may need access to internal platform datasets, such as logs of automated account creation or incident reports, which fall under the DSA's vetted researcher regime in Article 40(4). In contrast, exploratory studies that examine patterns of phishing campaigns or malware distribution through public content, like comments or shared links, can often proceed using openly accessible data, as protected under Article 40(12).

Narrow research is regulated by the mechanism for vetting researchers as foreseen by Article 40 (12) of the DSA. The DSA grants vetted researchers access to data from VLOPs and VLOSEs to study systemic risks and assess mitigation measures. This access is crucial for understanding and addressing issues like the spread of disinformation, illegal content and other societal harms.[50]

Under article 40 (8) to be vetted, researchers must demonstrate that they meet all of the requirements stemming from the provision. Researchers requesting access to data must be affiliated with a research organisation[51] as defined in Article 2(1) of Directive (EU) 2019/790 and demonstrate independence from commercial interests.[52] They must also be capable of meeting specific data security and confidentiality standards relevant to the request, including describing the technical and organisational measures they have implemented to ensure personal data protection.[53] Their application must clearly show that the requested access and time frames are necessary and proportionate for the intended research purposes, and that the outcomes of the research will contribute meaningfully to the systemic risk research.[54] Furthermore, the planned research must align with the purposes specified in the DSA, and researchers must commit to publishing their results openly and free of charge[55] within a reasonable period after completing the research, in compliance with Regulation (EU) 2016/679 and with due regard to the rights and interests of the service recipients concerned.

Explorative research or research on public data is available for research purposes to those who meet the relevant criteria. Researchers seeking to access publicly available data under Article 40(12) of the DSA must be independent from commercial interests, disclose their research funding, ensure they can meet data security and confidentiality standards

proposal for the EU Digital Services Act" in D Moura Vicente, S de Vasconcelos Casimiro and C Chen (eds), *The Legal Challenges of the Fourth Industrial Revolution* (Law, Governance and Technology Series vol 57, Springer 2022) https://doi.org/10.1007/978-3-031-40516-7_3 (accessed 7 August 2025).

[48] M Husovec, "How to facilitate data access under the Digital Services Act" (19 May 2023) <https://ssrn.com/abstract=4452940> (accessed 7 August 2025).

[49] Algorithmic Transparency Centre, "FAQs: DSA data access for researchers" (3 July 2025) <https://algorithmic-transparency.ec.europa.eu/news/faqs-dsa-data-access-researchers-2025-07-03_en> (accessed 7 August 2025).

[50] European Commission, "DSA whistleblower tool" <https://digital-strategy.ec.europa.eu/en/policies/dsa-whistleblower-tool> (accessed 7 August 2025).

[51] Regulation (EU) 2022/2065 (Digital Services Act), Art 40(8)(a).

[52] Regulation (EU) 2022/2065 (Digital Services Act), Art 40(8)(b).

[53] Regulation (EU) 2022/2065 (Digital Services Act), Art 40(8)(c).

[54] Regulation (EU) 2022/2065 (Digital Services Act), Art 40(8)(e).

[55] Regulation (EU) 2022/2065 (Digital Services Act), Art 40(8)(g).

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

including the protection of personal data, and access only data that is necessary and proportionate for conducting research aimed at detecting, identifying or understanding systemic risks as foreseen by the DSA.[56]

According to Husovec, Article 40(12) of the DSA serves a dual function in the context of research access to platform data. On the one hand, it acts as a protective mechanism ("shield") for researchers, pre-empting legal actions that providers might pursue under other areas of law such as sui generis database rights, copyright, technical protection measures, unfair competition or contractual claims. So long as the conditions of Article 40(12) are fulfilled, attempts to obstruct or litigate against such research activities are effectively blocked. On the other hand, Article 40(12) also operates as a "sword" by empowering researchers to challenge illegitimate technical barriers such as IP blocking or CAPTCHA mechanisms that platforms may impose to hinder data access. This enables researchers to invoke the DSA either to remove such restrictions or to secure specific exemptions that facilitate data scraping for legitimate research purposes.[57] This is particularly interesting in terms of the CRA and NIS2 which encourages EU Member States to adopt measures to protect security researchers from criminal or civil liability and recommend the development of non-prosecution guidelines and liability exemptions for those conducting information security research in good faith.[58]

There is no way of knowing what data VLOPs actually gather, infer, process and use in their business operations. However, researchers will be expected to be specific about the data they require for their scientific investigations. The DSA give them unprecedented data access to online platforms to unpack opaque algorithmic systems.[59] However, the absence of a full picture of the data VLOPs may render data access less effective than intended. Considering these major interpretational and operational limitations, data access under Article 40 DSA remains, for the time being and most part, shrouded in mystery.[60]

b. Auditing by researchers?

