Technology and Regulation

special issue: security in the digital age

# The Issue Of Security In The Digital Age

| | |
|---|---|
| **Author(s)** | Clara Boggini, Julia Krämer, Wouter Scherpenisse, Daan Albers, Silvia de Conca & Sascha van Schendel |
| **Affiliation(s)** | Clara Boggini – PhD candidate at the Erasmus School of Law and the Erasmus Center of Law & Digitalization, of Erasmus University Rotterdam, the Netherlands.<br>Julia Krämer – PhD candidate at the Erasmus School of Law and the Erasmus Center of Law & Digitalization, of Erasmus University Rotterdam, the Netherlands.<br>Wouter Scherpenisse – PhD candidate at the Erasmus School of Law and the Erasmus Center of Law & Digitalization, of Erasmus University Rotterdam, the Netherlands.<br>Daan Albers – Research assistant at the Erasmus School of Law and the Erasmus Center of Law & Digitalization, of Erasmus University Rotterdam, the Netherlands.<br>Silvia de Conca – Assistant Professor in Law and Technology at the Transnational Legal Studies department, Faculty of Law, Vrije Universiteit Amsterdam, the Netherlands.<br>Sascha van Schendel – Assistant Professor of Data Protection & Cybersecurity at the Erasmus School of Law and theErasmus Center of Law & Digitalization, of Erasmus University Rotterdam, the Netherlands. |

| | |
|---|---|
| **Published** | **Published**: 31 Mar 2026 |
| **Citation** | Clara Boggini, Julia Krämer, Wouter Scherpenisse, Daan Albers, Silvia de Conca & Sascha van Schendel, The issue of security in the digital age, Technology and Regulation, 2026, 01-09 • 10.71265/d86a0p28 • ISSN: 2666-139X |

This Special Issue is the outcome of the workshop *Security in the digital age*, that took place on June 3-4 2025 at Erasmus University Rotterdam. The workshop was organised by a team of law scholars of the Erasmus Center of Law and Digitalization from Erasmus University Rotterdam, and the Amsterdam Law and Technology Institute of Vrije University Amsterdam, thanks to the financial support of the Sectorplan SSH-Breed[1] on Digitalization, and the Working Group on Human Rights in the Digital Age of the Netherlands Network for Human Rights Research. During those two days, academic experts of all seniorities and nationalities presented their research at the intersection of security, digital infrastructures, and fundamental rights. Selected papers among those presented have been collected in this Special Issue.[2]

The idea for the workshop comes from the realization that there is a gap in the discourse on digital infrastructures and cybersecurity: the implications for human rights of the interactions of the two phenomena is noticeably underexplored. The debate around digital infrastructures has developed in recent years along some very important lines. The first line is the very nature of infrastructure in the digital society, which has been changed by the process of digitalization of existing public infrastructures, such as electricity and water grids, as well as the development of online and digital tools for public administration and the exercise of citizens' rights. In parallel, the role of many digital services has grown to include that of infrastructures, especially with the provisions of web services for Cloud computing and storage, and necessary suites of software for private and public entities. Additionally, the emergence of *quasi*-infrastructures is also debated,

1. Sectorplan SSH-Breed: The Influence of Digitalisation on Work, Prosperity and Entrepreneurship.
2. The guest editors of the special issue wish to thank the editorial team at Technology and Regulation for their support in this special issue.

