International Journal of Multidisciplinary and Current Research ISSN: 2321-3124
Research Article Available at: https://ijmcr.com

The Impact of Cybersecurity Regulations on Innovation in Startups

Piyush Rana[1*]

[1]Ph.D. Scholar, University of Delhi, New Delhi

Received 01 Apr 2026, Accepted 27 Apr 2026, Available online 29 Apr 2026, **Vol.14, No.2 (Mar/Apr 2026)**

Abstract

The accelerating digital shift has made cybersecurity a strategic priority, prompting a global rise in regulatory frameworks to safeguard data and infrastructure. Startup s, key drivers of innovation, face mounting compliance challenges—especially in sectors like fintech, health-tech, and SaaS—while working with limited resources. This paper examines how cybersecurity regulations both hinder and drive innovation. Using theories such as compliance burden, institutional legitimacy, and dynamic capabilities, it highlights the tension between regulatory demands and startup agility. Case studies reveal that while regulations impose costs and slow experimentation, they also promote trust, operational maturity, and innovation in areas like privacy-enhancing technologies. The findings underscore the need for balanced policies that protect digital ecosystems without stifling startup growth.

Keywords: *Cybersecurity Regulation, Startup Innovation, GDPR, CCPA, HIPAA, Compliance Burden, Privacy-Preserving Technologies, Security-By-Design, Fintech, Health-Tech, SaaS.*

Introduction

The pervasive digitisation of society and the economy have made cybersecurity a priority. Data breaches, ransomware attacks, and threats to critical infrastructure highlight the vulnerabilities in our globalized society, prompting governments worldwide to implement stricter laws (Lewis, 2018). Simultaneously, startups contribute significantly to economic growth, technological innovation, and the disruption of established industries through novel solutions. These young, agile companies, which are frequently characterized by low funding, small teams, and emphasis on quick iteration and market validation, now functions in an landscape that significantly influenced by complex cybersecurity regulations such as the California Consumer Privacy Act (CCPA), the Network and Information Security Directive 2 (NIS2), the General Data Protection Regulation (GDPR) of the European Union, and various industry-specific frameworks (OECD, 2023).

This research examines the challenge of balancing important cybersecurity regulations with the difficulties they create for startups with limited resources. It is unclear whether following these rules mainly slows down innovation by using up time and money, or if it encourages the creation of safer, more trustworthy technologies that shape new paths for innovation.

The main goal of this paper is to understand how cybersecurity rules affect how tech-based startups—especially in heavily regulated fields like fintech, healthtech, and Software-as-a-Service (SaaS)—approach innovation, manage their resources, and stay competitive.

The paper focuses on three key questions:

1. What problems do startups face when following cybersecurity rules?
2. Do these rules mostly block, support, or change how startups innovate?
3. How do startups adjust their products, work processes, and business models to meet regulatory demands?

This topic matters to many people. Policymakers need insights to create smart rules that protect users without hurting young businesses. Investors want to understand how much risk regulations pose to startups. Startup founders must determine how to follow these rules while growing their companies.

The structure of this paper starts by explaining key concepts, then outlines current cybersecurity laws, examines how these laws impact startups, provides real-world examples, discusses how startups balance compliance and innovation, considers policy options, and finally offers conclusions and ideas for future research.

*Correspondant Author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijmcr/v.14.2.17

Conceptual Framework and Definitions

To understand the interplay between cybersecurity regulations and startup innovation, we first need clear definitions and a helpful theoretical background. Cybersecurity regulations are legally binding rules created by governments or industry groups that require organizations to follow certain practices to protect their information systems, networks, and data from being accessed, used, changed, or destroyed without permission (ENISA, 2022). Examples include:

1. GDPR (General Data Protection Regulation): A strict European law that regulates data processing and sharing, even beyond Europe's borders.
2. CCPA/CPRA (California Consumer Privacy Act / California Privacy Rights Act): Gives robust privacy rights to California residents.
3. ISO/IEC 27001: An international standard that guides building a secure information management system (ISMS).
4. PCI DSS: A Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards for companies handling credit card data.
5. HIPAA: Health Insurance Portability and Accountability Act (HIPAA) is a Sector-specific regulations, such as U.S. law that protects personal health information, are particularly impactful.

