The Legal Framework for Managing Cybersecurity Risks in Financial Institutions

1. Anjali Sharma*: Department of International Trade Law, University of Delhi, Delhi, India

***Correspondence: e-mail: Anjalisharm15@gmail.com**

Abstract

Cybersecurity risks in financial institutions have become an increasingly significant concern as the sector continues to embrace digital technologies. With the rise of online banking, mobile payments, and cloud computing, financial services are more vulnerable than ever to a wide array of cyber threats, including hacking, phishing, ransomware, and data breaches. This narrative review examines the current legal frameworks in place to manage cybersecurity risks within the financial sector, analyzing both international and national regulations, as well as sector-specific guidelines. The article explores the challenges financial institutions face in maintaining robust cybersecurity practices, including the complexity of governance, the tension between innovation and security, the shortage of skilled cybersecurity professionals, and the jurisdictional issues arising from cross-border operations. It also discusses the vital role of financial supervisory bodies in guiding institutions through these challenges, fostering collaboration, and ensuring compliance with cybersecurity standards. As the threat landscape evolves, the review suggests several future directions for enhancing cybersecurity legal frameworks, including the integration of AI-based security systems, blockchain applications, and real-time risk monitoring. Recommendations are provided for improving legal structures by strengthening enforcement mechanisms, harmonizing international regulations, and ensuring the continuous adaptation of frameworks to address emerging threats. The article concludes by emphasizing the need for ongoing collaboration between financial institutions, regulators, and industry bodies to ensure the cybersecurity resilience of the financial sector, stressing the importance of a proactive and adaptive legal approach.

Keywords: Cybersecurity, financial institutions, legal frameworks, data breaches, AI-based security, international regulations

Received: 03 May 2024
Revised: 14 June 2024
Accepted: 20 June 2024
Published: 01 July 2024

Citation: Sharma, A. (2024). The Legal Framework for Managing Cybersecurity Risks in Financial Institutions. *Legal Studies in Digital Age*, 3(3), 8-14.

1. Introduction

In recent years, financial institutions have experienced a profound transformation due to the increasing reliance on digital platforms. The integration of technologies like online banking, mobile payments, cloud computing, and blockchain has redefined the way financial services are delivered and consumed. These digital advancements have not only enhanced the efficiency of financial transactions but also expanded access to financial services on a global scale. However, this digitalization has also brought about a significant shift in the risk landscape. Cybersecurity threats have escalated as financial institutions become prime targets for malicious actors seeking to exploit vulnerabilities in digital infrastructures. The rise in cyberattacks, ranging from data breaches and ransomware attacks to sophisticated financial fraud schemes, has highlighted the need for

robust cybersecurity measures in this sector. As financial systems continue to intertwine with digital technologies, the scale and sophistication of these cyber threats are expected to grow, placing even greater pressure on institutions to safeguard their operations, data, and customers. This growing threat landscape makes it increasingly difficult for financial institutions to remain resilient in the face of constant and evolving cyber risks (Crum & Merlo, 2020).

The importance of cybersecurity in financial institutions cannot be overstated. Financial systems are critical to the functioning of economies, and any disruption can have far-reaching consequences, not just for the institutions themselves but for the broader economic system. A successful cyberattack can compromise sensitive financial data, disrupt banking operations, and result in financial losses, affecting customers, employees, and stakeholders. Given the central role that financial institutions play in global commerce, their vulnerability to cyberattacks poses a serious threat to economic stability. In response to these rising risks, financial institutions have begun investing heavily in cybersecurity technologies, including encryption, multi-factor authentication, and advanced threat detection systems. However, technological solutions alone are not sufficient to protect against the myriad of cybersecurity threats. A comprehensive approach that includes not only technical measures but also legal and regulatory frameworks is essential for managing these risks effectively (Grzybowski, 2019).

Legal frameworks serve as the backbone for ensuring that financial institutions take the necessary steps to mitigate cybersecurity risks. A well-designed legal structure provides the foundation for establishing clear security requirements, promoting compliance with cybersecurity standards, and ensuring accountability when institutions fail to protect their systems adequately. Financial institutions must adhere to various regulations that mandate the implementation of robust cybersecurity protocols to safeguard sensitive financial data and customer information. Without a solid legal framework, financial institutions may fail to prioritize cybersecurity, leaving them vulnerable to attacks. Furthermore, the dynamic nature of cyber threats requires that legal frameworks be adaptable and responsive to emerging risks. Cybercriminals are continually developing new strategies to bypass security measures, making it imperative for laws and regulations to evolve in tandem with technological advancements. By establishing mandatory cybersecurity practices, facilitating information-sharing between institutions, and creating mechanisms for enforcement, legal frameworks play a pivotal role in protecting the financial sector from cyber threats (Bytyci & Phillips, 2017).