On the other hand, the DSA imposes the VLOPs and VLOSEs with broad transparency and due diligence obligations, that include the obligation to perform annual independent audits to assess their compliance with their obligations[61] and approach towards risk assessment and mitigation of identified risks.[62] Audit in general, is systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.[63] External audits include those generally called second and third party audits. Second party audits are conducted by parties having an interest in the organisation, such as customers, or by other individuals on their behalf. Third party audits are conducted by independent auditing organisations, such as those providing certification/registration of conformity or governmental agencies.

[56] Regulation (EU) 2022/2065 (Digital Services Act), Art 40(12).

[57] *Supra*, n 48.

[58] Regulation (EU) 2024/2847 (Cyber Resilience Act), rec 75; Directive (EU) 2022/2555 (NIS 2), rec 60.

[59] P Leerssen, "Outside the black box: from algorithmic transparency to platform observability in the Digital Services Act" (2024) 4(2) Weizenbaum Journal of the Digital Society https://doi.org/10.34669/WI.WJDS/4.2.3 (accessed 7 August 2025).

[60] C Goanta and others, "The great data standoff: researchers vs platforms under the Digital Services Act" (2025) *arXiv preprint* arXiv:2505.01122 https://arxiv.org/abs/2505.01122 (accessed 7 August 2025).

[61] Regulation (EU) 2022/2065 (Digital Services Act), Art 37.

[62] Regulation (EU) 2022/2065 (Digital Services Act), Arts 34 and 35.

[63] ISO 19011:2018, *Guidelines for auditing management systems*, cl 3.1.

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

Pursuant to Article 37 of the DSA, VLOPs and VLOSEs are subject to periodic assessments carried out by independent and qualified external auditors. These audits are intended to evaluate the platform's adherence to its legal obligations under the DSA, with particular attention to the identification and mitigation of systemic risks, including the moderation of illegal content and the safeguarding of minors. The auditing process plays a crucial role in enhancing transparency and accountability, as it results in detailed reports that include recommendations for remedial measures. These reports are submitted to the European Commission and may trigger enforcement action in cases where substantial shortcomings are detected.

Audits of VLOPs under the DSA require a holistic and layered examination of compliance with a broad spectrum of due diligence obligations. These obligations form a cohesive regulatory framework, wherein each tier from universal to special obligations reinforces the others. At the core lies the obligation to manage systemic risks, demanding that VLOPs identify, assess and mitigate a wide array of potential harms, including the dissemination of illegal content, infringements on fundamental rights, threats to civic discourse and public security, risks to public health and minors, and impacts on user well-being. Auditors must evaluate not only whether these risks are adequately addressed, but also whether mitigation measures are clearly formulated, effectively implemented and supported by verifiable evidence. Equally important is the quality of the VLOP's reporting practices, particularly the transparency and methodological soundness of their risk assessments and mitigation documentation. These special obligations are embedded within a broader compliance architecture that includes advanced obligations such as the handling of trusted flaggers, transparency of recommender systems, and fairness in design as well as basic and universal obligations related to content moderation, user redress mechanisms, and regulatory cooperation. The audit thus functions as a comprehensive accountability tool, scrutinising the VLOP's conduct across this interconnected compliance structure to ensure alignment with the DSA's overarching goal of mitigating systemic risks and safeguarding users' rights in the digital environment.

Beyond due diligence requirements, auditors must evaluate the compliance of VLOPs with their specific obligations and commitments, specifically potential adherence to Codes of Conduct pursuant to Article 45 or Crisis Protocols under Article 48.