especially with regard to instant messaging apps and social media. The nature of infrastructures following digitalization and the diffusion of online intermediaries brings to the forefront themes of the convergence of the public with the private domain, and the arm wrestling between public interests (among which the respect of fundamental rights occupies a prominent position) and profit. The second line (closely connected to the first line), concerns the development of more plans for digital infrastructures (e.g. the UN Global Digital Compact, or regional initiatives such as the European Energy Strategy and the Twin Transition) and raises the question of how to manage the access to both digitalized public infrastructures and new digital quasi-infrastructures. Here, intermediaries mediate the relationship between other companies and the government (B2G), citizens and the government (G2C) and even between government and government (G2G).[3] The characteristics of infrastructures and public services and the nature of a 2-way market create the perfect recipe for dependencies and concentration of services within the hands of a few private actors. If, on top of that, we add the mandatory mass adoption of certain digital infrastructures, the vulnerabilities for individuals and their rights become even more cause of concern. Finally, the third line concerns the interaction of hardware and software, from the fundamental role of the internet backbone and satellites, to the diffusion of Cloud services and server farms. The hardware and software components of digital infrastructures raise issues of safety and resilience, but also access, inclusion, digital divide, and Global justice.

Cybersecurity has gained importance in connection with all three lines of the development of digital infrastructures, and rightly so. The security, safety and resilience of these infrastructures directly affects human rights and the rights of citizens, and each of the themes listed above brings its own challenges from a cybersecurity perspective. But there is more. Underpinning the digitalization of public infrastructures, the emergence of quasi-infrastructures, the bottleneck created by intermediaries, and the interplay of software and hardware, there is *power*. And power requires strong human rights protection. Digital infrastructures can enhance existing systems of power or create new dependencies, new asymmetries of power, and new distributional injustices at global, national, and local level. Cybersecurity might appear like a purely technical matter, based on standards and governance mechanisms, but it entails choices that can make a significant difference between empowering individuals, citizens, marginalised and vulnerable groups, or sacrificing their rights in the name of other (public and private) values. Sometimes choices even need to be made within the framework of human rights protection, where rights of groups with different needs must be balanced. As we explore in this special issue: how we, as a society, decide to secure our digital infrastructures, will make a world of difference.

## 1. Responsibilities In The Digital Age

Thomas Hobbes stipulated in his *Leviathan* a fundamental premise of modern political thought: that the primary function of political authority is to provide security.[4] Without a 'common Power' that stipulates in 'Lawes' a clear distinction between 'Good and Evil',[5] it would be impossible to provide a 'common Peace and Safetie' because: '*Where there is no common Power, there is no Law: where no Law, no Injustice*.'[6] Hobbes describes how sovereign, centralised power (ergo: government) arises from a collective need to escape the anarchic state of nature, where life is '*solitary, poore, nasty, brutish, and short*.'[7]

Security, in this sense, was a concept that – for a long time – was only used in relation to the physical world. The 'Information Technology Revolution',[8] however, has profoundly unsettled this paradigm, e.g. in relation

3. As the tensions over Chinese-manufactured solar panels have shown, for example: Linus Höller, 'Chinese hold on solar-power tech raises fresh sabotage fears in Europe' (*DefenseNews*, 29 May 2025) https://www.defensenews.com/global/europe/2025/05/29/chinese-hold-on-solar-power-tech-raises-fresh-sabotage-fears-in-europe/ accessed 24 February 2026.
4. Thomas Hobbes, *Leviathan* (first published 1651, Penguin Classics 2017) 140.
5. Hobbes (n 4) 146.
6. Hobbes (n 4) 104.
7. Hobbes (n 4) 103.
8. Manuel Castells, *The Rise of the Network Society* (Blackwell 1996).

to traditional concepts such as state sovereignty.[9] Furthermore, the transition of a significant part of our social, economic, and political life to digital spaces comes with new security risks. In cyberspace, threats are no longer solely confined to the physical world; cyber attacks, data breaches, misinformation campaigns stress the relevance of digital security as well. This Digital Age requires a new perspective on traditional frameworks concerning government responsibilities.

Unlike security responsibilities in the physical world – such as those performed by the armed forces and the police – the digital world relies heavily on assistance from the private sector. This is because a large part of the digital infrastructure is owned by the private sector, best practices at individual level can decrease cyber risks significantly,[10] and the government does not have the capacity (and authority) to monitor all digital spaces and devices adequately. This hybrid responsibility makes the digital world such an interesting area of research.