Startups often need to follow rules like encryption and access controls, minimizing the data they collect, reporting data breaches quickly, and keeping detailed records to pass audits (e.g., under GDPR Articles 32–34).

Innovation in startups goes beyond just new ideas. It includes turning those ideas into real products or services, better working methods, or new business models. It may look like:

1. Product innovation: New or improved products/services.
2. Process innovation: Better methods of making or delivering things.
3. Business model innovation: New ways of creating, delivering, or earning from value (OECD/Eurostat, 2018).

Startups are usually new, fast-growing companies with limited money and staff. They often work in short cycles of testing and learning ("build-measure-learn") to quickly adapt to customer needs. Since they rely heavily on outside funding, investor confidence—especially in handling risk and rules—is very important (Gans et al., 2019).

Several theories help explain how regulations affect startups:

1. Compliance burden theory says complex and expensive regulations can be more complicated for smaller firms. The cost of compliance can take resources away from important areas like R&D and growth (Crain & Crain, 2014).
2. Institutional theory argues that following regulations helps organizations appear trustworthy and legitimate. For startups, compliance can help build trust with customers, investors, and partners, especially with larger, regulated companies (Suchman, 1995).
3. Dynamic capabilities theory sees the ability to adapt and reorganize quickly as a key strength. From this angle, regulations might help startups build strong internal security and risk management systems early on. These capabilities can give them a long-term advantage by helping them create more secure and reliable products (Teece et al., 1997).

In reality, startups face a mix of these forces: the burden of compliance, the need for legitimacy, and the push to build adaptive capabilities. Together, they shape how startups deal with cybersecurity regulations and continue to innovate.

Regulatory Landscape Overview

The global landscape of cybersecurity regulation is changing rapidly and getting more complicated. Many countries are making new regulations to address cybersecurity and data protection. For example, in the European Union, the NIS2 Directive builds upon the GDPR by broadening the scope of entities that follow cybersecurity standards and setting stringent requirements for risk management and reporting security incidents (Directive (EU) 2022/2555). In the United States, the regulatory system remains a mix of federal and state laws. While a national law like the American Data Privacy and Protection Act (ADPPA) is still under debate, states like California have already enacted robust laws such as the California Consumer Privacy Act (CCPA) and its amendment, the California Privacy Rights Act (CPRA). In other regions, countries like Brazil (with the LGPD), China (with the PIPL and DSL), and India (with the DPDP Act) have introduced or updated comprehensive data protection and cybersecurity legislations to address the challenges of the digital age (Chander & Le, 2023).

A significant feature of these regulations is that they often apply beyond the borders of the country that created them. For instance, laws like the GDPR and CCPA can affect firms worldwide if they collect or process data from people in the EU or California. This global reach can create considerable challenges for startups that want to grow internationally (Svantesson, 2016). It also raises the issue of harmonization versus fragmentation. While there are efforts to make rules more consistent across nations (like the GDPR's adequacy decisions or the APEC Cross-Border Privacy Rules), the reality is that many countries still have their unique laws. This patchwork environment can make it especially difficult for startups to stay compliant across different regions (Bradford, 2020).

The effect of these regulations varies by sector. In the health technology industry, for example, startups have to follow strict rules such as HIPAA in the U.S. and similar laws in other countries. These rules require companies to protect sensitive patient information by using strong security controls, limiting who can access the data, keep detailed records, and make agreements with third-party vendors that handle health data. As a result, startups often need special infrastructure and expert knowledge, which can shape how they design their products and what kind of data they choose to handle (Cohen & Mello, 2018).