Procedure of the audits is specified in more detail by the Commission delegated regulation laying down rules on the performance of audits for very large online platforms and very large online search engines ("Audit rules").[64] Audit rules specify the procedures, methodologies and criteria that must be followed to assess the compliance of designated services with their obligations under the DSA, particularly in relation to risk management, content moderation and transparency. The delegated regulation defines the qualifications and independence requirements for auditors, outlines the audit scope, and introduces a structured process for audit planning, execution, and reporting. Its objective is to ensure that audits are reliable, consistent and capable of holding VLOPs and VLOSEs accountable for systemic risks they pose.

In general, researchers play a multifaceted role in the audit ecosystem established by DSA. Research institutions may be formally recognised as eligible audit bodies and carry out audits directly. Additionally, researchers are empowered to independently assess and verify the outcomes of audits, introducing a crucial mechanism for external accountability. This oversight extends beyond platforms to include the auditors themselves, allowing researchers to identify and call out inadequate or overly permissive audit findings. Furthermore, the DSA enhances transparency by requiring providers, after an audit, to

[64] Commission Delegated Regulation (EU) 2024/436 of 20 October 2023 supplementing Regulation (EU) 2022/2065 by laying down rules on the performance of audits for very large online platforms and very large online search engines [2024] OJ L (2 February 2024).

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

submit written explanations of their actions or inaction to the European Commission. These justifications are then published in a public repository in a redacted form, enabling researchers, journalists, and civil society to scrutinise the reliability of both the audits and the audited platforms' responses.[65] This framework fosters a dynamic and transparent flow of information, making it more challenging for auditors or platforms to distort the findings. In addition, audit bodies may also draw upon independent academic research as a valuable source of insight when evaluating platform compliance.[66]

Audit and data access processes intersect in several ways. First, findings obtained by vetted researchers through data access can serve as valuable evidence for audits. These findings may reveal systemic risks or operational weaknesses, and platforms are expected to demonstrate how they have taken such external research into account in their own risk assessments and audit responses. Second, both the audit process and the data access aim to improve transparency and accountability. The extent to which a platform has cooperated with vetted researchers may be a relevant factor in assessing its overall compliance posture. Third, independent auditors may use external research reports derived from data access as part of their verification of a platform's risk mitigation strategies. The way a platform responds to and engages with such research can influence the outcome of the audit, including the auditor's confidence in the platform's governance. Finally, where vetted research uncovers systemic issues such as algorithmic amplification of harmful content or ineffective moderation practices the audit must evaluate whether the platform implemented effective corrective measures.

III. Rethinking Cybersecurity Research and the DSA as a model rules?

Cybersecurity research involves the collection, use and disclosure of information and/or interaction with connected network context, shaped by diverse and sometimes contradictory legal systems and societal norms.[67] The field of cybersecurity research is inherently multidisciplinary, integrating technical, social and policy-oriented dimensions. The EU cybersecurity research community is diverse and expansive, comprising over 750 research centres, more than 100 higher education programmes, and numerous policy-driven initiatives and networks. This ecosystem includes universities, specialised R&D institutions, public–private partnerships, and EU-level bodies working collaboratively on strategic and applied research.[68] A defining feature of cybersecurity research is its focus on pushing the boundaries of current knowledge.

Cybersecurity researchers are not merely assessors of existing systems; they act as innovators, conceptual thinkers, and systems analysts who decompose technologies to understand weaknesses, test hypotheses,[69] and propose novel mitigation strategies.[70] Their outputs typically include prototypes, proof-of-concepts, publications,[71] and contributions

[65] M Husovec, *Principles of Digital Services Act* (Cambridge University Press 2024).

[66] Regulation (EU) 2022/2065 (Digital Services Act), rec 92.

[67] EE Kenneally and D Dittrich, "The Menlo Report: ethical principles guiding information and communication technology research" (3 August 2012) https://doi.org/10.2139/ssrn.2445102 (accessed 7 August 2025).

[68] ENISA, "Research and Innovation Brief: Annual report on cybersecurity research and innovation needs and priorities" (2022) 10 <www.enisa.europa.eu/sites/default/files/publications/RIT%20Annual%20Report%202021.pdf> (accessed 7 August 2025).