## 2. The Infrastructural Shift in Cybersecurity Studies

The link between infrastructure studies, and data privacy and cybersecurity has increasingly drawn the attention of experts, reflecting how digital platforms have taken on infrastructural functions. Plantin et al. show that companies such as Google and Meta are no longer just websites or apps, but have taken on *infrastructural properties* by functioning as essential communication and information infrastructure.[11] Consequently, ensuring cybersecurity and data protection is framed as an infrastructural issue, rather than a legal compliance concern. This view is echoed by scholars analysing Big Tech's "infrastructural power", a term that has been defined as "a platforms control over gatekeeping, transmission and scoring mechanisms"[12] and that illustrates how control over central technical architectures, such as software production, data centers or networks, can lead to far-reaching influence on markets and communication systems.[13] Infrastructural power goes beyond the notion of "platform power", which is another well-known concept used to describe the influence of powerful digital platform providers.[14] While platform power highlights the possibility of platform providers to restructure data flows, govern intermediaries, and the ability of those companies to impact social and democratic functions of society, infrastructure puts the focus on the control of the underlying structures the digital world is built upon.[15]

Concentrating essential digital infrastructure in the hands of a few powerful companies entails significant systemic risks in cases of malfunction or disruption. Recent incidents have illustrated these vulnerabilities vividly, such as the global *CrowdStrike* outage that temporarily paused critical systems relying on Microsoft across sectors[16], or the recent failure of Amazon Web Services (AWS) that rendered thousands of websites inaccessible.[17] These examples reveal that even in the absence of a cyberattack, the centralisation of infrastructural control, opposed to more decentralised and resilient architectures, creates structural fragility. The infrastructural power of these companies thus derives not only from their ability to mediate access

9. Lucie Kadlecová, *Cyber Sovereignty: The Future of Governance in Cyberspace* (Stanford University Press 2024) 30.
10. David Clemente, 'Personal Protection: "Cyber Hygiene"' in Paul Cornish (ed), *The Oxford Handbook of Cyber Security* (Oxford University Press 2021) 361–76.
11. Jean-Christophe Plantin and others, 'Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook' (2018) 20 New Media & Society 293.
12. Sabeel Rahmaan, 'Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities' (2018) 2(2) Georgetown Law Technology Review 235.
13. Stine Lomborg and others, 'Monitoring Infrastructural Power: Methodological Challenges in Studying Mobile Infrastructures for Datafication' (2024) 13(2) Internet Policy Review 3.
14. Inge Graef and Friso Bostoen, 'A Typology of Platform Power and Its Regulation' (2025) Information, Communication & Society 1; Lina Khan, 'The Separation of Platforms and Commerce' (2019) 119 Columbia Law Review 973; José van Dijck, David Nieborg and Thomas Poell, 'Reframing Platform Power' (2019) 8 Internet Policy Review https://policyreview.info/node/1414 accessed 24 February 2026.
15. van Dijck et al (n 14) 3.
16. Tom Warren, 'Major Windows BSOD Issue Hits Banks, Airlines, and TV Broadcasters' (*The Verge*, 19 July 2024) https://www.theverge.com/2024/7/19/24201717/windows-bsod-crowdstrike-outage-issue accessed 24 February 2026.
17. Perez Z.W. Sarah, 'Amazon Identifies the Issue That Broke Much of the Internet, Says AWS Is Back to Normal' (*TechCrunch*, 21 October 2025) https://techcrunch.com/2025/10/21/amazon-dns-outage-breaks-much-of-the-internet/ accessed 24 February 2026.

and modalities for digital interactions, but also from their control over the foundational infrastructures on which economic, social, and governmental processes rely.[18] This conceptual shift underscores the growing interdependence between data protection, cybersecurity, and infrastructural governance, rendering the protection of digital infrastructures a priority policy concern within the European Union (EU).