Fintech startups face even more complicated regulations. Besides privacy laws like GDPR and CCPA, they must also follow financial rules to prevent fraud and ensure stability. These include anti-money laundering (AML) and know-your-customer (KYC) requirements, financial reporting standards and cybersecurity rules from regulators such as the New York Department of Financial Services (NYDFS). As a result, fintech startups often need to invest heavily in identity checks, security tools, and systems that monitor activity continuously. This shapes how they build their products and onboard new users (Zetzsche et al., 2020).

Startups in the SaaS and cloud services sector face their unique challenges. They often must follow data sovereignty laws, requiring user data to be stored in specific countries. They also need to sign detailed data processing agreements (DPAs) with clients and may be expected to earn certifications like ISO 27001 or SOC 2 to prove their systems are secure. Serving customers in multiple countries, they often simultaneously deal with different —and sometimes conflicting—regulations (Bradford et al., 2020).

Across all sectors, startups face core regulatory demands that can be tough to meet due to limited resources. One key requirement is to build products with security-by-design and privacy-by-design principles. This means building products with data protection and security in mind from the start, rather than adding them later. Doing this properly often requires changing the mindset and hiring people with the right skills. Another important task is keeping detailed records that show how the company collects and protects data, manages risks, and stays compliant, especially since regulators ask for proof. Startups also rely heavily on third-party services like cloud providers and APIs, but regulations also require them to ensure these partners meet security standards. This adds extra responsibility and a need for careful oversight (ENISA, 2022).

Impacts on Startups

Cybersecurity regulations affect startups in many ways, creating complex challenges and adjustments. The most immediate and often most difficult impact is financial. Startups face high direct costs for compliance, such as paying legal experts in data protection and cybersecurity, hiring consultants to help implement regulatory frameworks, and covering the expenses of certifications like ISO 27001 or SOC 2, which require audits and preparation (Goldfarb & Tucker, 2019).

Beyond direct costs lie significant indirect expenditures. Founders and key technical staff, whose time is crucial for early-stage companies, are diverted from building core products, market research, or acquiring customers to focus on compliance tasks such as drafting policies, implementing controls, and preparing for audits. This shift creates substantial opportunity costs and can delay product launches, giving competitors a chance to get ahead.

Startups may also lose their ability to move quickly. The speed at which startups test, improve, and release products, a key strength, gets slowed down. Using user data, especially for AI or personalized services, becomes more complex and riskier, making innovation harder (Feldstein, 2019). These combined costs can be particularly daunting for pre-revenue or early-stage startups, potentially discouraging innovation in highly regulated industries or forcing startups to shift resources away from growth too early.

Despite the Challenges, regulatory compliance can also bring important benefits to startups. The need to follow regulations often pushes startups to improve their internal capabilities and processes sooner than they might have planned. These startups are forced to adopt more organized methods for managing risks, handling data and preparing for security incidents. This can lead to early use of strong security practices such as regular vulnerability scans, secure coding guidelines, penetration testing and employee training on cybersecurity. While these steps may begin as a response to compliance, they can significantly enhance the startup's overall security and reduce the chance of expensive breaches later on (Romanosky et al., 2019).

Compliance can also help startups build trust. For startups targeting enterprise customers, especially in regulated sectors, having the proper certifications and demonstrating adherence to frameworks like GDPR and HIPAA is often necessary just to be considered a vendor. In this way, compliance becomes a sign of credibility, helping startups stand out from competitors and making it easier to gain partnerships and customers (Benlian et al., 2020).

Cybersecurity regulations significantly influence how startups innovate and where they focus their efforts. On one hand, regulations can limit certain types of innovation. Rapid testing and experimentation, especially those involving user data, such as A/B testing or prototyping, become more complex and legally risky due to strict rules around data minimization and purpose limitation principles. Features that rely on large-scale data collection or creative uses of personal data may face delays, legal reviews, or require complicated consent mechanisms, slowing development and limiting potential product functionalities (Goldfarb & Tucker, 2019).

On the other hand, regulations can also push startups to innovate in new and valuable directions. The pressure to comply often encourages using privacy-enhancing technologies (PETs). Startups are more likely to adopt methods like federated learning (training models without centralizing data), homomorphic encryption (computing on encrypted data), differential privacy (protecting identities by adding noise to data), and zero-knowledge proofs (verifying facts without exposing the data itself) (ICO, 2022).