[69] Among main tasks of cybersecurity researcher belongs to manifest and generate research and innovation ideas; analyse and assess cybersecurity technologies, solutions, developments and processes. See *supra* n 16, 19.

[70] Among key skills of cybersecurity researcher belongs to generate new ideas and transfer theory into practice; decompose and analyse systems to identify weaknesses and ineffective controls. See *supra* n 16, 19.

[71] Publication in cybersecurity are deliverables of the cybersecurity research. See *supra* n 16, 19.

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

to open-source tools or policy recommendations.[72] Importantly, cybersecurity research often necessitates direct interaction with digital systems and datasets, which raises complex legal and ethical questions around data access, system integrity and responsible disclosure.[73]

This interaction with real systems places cybersecurity researchers at the intersection of technical exploration and regulatory constraint. Engaging with live environments, e.g., through vulnerability discovery, proof-of-concept exploitation or simulation of attack vectors, may involve temporary or partial violation of system boundaries. Therefore, the legitimacy of cybersecurity research hinges not only on its intent (such as improving public safety or advancing knowledge) but also on compliance with legal frameworks concerning unauthorised access, personal data protection and ethical integrity.

Cybersecurity auditing, in contrast, is rooted in the assessment of compliance with established norms, policies and legal requirements.[74] Auditors operate under a mandate, either internal or external, to review, verify and report on the effectiveness of security controls, typically using standardised procedures and audit frameworks. Unlike researchers, auditors do not generate new cybersecurity solutions or push for technological innovation. Rather, they validate and document the correct implementation of existing ones. The contrast becomes especially visible when analyzing their respective approaches to system and data access. Researchers may seek deeper, exploratory access to understand emerging threats or technological behaviour, often pushing against the limits of the known or permitted. Auditors, by contrast, access data within predefined scopes and with a clear mandate to verify rather than to discover or innovate. As such, researchers must operate with heightened sensitivity to legal boundaries, especially in jurisdictions where active interaction with live systems may trigger criminal or civil liability, even if done in good faith.

The key question in terms of DSA pertains to the scope of data access requirements. These are applicable when research pertains to systemic risk. Systemic risks are a new concept in the EU platform regulation. The DSA uses four non-exhaustive examples to illustrate systemic risks including actual or foreseeable negative effects for the exercise of fundamental rights.[75] The first concerns the spread of illegal content and criminal activity, such as child sexual abuse material, hate speech, or the illegal sale of prohibited goods, including counterfeit products or endangered species. These risks are particularly acute when content can be rapidly amplified via high-reach accounts or algorithmic tools, regardless of whether such content also violates the platform's terms of service.[76] The second category relates to potential or actual harm to fundamental rights protected by the EU Charter of Fundamental Rights. This includes threats to freedom of expression, data protection, non-discrimination and the rights of children and consumers. Such risks may arise from algorithmic systems or features that facilitate abusive practices, such as malicious takedown notices or interface designs that exploit users.[77] The third category

[72] Among main tasks of cybersecurity researcher belongs also to conduct experiments and develop a proof of concept, pilots and prototypes for cybersecurity solutions; assist in the development of innovative cybersecurity-related solutions; publish and present scientific works and research and development results. See *supra* n 16, 19.

[73] Key knowledge of cybersecurity researcher includes legal, regulatory and legislative requirements on releasing or using cybersecurity-related technologies; responsible information disclosure procedures. See *supra* n 16, 19.

[74] Auditor conducts independent reviews to assess the effectiveness of processes and controls and the overall compliance with the organisation's legal and regulatory frameworks policies. Evaluates, tests and verifies cybersecurity-related products (systems, hardware, software and services), functions and policies ensuring, compliance with guidelines, standards and regulations. See *supra*, note 16, 15

[75] Regulation (EU) 2022/2065 (Digital Services Act), Art 34(1)(b).

[76] Regulation (EU) 2022/2065 (Digital Services Act), rec 80.

[77] Regulation (EU) 2022/2065 (Digital Services Act), rec 81.