## 3. The Emergence Of An Eu Governance Over Cybersecurity

Data and technologies have become the backbone of European Integration.[19] Securing the digital infrastructure prevents the EU internal market from coming to a halt, violations of the rights of EU citizens, or exposure to abuse by foreign powers.[20] However, to secure the digital infrastructure, the EU had to account for the multi-dimensional nature of cybersecurity. Cybersecurity is an umbrella term covering a wide range of issues, such as cybercrime, network and information security, or cyber-defence.[21] Each of these issues requires to be dealt under a different EU mandate, through different processes or logics, and through different policy instruments.[22]

Based on these premises, over the past decades, the EU has increased its policy-making in the domain of cybersecurity. Mapping the securitisation efforts of the EU reveals cybersecurity provision in Directives and Regulations related to the functioning of the internal market, as well as in Directives and Regulations concerning Economic, Monetary, and Financial Affairs, or concerning Internal Security, Justice, and Law Enforcement. More cybersecurity provisions are also present in Directives and Regulations related to the Energy, Transport and Health Policy, or the Education, Research and Space Policy, and the Foreign and Security Policy.[23]

Each of these Directives and Regulations focus on a different aspect of the securitisation of the digital infrastructure. Some of these provisions focus on the role of Member States in preventing cybercrime. Others impose obligations for the secure development and design of products with digital elements. Others focus more on the cyber resilience of the EU institutions or securing AI technologies. What emerges from this scenario is that the EU is securing the digital infrastructure with a multilayered approach, which crosses policies and dimensions of security.

## 4. Different Dimensions of Security in the Digital Age

As described above, the issue of security in the digital age raises new regulatory and societal questions, especially due to the involvement of various regulatory fields, stakeholders, fundamental rights involved, and societal, political and economic interests. Combining the different challenges and thematic fields, we can 'peel down' the different dimensions of security in the digital age in the following schematic:

18. van Dijck et al (n 14) 3.
19. Rocco Bellanova, Helena Carrapico and Denis Duez, 'Digital/Sovereignty and European Security Integration: An Introduction' (2022) 31 European Security 337, 337.
20. Helena Carrapico and Benjamin Farrand, 'Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy' (2020) 42 Journal of European Integration 1111, 1115.
21. George Christou, 'The Collective Securitisation of Cyberspace in the European Union' (2019) 42 West European Politics 278, 281.
22. Christou (n 21) 281.
23. Christina Rupp, *Navigating the EU Cybersecurity Policy Ecosystem* (Interface 2024) 17–35.

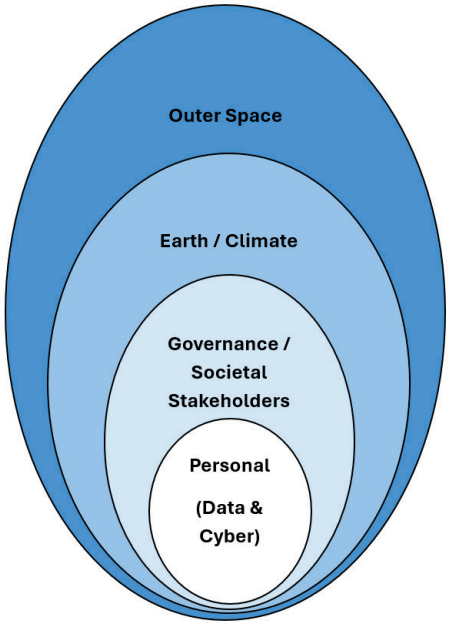


**Figure 1:** Layers of security in the digital age.

First, on the outer layer, we have the *Outer Space* dimension. Here we see new territorial, technical and regulatory questions on space infrastructure and cyber incidents in the outer space domain. Although space is not something we think about every day, partly because of its physical distance, the relevance of this domain is evident. What would happen if e.g. satellites were to fail? It's not just navigation systems that become unusable,[24] but also critical communication depends on satellites (Satcoms).[25] Disruptions to navigation and communication systems would not only impact our everyday economic and social activities, but could also carry significant strategic consequences. A recent example of the strategic value of space infrastructure is the deployment of Elon Musk's Starlink in Ukraine and Iran.[26] Protecting space infrastructure is therefore of great economic, societal and strategic importance. Space must therefore be seen as an essential part of overarching cybersecurity strategies.