Regulations can inspire "compliance-driven" innovation, where startups create novel products or services that help other businesses meet regulatory requirements. These include tools for managing user consent, handling data access or deletion requests, monitoring compliance, and specialised secure cloud solutions tailored to regulated industries. Successfully navigating compliance can become a core element of a startup's value proposition and provide a strong competitive edge, especially in markets where trust and security are paramount (Benlian et al., 2020).

The rules and regulations around cybersecurity can also affect the overall market for startups. Strict compliance requirements can make it harder for new companies to enter the market, especially if they lack money or resources. Larger, well-established companies usually have the staff and tools to handle these rules, which gives them an advantage and may reduce competition and fresh ideas in the industry (Crain & Crain, 2014). Because of these challenges, smaller startups might get bought by bigger companies that already meet the rules, or they might choose to work with larger platforms like AWS or Azure that have the needed certifications, making it easier to meet compliance standards. Investors also care a lot about how seriously a startup takes these issues. Venture capitalists and angel investors are more likely to invest in startups that show they are thinking ahead about cybersecurity and data privacy. Startups that follow best practices, like designing systems with security in mind and earning key certifications, are seen as less risky. On the other hand, if a startup ignores compliance, it can scare off investors and make it harder to raise money (Gans et al., 2019).

Case Studies and Empirical Evidence

Examining specific cases shows the varied experiences of startups dealing with cybersecurity regulations. Take a European fintech startup aiming to offer personalized financial management tools using open banking APIs. When the GDPR came into effect, it greatly impacted how the company worked. For example, the rule that users must give explicit and detailed consent meant the company had to redesign its sign-up process, making it longer and possibly causing more users to drop out. Another rule—the “right to be forgotten” (Article 17 of the GDPR)—meant the startup had to build systems that could completely erase a user’s data from all storage, including backups. This was a difficult and time-consuming technical task. The company also had to spend a lot to hire a Data Protection Officer (DPO), either bringing in someone new or using an experienced person from within the team. On top of that, they had to set up strong security measures like encryption for stored and shared data, and detailed logging to meet audit requirements. While these steps helped build user trust and were required by law, they took up money and developer time that the startup planned to use to build new features. As a result, they had to delay launching some of their premium services (Jones & Nguyen, 2021).

A U.S.-based health tech startup building a remote patient monitoring platform offers another clear example. To follow HIPAA rules, the startup had to design its entire tech system around strict privacy and security standards. From the beginning, it had to choose a HIPAA-compliant cloud provider, like AWS, with a signed Business Associate Agreement (BAA), which was more expensive than regular options. HIPAA also shaped decisions about how to store patient data. The startup had to carefully consider keeping raw personal health information (PHI) or only storing de-identified data to reduce risk. Features like secure messaging between doctors and patients required special tools that met HIPAA standards. All this made the development process much longer. The team spent months setting up infrastructure, making legal agreements with every vendor (including data analytics providers), and completing security checks before they could onboard their first patient.

These steps were essential for working in healthcare, but they used up many of the startup’s funds and pushed back key timelines. When it came time to raise money during their Series A round, investors focused heavily on how well the startup handled HIPAA compliance. Showing a solid plan helped attract funding, but it also meant the team had to spend less time developing new medical features early on (Miller & Sharma, 2022).

A SaaS startup offering a project management tool and aiming to grow quickly across the globe faced even more challenges. Dealing with different data privacy laws in various countries became a primary task. To serve customers in the EU, the startup had to fully follow GDPR rules, like managing user consent, handling data access and deletion requests, and running data protection impact assessments for new features. For users in California, it had to meet CCPA/CPRA standards, which required adding features like opt-out buttons and ways to handle deletion requests.

Entering new markets like Brazil and India meant complying with their local laws (the LGPD and the DPDP Act), adding more complexity. To handle all these differences, the company had two choices: either build a very flexible system that could follow different rules depending on the country, or limit market access initially—both of which were expensive options.