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

focuses on the potential impact of these services on democratic integrity, including threats to electoral processes, public discourse and civic engagement.[78] Finally, the fourth category addresses broader societal harms such as risks to public health, safety and well-being. These may arise from manipulative platform designs, coordinated disinformation campaigns, or interfaces that promote harmful behaviour or contribute to gender-based violence.[79] Together, these categories define a comprehensive framework for risk identification and mitigation that VLOPs and VLOSEs must incorporate into their systemic risk management obligations that may be researched or audited by researchers.

How cybersecurity research fits the scope? In our view, assessing cybersecurity risks may well fit within all the categories mentioned above. As indicated by the DSA, the interpretation of the notion of systemic risks may be perceived broadly and should include societal issues related to platform in the broadest sense. This ambiguity means that if a cybersecurity threat including a botnet or account hijacking campaign leads to societal harm, e.g., undermining election integrity or enabling crime it may be treated as part of the platform's DSA risk assessment and subject to subsequent audit or research.[80] Cybersecurity research is essential for identifying and preventing vulnerabilities that allow illegal content (such as child sexual abuse material, hate speech, counterfeit sales) to be distributed at scale. For example, research into bot networks, compromised accounts or unmoderated APIs can reveal how attackers exploit technical weaknesses to spread illegal material or coordinate illicit activity. Secondly, insufficient cybersecurity practices can expose users to data breaches, unauthorised surveillance or profiling, thereby infringing on rights such as privacy, data protection or non-discrimination. Research that examines the security of algorithmic systems or the resilience of user data protections directly contributes to assessing how platform design or misuse could harm fundamental rights. Thirdly, cybersecurity is critical in identifying threats like election interference, foreign influence operations and platform manipulation, e.g., through coordinated inauthentic behaviour or synthetic media. Research in this area can uncover how platform vulnerabilities are exploited to undermine civic discourse, spread false narratives or suppress legitimate voices, thus affecting democratic institutions and public trust. And finally, cybersecurity research plays a role in identifying how malicious actors spread disinformation related to health, e.g., during pandemics or target users with harmful content that contributes to mental health issues, addictive behaviour or gender-based violence. It can also uncover how interface manipulation or dark patterns are deployed in ways that amplify harmful behaviour or bypass user protections.

However, the research should always be grounded in the investigation of the systemic risks as foreseen by the DSA. Pure security research, e.g., in the form of probing the platform's code for vulnerabilities or studying techniques of cyber-attacks is *not explicitly covered* unless it ties back to the systemic risks of Article 34(1). This could be a limiting factor for cybersecurity research via DSA. On the other hand, a study that investigates the platform's susceptibility to hacking *in general* might not qualify for Article 40 access, whereas a study on how bot-driven disinformation campaigns operate (which has clear civic discourse implications) likely would.

The breadth of systemic risks creates challenges for data access requests. As recent TikTok case analysis revealed, not only are systemic risks very vague to define and identify, but requesting data can lead to a standoff problem between platforms and

[78] Regulation (EU) 2022/2065 (Digital Services Act), rec 82.

[79] Regulation (EU) 2022/2065 (Digital Services Act), rec 83.

[80] Similarly R Griffin, "The politics of risk in the Digital Services Act: a stakeholder mapping and research agenda" (2025) 5(2) Weizenbaum Journal of the Digital Society https://doi.org/10.34669/wi.wjds/5.2.6 (accessed 7 August 2025).

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

researchers.[81] However, some evidence gathered from researchers requesting to be vetted indicates that at least some platforms interpret requirements in a very flexible way.[82] Such cases stem also from the fact that there is no universal and horizontal legal definition of a "researcher" in the EU law. The DSA only references the notion of "research organisation" as defined in the Article 2 of the Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market[83] stating that researchers shall be affiliated with such organisations in case of seizing data access according to the DSA. The provision in question defines a research organisation as a university (including its libraries), a research institute or any other entity whose primary objective is to conduct scientific research or engage in educational activities that also involve scientific research, provided that it operates either on a not-for-profit basis or reinvests all profits into its scientific research, or carries out its activities pursuant to a public interest mission recognised by a Member State. Additionally, the results generated by such research must not be accessible on a preferential basis to any undertaking that holds a decisive influence over the organisation.[84]