Second, we turn to the *Earth and Climate* dimension. While climate change is often framed as a security issue in itself,[27] the intersection with (cyber)security reveals a far more intricate relationship. On one hand, innovation of digital technologies opened new avenues to enhance climate security and resilience. Artificial intelligence (AI) technologies in particular, may strengthen disaster warning systems, enable climate modelling, and optimize resource management, all of which could be favourable to a secure and stable environment.[28] Applications range from precision agriculture to monitoring environmental degradation, illegal resource extraction, and biodiversity loss.[29] At the same time, the infrastructure, data flows, and algorithmic systems that underpin (cyber)security depend on energy- and water-intensive data centres, require the extraction of rare minerals, and generate electronic waste, which are each driving ecological

24. GPS and Galileo e.g. Galileo – Satellite Navigation (*Defence Industry and Space, European Commission*, 2025) https://defence-industry-space.ec.europa.eu/eu-space/galileo-satellite-navigation accessed 24 February 2026.
25. Oltjon Kodheli and others, Satellite Communications in the New Space Era: A Survey and Future Challenges (2021) 23 IEEE Communications Surveys & Tutorials 70–109.
26. Joey Roulette and Cassell Bryan-Low, Musk's Starlink faces high-profile security test in Iran crackdown (*Reuters*, 16 January 2026) https://www.reuters.com/world/musks-starlink-faces-high-profile-security-test-iran-crackdown-2026-01-16/ accessed 24 February 2026.
27. Eliana Cusato, 'Of Violence and (In)visibility: The Securitisation of Climate Change in International Law' (2022) 10 London Review of International Law 203, 204.
28. Aude-Solveig Epstein, 'EU Environmental Law in the Digital Age: A Critical Outlook on the Twin Transition's Legal Structure' (2025) European Journal of Risk Regulation 1, 2.
29. Marie Francisco, 'Artificial intelligence for environmental security: national, international, human and ecological perspectives' (2023) 61 Current Opinion in Environmental Sustainability 101250, 101253.

costs.[30] Moreover, the cybersecurity infrastructures themselves are vulnerable to climate impacts, such as resource scarcity and power grid disruptions, which emphasise the need for closer integration between cyber and ecological systems.[31] Ultimately, the carbon footprint of digital technologies, the environmental cost of infrastructures, and the geopolitics surrounding critical minerals become central to understanding security in the digital age.

Third, on the societal level we see intricate issues of *Governance* and regulation, such as the shift and constant development in scholarly and regulatory debates on definitions and categorisation of infrastructures and (cyber) risk. Between legislators and jurisdictions, we can even see turf wars.[32] Furthermore, as cyberspace has expanded, more and more *Societal Stakeholders* have become involved. These stakeholders, while all recognising the need to secure against digital risks, often have diverging approaches and interests.[33] Consequently, their diverging interests and approaches create imbalances and power struggles. For instance, the reliance of EU actors on non-EU digital infrastructure creates gaps in digital governance. As the EU lacks sovereignty over the entities that control or provide these services, potential security shortcomings and jurisdictional clashes arise.[34] Therefore, ensuring the proper approach to governing these dynamics is a crucial dimension of security in the digital age. The choice of a given legal instrument, interpretation, or technical standard can deeply impact the governance of infrastructure and (cyber) risks. Therefore, security in the digital age has become a struggle to find the correct form of governance capable of aligning the security goals of the various stakeholders.