The startup had to spend a lot on legal experts to understand the rules and on engineers to build region-specific features. However, it also turned this challenge into a strength. They got ISO 27001 certified and highlighted this on their website and in sales talks, showing they took security and compliance seriously. Offering GDPR-compliant Data Processing Agreements (DPAs) became a selling point, especially when trying to win big European clients. Even though staying compliant took a lot of time and money, the startup used it to stand out. It helped them win the trust of large companies that cared deeply about data protection and were willing to pay more. Still, keeping up with changing laws required ongoing effort (Bradford et al., 2020).

Balancing Compliance and Innovation

Startups are not just victims of strict cybersecurity rules—they are actively finding ways to meet these demands while being innovative. One smart approach many startups use is to include compliance planning right from the beginning of product development. Instead of later adding security and privacy features, they build them using *security-by-design* and *privacy-by-design* principles. This means doing things like:

1. Running *Data Protection Impact Assessments (DPIAs)* early for new features,
2. Using *privacy-enhancing technologies (PETs)* in the product's structure,
3. Following secure software development practices, including threat modelling and regular security tests (ENISA, 2022; ICO, 2022).

By designing their products with compliance in mind, startups avoid costly changes later and build more secure, trustworthy products from the beginning.

Innovative startups treat compliance as a selling point, not just a burden. Certification (e.g., ISO 27001; SOC 2, or industry-specific standards) shows they take security seriously. These certifications are proudly displayed in marketing materials, sales talks, and investor presentations to build trust and attract enterprise customers (Benlian et al., 2020).

Since building a complete compliance system in-house can be too much for a small team, many startups work with big tech providers. By building on platforms like AWS, Azure, or Google Cloud, they can benefit from these companies' built-in security and compliance certifications. They also use third-party services for specific tasks—like secure payment processing or consent management—to focus on their main product while leaving complex regulatory tasks to experts (Bradford et al., 2020).

The broader startup ecosystem also helps. Incubators and accelerators now offer legal guidance, workshops on GDPR and HIPAA, and connections to compliance experts. This support helps new startups understand and practically apply the rules (OECD, 2023).

New tools are also making things easier. Now, software platforms automate many compliance tasks, like managing user consent, handling data deletion requests, assessing vendor risks, and generating policy documents. These tools reduce the time, effort, and cost of staying compliant, although some expert help is still needed (Goldfarb & Tucker, 2019).

Standardized legal tools are another big help. Using things like Standard Contractual Clauses (SCCs) for sending data internationally under GDPR, or pre-approved Data Processing Agreements (DPAs) from cloud providers, makes legal compliance faster and easier.

For policymakers, the main challenge is to write cybersecurity laws that protect people and data *without* placing such heavy demands on startups that it kills innovation. This means making the rules proportional, scaled according to the company's size, risk, and activity. Instead of applying the same complex rules to global corporations and small startups, governments should consider lighter or simplified rules for small or low-risk businesses. Risk-based regulation—focusing strict rules only on the most sensitive or dangerous data uses—is key to finding the right balance (OECD, 2023).

Policy and Regulatory Implications

The impact of cybersecurity regulations on startups points to several important areas that policymakers should consider when designing future rules. One of the main goals should be to reduce the early-stage burden and uncertainty that new startups face. One helpful tool is the idea of *regulatory sandboxes*, which were first introduced by financial regulators like the UK's Financial Conduct Authority (FCA). These sandboxes let startups—especially in fintech, and health-tech—test their new products, services, or business models with real users under relaxed or temporary regulatory rules. This helps startups learn and grow without fully meeting all legal requirements right away (Zetzsche et al., 2020). Another helpful idea is *safe harbor* provisions, which protect startups from heavy penalties if they make honest efforts to follow the law. If a startup is still growing but trying in good faith to comply, these protections can encourage innovation without putting users at risk.