The EU law contains the legal definition of researcher for purposes of migration. According to the Directive (EU) 2016/801[85] the researcher is defined as "a third-country national who holds a doctoral degree or an appropriate higher education qualification which gives that third-country national access to doctoral programmes, who is selected by a research organisation and admitted to the territory of a Member State for carrying out a research activity for which such qualification is normally required."[86] Interestingly, the definition of research organisation is much broader than in the Directive (EU) 2019/790 as it includes "public or private organisation which conducts research" without further requirements.[87]

Considering the definition and requirements, there are several limits in terms of cybersecurity research. The first one presents limitations for cybersecurity researchers not currently affiliated with universities or research institutes. Furthermore, the notion of research organisation may be interpreted flexibly, particularly regarding non-profit research institutes with full or partial funding by private entities. Regarding explorative research bearing lower requirements for classification, cybersecurity researchers may still face tough barriers. They still must be free from commercial interests that might be specifically tricky for organisations conducting ethical hacking as a service. Additionally, funding disclosure obligation may be complicated as well. However, in general, explorative research provision is better suited for researchers in the field of cybersecurity.

In terms of auditing criteria for organisations, cybersecurity organisations may easily fit in within the scope and conduct independent audits. However, the scope of audited risks may be too narrow for VLOPs and VLOSEs to contract such organisation to conduct full

[81] C Goanta and others, "The great data standoff: researchers vs platforms under the Digital Services Act" (2025) arXiv preprint arXiv:2505.01122 https://arxiv.org/abs/2505.01122 accessed 7 August 2025.

[82] See, e.g., I Srba, "When research APIs close the door: using algorithmic auditing as an alternative approach to study social media" (Kempelen Institute of Intelligent Technologies, 11 July 2025) <https://kinit.sk/when-research-apis-close-the-door/> (accessed 7 August 2025); JG Bourrée and others, "On the relevance of APIs facing fairwashed audits" (2023) *arXiv preprint* arXiv:2305.13883 https://doi.org/10.48550/arXiv.2305.13883 (accessed 7 August 2025).

[83] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L 130/92.

[84] Directive (EU) 2019/790, Art 2(1).

[85] Directive (EU) 2016/801 of the European Parliament and of the Council of 11 May 2016 on the conditions of entry and residence of third-country nationals for the purposes of research, studies, training, voluntary service, pupil exchange schemes or educational projects and au pairing (recast) [2016] OJ L 132/21.

[86] Directive (EU) 2016/801, Art 3(1).

[87] Directive (EU) 2016/801, Art 3(10) and Art 3(9). The same directive defines research as "creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture and society, and the use of this stock of knowledge to devise new applications." Art 3 (9).

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

audit as required by the DSA. This does not rule out sub-contractors of auditing organisations.

Under the DSA, the rationale for vetting researchers stems from the fact that they request privileged access to internal data. This includes, for example, access to proprietary recommendation algorithms, training datasets, systemic risk indicators and internal moderation decisions. These data are generally protected for reasons of confidentiality, intellectual property, or user privacy. In our opinion, vetting would not help cybersecurity researchers. Most ethical hackers do not require privileged access to internal datasets or models. What they need instead is legal protection for good-faith security testing, clear rules for coordinated vulnerability disclosure, and assurance that they will not face disproportionate penalties for reporting flaws responsibly. In this field, the lack of legal clarity creates a chilling effect, and vetting does little to address that core concern.

Access to internal, non-public systems for the purpose of cybersecurity research lies outside the traditional understanding of public-interest cybersecurity research. It more closely resembles targeted, privately initiated vulnerability discovery programmes, such as private bug bounty schemes. Such activity including a possible vetting process, should be acknowledged as a legitimate component of the broader cybersecurity research ecosystem, particularly given its potential to uncover critical vulnerabilities in real-world environments.

However, this recognition should not lead to the imposition of blanket pre-vetting or registration requirements for all cybersecurity researchers. Such measures risk having a disproportionately deterrent effect, especially on independent or unaffiliated researchers who may lack institutional backing or formal recognition. Imposing formal vetting obligations as a condition for legal protection could undermine the open and inclusive character of responsible vulnerability disclosure and research.

This principle should apply equally to CVD policies. While some jurisdictions, such as Malta,[88] have introduced a researcher notification requirement within their national CVD frameworks, such approaches remain the exception rather than the norm.