On the fourth layer, at the core of our schematics lies the dimension of the person, or the individual. Here we delve into questions of responsibilities and protection of individual (and group) rights. In this dimension we see the culmination of complexities. For example how different rights such as cybersecurity or privacy can overlap, can create tensions, such as in the domain of environmental protection and security, or can show the need for the development of new rights that may arise in the age of AI. Or how actors can be faced with obligations from a multitude of regulatory ambiguous or grey areas. Individuals, however, should not and cannot be seen as mere passive actors. Within this fourth layer we find that individuals bear responsibilities as well. Cyber resilience depends on a collective engagement. A great example of the value of individual responsibilities can be found in the so called 'coordinated vulnerability disclosure' (CVD) policies, that facilitate ethical hackers to report (software) vulnerabilities.[35]

## 5. Summary of the Papers in the Special Issue

The keynote address for the workshop was delivered by Prof. Bibi van den Berg and inspired the paper *Risk and uncertainty in the digital ecosystem*. In this paper, van den Berg brings to the fore the focus on (cyber) risk management in current debates and legislation, especially in the domain of digital technologies. Van den Berg explores different types of risk and uncertainties to challenge the convergence of risk management and the digital domain. In this paper, van den Berg delves into the strengths and weaknesses of cyber risk management and risk-based regulation, to establish under which conditions these approaches have merit, and where their limits lie. In this analysis of risk management, the following questions are answered:

30. Jessica Commins and Kristina Irion, 'Towards Planet Proof Computing: Law and Policy of Data Centre Sustainability in the European Union' (2025) Technology and Regulation 1, 2; Blair Attard-Frost and David G. Widder, 'The Ethics of AI Value Chains' (2025) Big Data & Society 1, 3.
31. Sandra Cassotta and Maria Pettersson, 'Climate Change, Environmental Threats and Cyber-Threats to Critical Infrastructures in Multi-Regulatory Sustainable Global Approach with Sweden as an Example' (2019) 10 Beijing Law Review 616, 622.
32. Lee Bygrave, 'The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes' (2025) 56 Computer Law & Security Review 106071.
33. Peter Davis and others, 'EU Cybersecurity Regulation in the Quantum Age' (*Social Science Research Network,* 8 August 2025) https://papers.ssrn.com/abstract=5383838 accessed 24 February 2026.
34. Benjamin Farrand, Helena Carrapico and Aleksei Turobov, 'The New Geopolitics of EU Cybersecurity: Security, Economy and Sovereignty' (2024) 100 International Affairs 2379, 2382-2385.
35. The NIS2-Directive confirms this value, but there are still some untapped opportunities (Max H. van der Horst, Rowin H.T. Jansen and Wouter Scherpenisse, 'Coordinated Vulnerability Disclosure en notificatie in het licht van NIS2' (2025) 5 Computerrecht 163, 309-315).

what are the implications of the conflation of different types of uncertainties into the singular notion of risk for risk management? Where does risk management fall on the risk-uncertainty scale? And what can risk management deliver for the digital ecosystem and other domains? To what extent regulation with risk management works well depends on where domains fall on the risk-uncertainty scale: risk management may lead to an illusion of control for problems for which no such control is feasible. Van den Berg proposes that for a number of different kinds of uncertainty in the digital ecosystem, we will not be able to tackle these effectively with risk management, for reasons such as: too little data, too much complexity, too few options to model in any meaningful way, plus the role of human intentionality in instigating incidents. Nonetheless, risk management has value for some specific cybersecurity challenges, especially for ' subway uncertainties'. The paper finishes with two suggestions for additional tools that could be used to resolve some of the risk- and uncertainty-related challenges in relation to digital technologies, when risk management is not the effective tool. First, the approach of *preparedness* embraces the fact that incidents will materialise as a given, and places emphasis on being able to deal with incidents and crises effectively and efficiently once they occur. Second, the approach of *Security by Design* motivates designers and developers to invest effort into making digital technologies secure when they are created and then keeping them secure throughout their entire lifecycle.