Startups also need more precise and easier-to-understand guidance. Regulators should create simple explanations of legal requirements, standard forms and templates (like those for Data Protection Impact Assessments or privacy notices), and checklists designed specifically for small companies. Help-desks or support center's that answer questions can also make a big difference. Cutting down on paperwork, making it easier to submit reports online or reducing how often they need to file can help startups focus more on building their products (OECD, 2023).

When it comes to *international rules*, the picture is more mixed. Having common standards across countries can help startups grow globally. Things like mutual

recognition of certifications (for example, an ISO 27001 certificate that works in more than one country), agreements on data protection (like the GDPR's adequacy decisions), and shared principles through groups like the OECD can reduce the cost and complexity of following different laws in different places (Bradford, 2020).

But accurate global alignment is hard to achieve. Big economies often have conflicting rules, such as differences in how they handle data storage or government access to user data. This leaves startups stuck, limiting where they do business, or spending much money creating separate systems for each region. A more realistic solution might be to push for *smaller agreements* between countries with similar values to reduce the patchwork of rules start-ups must follow.

Besides formal laws, industry standards and self-regulation can also help. Creating widely accepted codes of conduct—with input from businesses, consumer groups, and regulators—can give industries flexible but clear guidance tailored to their needs (Bamberger & Mulligan, 2015). Certification programs based on global standards like ISO 27001 can help companies show they are doing the right thing and earn customer trust.

However, self-regulation only works if there is strong oversight. Without it, there is a risk that companies will cut corners to save costs. It is also important to have strong partnerships between the public and private sectors. These partnerships can help share cyber threat information, build useful tools and advice, and ensure new rules are grounded in how things work. This makes regulations more effective and workable for everyone, especially startups with limited resources (ENISA, 2022).

Conclusion

The link between cybersecurity rules and startup innovation is both complicated and full of trade-offs. On one hand, strong regulations are essential to protect people, digital systems, and the broader economy. But at the same time, these rules often place a heavy burden on startups. The costs of legal advice, certifications, and time spent on compliance—rather than building products—can delay product launches, reduce experimentation, and use up limited resources. For startups in tightly regulated fields like fintech and health-tech, this can make it even harder to grow. The case studies clearly show how regulations affect everything from product design to company strategy during the critical early stages of development.

Still, not all impacts are negative. Regulations can also push startups to grow in productive ways. Being forced to comply with strict rules can lead startups to adopt strong security practices, improve internal processes, and gain early experience in managing risk and handling data responsibly. These steps can make startups more resilient and professional over time. Regulations can even point the way toward new types of innovation, like technologies that protect user privacy (such as federated learning or homomorphic encryption) or new tools that help automate compliance tasks. Following the rules well can also build trust with customers, especially in sectors where showing strong security standards is important. For investors, startups that handle compliance well are often seen as less risky and more mature.

The most important takeaway is that regulations don't simply block or enable innovation; they *reshape* it. They close off some options (like experimenting freely with user data) but also highlight or open up others (like privacy-focused innovation or compliance-as-a-service). They require startups to build security and privacy into the core of their business strategy. To succeed, startups need to treat compliance not just as an obligation, but as something that adds value and improves their chances of long-term survival. For policymakers, the challenge is finding a balance: protecting people and systems without crushing the creative energy and growth potential of startups. To strike this balance, future rules must be flexible, scalable, and supportive, offering clear guidance, simplified procedures, and tools like regulatory sandboxes and international cooperation.

This research helps show how deeply cybersecurity regulations shape the startup world, affecting costs, direction, products, and market strategy. It shows the trade-offs startups face, and how they adapt to survive and thrive in a rule-heavy environment. Going forward, more research is needed to better understand these effects. For example, long-term studies could track how different regulations affect startup survival and growth. Comparative research could dig deeper into the specific challenges faced by startups in fields like health-tech or cleantech. Data-driven studies could measure how much of a startup's R&D budget goes toward compliance. And new research into privacy-enhancing technologies and AI's role in making compliance easier could help guide both startups and regulators. Understanding these issues is key to creating an ecosystem where both innovation and digital security can grow side by side.