On the other side, as AI systems are bringing new types of **AI-specific vulnerabilities**. These include not only traditional security flaws (such as model inversion or data poisoning) but also failures that blur the lines between safety, security, and robustness.[89] Unlike conventional software bugs, many AI vulnerabilities stem from statistical behaviour, machine learning algorithms, or training data. For this reason, **AI vulnerability disclosure may require new forms of oversight and coordination**. Disclosures may involve sensitive proprietary architectures, unsafe training data, or flaws that could be exploited at scale. Thus, AI vulnerability research may, in some cases, justify **a controlled coordination, protection of sensitive assets**, and **structured mitigation timelines**.

It is important to underscore that privacy and security are no longer separable regulatory domains. Vulnerabilities in AI systems frequently have privacy implications whether through data leakage, insecure endpoints, or unauthorised access to model weights. If researchers under the DSA are to meaningfully assess compliance with privacy obligations, they must also possess the technical capacity to evaluate the security architecture on which those privacy guarantees depend. In that context, limited forms of technical probing, even by vetted researchers, may be necessary, provided that appropriate safeguards are in place.

[88] Malta Information Technology Agency (MITA), *National Coordinated Vulnerability Disclosure Policy (NCVDP)* (2024) P-SPG-001-01, 6 <https://mdia.gov.mt/app/uploads/2024/12/P-SPG-001-National-Coordinated-Vulnerability-Disclosure-Policy.pdf> (accessed 7 August 2025).

[89] H Nolte and others, "Robustness and cybersecurity in the EU Artificial Intelligence Act" in *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2025) <https://arxiv.org/abs/2502.16184) (accessed 7 August 2025).

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press

IV. Conclusion

It is evident from existing legal and technical practice that cybersecurity research encompasses a diverse and distributed community of actors who do not operate exclusively within institutional frameworks.

The DSA establishes a formal vetting framework for researchers who are granted privileged access to internal platform data. This includes access to proprietary recommendation algorithms, training datasets, systemic risk indicators, and moderation decisions, data that are protected for commercial, privacy or security reasons. In these contexts, formal vetting procedures are justified to ensure the confidentiality, integrity and lawful use of the data. We confirm that research activities conducted within the scope of the DSA framework also encompass a cybersecurity dimension.

Cybersecurity research, however, is structurally distinct. It is primarily adversarial and probing, rather than observational, and typically targets publicly reachable or improperly exposed systems, rather than relying on privileged access. In this context, the imposition of vetting requirements would not enhance trust or safety but would instead undermine the independence and spontaneity that are essential for discovering unknown vulnerabilities. Moreover, it would introduce barriers to entry, especially for unaffiliated or informal researchers, and could privilege well-resourced institutions over individual contributors. In contrast to the DSA, the CRA offers a more suitable approach for integrating cybersecurity research into legal frameworks, obliging manufacturers to implement CVD policies and procedures. In sum cybersecurity research in general cannot and should not be restricted to formally vetted actors alone. If researchers are tasked with assessing risks requiring at least limited access to system architecture or internal components in order to meaningfully assess the relevant risks, it may justify a degree of access vetting.

Further, the experience of pre-screened researchers in private programs demonstrates that **structured access control and independent discovery are not mutually exclusive**. Private bug bounty programs can serve as a regulatory model for integrating external cybersecurity research into structured risk management frameworks. These programs demonstrate how third-party security testing, when properly scoped, authorised and incentivised, can strengthen the cybersecurity posture of critical sectors or high-risk digital products, such as those governed by the NIS2 or the CRA.

Acknowledgments. Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 17R05-04-V01-00002 (Competence Center for the Regulation of Cybersecurity, Privacy Protection and Cybercrime).

Competing interests. The authors have no conflicts of interest to declare.

Cite this article: M Rampášek and M Mesarčík (2026). "Rethinking Cybersecurity Research Governance: Lessons from the Act on Digital Services?" *European Journal of Risk Regulation* **17**, 312–328. https://doi.org/10.1017/err.2025.10060

https://doi.org/10.1017/err.2025.10060 Published online by Cambridge University Press