Van Ark's contribution, *From 'Terrorizing the Other' to Securitising All: The Turn towards Coercive Identity Management,* traces the shift in contemporary security governance post 9/11 and how the counter-terrorism framework has steadily expanded into a far broader system of identity control that now covers whole populations, not only those suspected of terrorism. The paper argues that the counter-terrorism architecture after 2001 has become a floodgate through which a wide array of surveillance, border, immigrations, and citizenship measures have been expanded, connected, and normalised. By analysing traveller programmes in the US, UK, and Germany, and large mega-sporting events, such as the 2018 FIFA World Cup, Van Ark shows that contemporary security governance has become an integrated "security matrix" combining border control, immigration law, criminal law, counter-terrorism, biometric infrastructures, and transnational data-sharing networks. The pursuit of the "voracious ideal" of security is further amplified by technological solutions and moral panics. The result is a so-called downward recalibration of the individual-state relationship and an increasingly coercive form of identity management that now affects even those never suspected of posing a security threat. Although not every aspect of security governance changed after 9/11, the aftereffects still echo in both expected and unexpected ways today. Against a backdrop of heightened security fears, commitments to human rights and broader norms of tolerance will remain under pressure.

In the contribution *Attribute-based signatures and eIDAS 2.0*, Hu examines whether eIDAS 2.0 facilitates the use of privacy-friendly trust services, in particular attribute-based authentication (ABA) and attribute-based signatures (ABS), in the light of the new European Digital Identity Wallets. ABA and ABS provide benefits such as modular identity and role-based signing, compared to traditional trust services. Here Hu also demonstrates the possible coherence between security and privacy aspects of personal data protection through ABA and ABS: using a modular identity, instead of presenting a full identity each time, users disclose only certain characteristics about themselves, depending on the application, without sharing more personal data than necessary. This offers flexibility and the possibility of data minimisation. An additional feature of ABA is that attributes can be stored decentralised, allowing users to retain control over their own personal data. In addition, ABS can achieve user unlinkability by using a different key pair for each attribute. The legal analysis shows the difference between authentication and signing, revealing that eIDAS 2.0 only facilitates attribute-based authentication through the European wallets, but not yet attribute-based signatures: according to Hu, ABS cannot legally meet the requirement for a qualified certificate (like CBS) because ABS do not use a certificate for validation, but rather a qualified attestation of attributes. Hu argues that this is unfortunate, given the advantages and functions of ABS and that this restriction is unnecessary, as the intended goal is technically feasible. The requirements for qualified attestations of attributes are strict and practically the same as the requirements for a qualified certificate. Hu further analyzes the possibilities and limits for use of pseudonyms, non-identifying attributes, decentralisation and unlikability under eIDAS 2.0. The article concludes that it is important that further details are provided on the regulations and implementing acts that actively support ABS. Without further development, we will have to wait for eIDAS 3.0 before a truly future-proof, user-friendly and privacy-friendly framework for digital identity, including signing, can be established within the EU.

In the paper *Redefining Digital Sovereignty: Infrastructural Dependence, Epistemic Asymmetry, and Governance Challenges in the Age of Big Tech*, Chung argues that digital sovereignty is being structurally reshaped by the privatization of cybersecurity governance. The paper shows that governments increasingly rely on transnational technology firms for essential security functions, such as cloud hosting, threat detection and data analytics. In this respect, Chung identifies three dilemmas for states: infrastructural dependency, epistemic asymmetry and governance capacity gaps, each of which constrains how states define and exercise digital sovereignty in practice. By analysing three cases in the United States (Project Maven), EU (AWS Sovereign Cloud) and Korea (LG CNS Smart Surveillance), Chung demonstrates that the capacity to govern is increasingly more dependent on access to technological infrastructures and control thereof, rather than traditional territorial jurisdiction and institutional control. Sovereignty should in that regard be reframed as "capacity"; the institutional and epistemic ability to govern interdependence. The paper closes by calling for sovereignty-by-design approaches that embed public values directly into technical architectures and institutional arrangements, rather than relying solely on ex post regulation.