References

[1] Bamberger, K. A., & Mulligan, D. K. (2015). Privacy on the ground: Driving corporate behaviour in the United States and Europe. MIT Press.

[2] Benlian, A., Kettinger, W. J., Sunyaev, A., Winkler, T. J., & Wulf, J. (2020). Signalling value through regulatory certification: Evidence from the GDPR. Journal of Management Information Systems, *37*(3), 725-757. https://doi.org/10.1080/07421222.2020.1790183

[3] Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press.

[4] Bradford, A., Chilton, A. S., Linos, K., & Weaver, A. (2020). The global dominance of European data privacy regulation. Virginia Journal of International Law, *61*(1), 1-70. https://doi.org/10.2139/ssrn.3522675

[5] Chander, A., & Le, U. P. (2023). Data nationalism 2.0. Texas Law Review, *101*(forthcoming). https://doi.org/10.2139/ssrn.4097250

[6] Cohen, I. G., & Mello, M. M. (2018). HIPAA and protecting health information in the 21st century. JAMA, *320*(3), 231-232. https://doi.org/10.1001/jama.2018.5630

[7] Crain, W. M., & Crain, N. V. (2014). The cost of federal regulation to the U.S. economy, manufacturing and small businesses. National Association of Manufacturers. https://www.nam.org/uploadedFiles/Website/Content_Pages/News/Section_Contents/News_Articles/The_Cost_of_Federal_Regulation.pdf

[8] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333, 80-152. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

[9] ENISA. (2022). Startup security: Cybersecurity challenges and opportunities for startups and SMEs. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/startup-security

[10] Feldstein, S. (2019). The road to digital unfreedom: How artificial intelligence is reshaping repression. Journal of Democracy, *30*(1), 40–52. https://doi.org/ 10.1353/jod.2019.0004

[11] Gans, J. S., Stern, S., & Wu, J. (2019). Foundations of entrepreneurial strategy. Strategic Management Journal, *40*(5), 736-756. https://doi.org/10.1002/smj.3010

[12] Goldfarb, A., & Tucker, C. (2019). Digital economics. Journal of Economic Literature,57*(1), 3-43. https://doi.org/10.1257/jel.20171452

[13] ICO. (2022). Privacy-enhancing technologies (PETs). Information Commissioner's Office (UK). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/privacy-enhancing-technologies-guidance/

[14] Jones, C., & Nguyen, D. (2021). The impact of GDPR on fintech startup innovation: Evidence from Europe. Journal of Financial Transformation, *53*, 103-115. https://ssrn.com/abstract=3789265

[15] Lewis, J. A. (2018). Economic Impact of Cybercrime – No Slowing Down. Center for Strategic & International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

[16] Miller, R., & Sharma, P. (2022). Navigating HIPAA compliance: Challenges and strategies for digital health startups. Health Affairs, *41*(8), 1190-1197. https://doi.org/10.1377/hlthaff.2021.01945

[17] OECD. (2023). The impact of regulation on innovation. OECD Innovation Policy Papers. https://www.oecd.org/innovation/the-impact-of-regulation-on-innovation-92b7d3e7-en.htm

[18] OECD/Eurostat. (2018). Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation (4th ed.). OECD Publishing. https://doi.org/10.1787/9789264304604-en

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on protecting natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[20] Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cybersecurity policies. Journal of Cybersecurity, *5*(1), tyz002. https://doi.org/10.1093/cybsec/tyz002

[21] Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. Academy of Management Review, *20*(3), 571–610. https://doi.org/10.5465/amr.1995.9508080331

[22] Svantesson, D. J. B. (2016). Solving the Internet Jurisdiction Puzzle. Oxford University Press.

[23] Teece, D. J., Pisano, G., &Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, *18*(7), 509-533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z

[24] Zetzsche, D. A., Buckley, R. P., Barberis, J. N., & Arner, D. W. (2020). Regulating a revolution: From regulatory sandboxes to smart regulation. Fordham Journal of Corporate & Financial Law, *23*(1), 31-103. https://ssrn.com/abstract=3018534