In *Regulating data space connectors as an essential gateway to data spaces. The European Electronic Communications Code as a suitable choice for addressing a lack of interoperability and harmonisation?,* Fierens addresses a pressing and often overlooked issue within the EU's emerging framework on data spaces: the regulation of data space connectors which facilitate secure and controlled data sharing between different systems, platforms and organisations. These connectors, intended as neutral bridging software between existing data infrastructures, have developed in a heterogeneous and non-interoperable manner. The Data Governance Act, Data Act, and the Digital Markets Act are each designed to foster a data-driven internal market. Yet, as Fierens demonstrates, these legislative instruments inadequately address the technical or infrastructural dimensions of heterogeneous data space connectors. Instead, Fierens puts forward the hypothesis that data space connectors could be regulated under the European Electronic Communications Code (EECC). Drawing on the EECC's technologically neutral approach and interoperability obligations, he suggests that this framework could enhance interoperability between data space connectors and their core components, offer robust protection of end-users, and gives the flexibility to deploy a wide array of measures to ensure efficient investment and innovation.

In the contribution *Constructing Security for the Twin Transitions: The Tragedy of EU Law at the Intersection of Climate and AI Governance*, Sander offers a sharp critique on how the EU constructs the concept of "security" at the juncture of the green and digital transition. In its strategy of "twinning the green and digital transitions", the EU often puts forward AI technologies as potential remedies to combat the climate crisis. At the same time, AI technologies have become deeply intertwined with security concerns, both as tools deployed within security frameworks to combat risks across diverse contexts and as potential sources of new security risks. By adopting a narrative theoretical lens, Sander examines how certain security narratives have been integrated in three key EU legal instruments, namely the Critical Raw Materials Act, the AI Act, and the Digital Services Act. While each of these instruments aim to romantically portray the EU as a heroic, values-driven actor, these regulations end up falling within the genre of so-called "tragic governance". Security threats within these legal instruments are ultimately framed and addressed in terms that reinforce exploitative practices and tend to justify the exploitation against local communities, people on the move, and digital activists online, while only limitedly addressing existing problematic logics such as overconsumption, migrant neglect, and platform dominance. Still, Sander also identifies small openings within the legislative instruments, so-called "footholds for resistance", that could allow for alternative, more promising understandings of security to emerge.

In their paper *Space Infrastructure as Critical Infrastructure: Rights Beyond Earth in the Digital Age*, Casaril & Tricco make important connections between the dimensions of space infrastructure as a lesser explored type of critical infrastructure and cybersecurity. Casaril & Tricco demonstrate that the increased use and interconnection of space with terrestrial networks offers significant economic and societal opportunities, but also introduces new security challenges in the digital era. As critical infrastructure classifications extend to space-based systems, under evolving European Union legal frameworks, the space sector is adapting to broader requirements for resilience and sustainability. This requires space operators to balance economic development with the protection of fundamental rights, including the rights to security, access to essential

services, and a healthy environment. The paper explores the interconnection between terrestrial and orbital infrastructures by examining the emerging threats posed by the digitalisation of space systems. It assesses the mechanisms necessary to ensure their long-term safety and reliability, focusing on how space infrastructure is defined as critical under EU law and mapping the obligations arising for the space industry. Central to this analysis is the role of satellite networks in safeguarding multiple fundamental rights. In considering two use cases, Earth Observation for emergency management and Global Navigation Satellite Systems (GNSS) to enhance several critical services, this paper explores the impact of cyberattacks on these domains and their repercussions on fundamental rights. With this analysis, the authors aim to offer a fresh perspective on how to achieve a robust, secure, and rights-centric framework for space systems, contributing to a broader discussion on security in the digital age. The paper concludes that a next-generation space security regime must rest on four plain obligations. First, links that keep people alive must never go dark. Second, defence traffic and civilian traffic should run on separate circuits. Third, space assets that carry vital services must be clearly flagged in space-traffic systems so operators can spare them in a crisis. And lastly, constellations must include built-in failover mechanisms so that rescue teams and essential services remain connected even if one network is lost.