This article aims to explore the legal frameworks in place for managing cybersecurity risks in financial institutions. The review will provide a comprehensive analysis of current regulatory structures, their effectiveness, and the challenges that institutions face in complying with these regulations. One of the primary objectives of this article is to evaluate the robustness of existing legal mechanisms, such as data protection laws, cybersecurity directives, and financial regulatory frameworks, and to assess whether they adequately address the complexities of the evolving cyber threat landscape. Additionally, the article will examine the gaps in current legal frameworks, considering factors such as jurisdictional challenges, the lack of uniformity in cybersecurity regulations across borders, and the difficulties institutions encounter in balancing legal compliance with operational efficiency. Through this examination, the review will offer insights into the effectiveness of legal frameworks in mitigating cybersecurity risks and explore potential recommendations for strengthening these frameworks to ensure the resilience of financial institutions in the digital age (Beijerman, 2018).

Given the complex and dynamic nature of cybersecurity risks in the financial sector, this article will not only focus on the current state of legal regulations but also highlight the emerging trends and future challenges. The rapid pace of technological innovation, coupled with increasingly sophisticated cyber threats, demands that legal frameworks be continuously updated and re-evaluated. The article will explore the intersection of law and technology, examining how legal institutions can adapt to better support the cybersecurity needs of financial institutions. Ultimately, the goal is to provide a critical understanding of the current legal landscape, its effectiveness, and its potential for improvement, ensuring that financial institutions are better equipped to manage cybersecurity risks in a rapidly evolving digital environment.

2. Background: Cybersecurity in Financial Institutions

The integration of technology into financial services has transformed the industry over the past few decades, leading to a more efficient and accessible financial ecosystem. The rise of online banking, mobile payments, and digital wallets has allowed customers to access and manage their finances from anywhere in the world. Cloud services have further expanded the scope of financial services, enabling institutions to store vast amounts of data and facilitate the rapid processing of transactions.

However, these technological advancements have also given rise to a growing range of cybersecurity risks. As financial institutions increasingly rely on digital infrastructures, they have become prime targets for cybercriminals. Online banking, for example, while making it easier for users to access their accounts, has also opened the door to hacking attempts, phishing scams, and other cyberattacks. Cloud computing, though offering scalability and cost-effective storage solutions, has introduced concerns over data breaches and unauthorized access to sensitive financial data. The increased use of mobile payment platforms, while boosting convenience for consumers, has also exposed vulnerabilities in mobile applications, putting users at risk of fraud. The evolution of these technologies, therefore, has created new challenges for financial institutions in securing their systems and data (Beijerman, 2018).

Cybersecurity threats in the financial sector are diverse and ever-evolving. One of the most common threats is hacking, where cybercriminals attempt to exploit vulnerabilities in a financial institution's digital infrastructure to gain unauthorized access to sensitive information. Hacking attempts can lead to massive data breaches, theft of personal financial data, and the compromise of internal systems. Phishing attacks, another prevalent threat, involve cybercriminals attempting to trick individuals into revealing sensitive information such as passwords, account numbers, or credit card details through deceptive emails or websites. These attacks often rely on social engineering tactics to exploit the trust of users. Ransomware attacks, in which cybercriminals hold a financial institution's systems hostage and demand payment for their release, have become increasingly common. These attacks can disrupt operations, cause financial losses, and tarnish an institution's reputation. Insider threats, posed by employees or contractors with access to sensitive data, are also a significant concern. These individuals may intentionally or unintentionally leak confidential information or compromise systems. Data breaches, which occur when sensitive information is exposed to unauthorized individuals, are another major threat that financial institutions must address. These breaches can result in severe financial and reputational damage, as well as regulatory penalties if data protection laws are violated (Crum & Merlo, 2020).

The consequences of cybersecurity incidents for financial institutions are far-reaching and often devastating. Financial losses are one of the most immediate effects of a successful cyberattack. Institutions may face direct financial damages, including the costs of resolving the attack, compensating affected customers, and covering legal fees. Additionally, a cyberattack can result in long-term financial losses due to decreased customer trust, reduced business, and the potential for regulatory fines. Reputational damage is another significant consequence. Customers rely on financial institutions to safeguard their sensitive information, and a breach of that trust can lead to a loss of business and a tarnished reputation. The negative impact on an institution's reputation may result in customers switching to competitors, as they seek greater assurance that their data is secure. Moreover, cybersecurity failures can lead to regulatory fines and legal actions. Financial institutions are often required to comply with various data protection and cybersecurity regulations. Failure to adhere to these regulations, especially when an attack exposes sensitive data, can result in substantial penalties. Regulatory bodies may impose fines, mandate corrective actions, and even take legal action against institutions that fail to meet cybersecurity requirements (Bytyci & Phillips, 2017).

3. Legal and Regulatory Frameworks

As the risks associated with cybersecurity continue to grow, so too has the need for a strong legal and regulatory framework to guide financial institutions in managing these risks. The international legal landscape surrounding cybersecurity has evolved in response to the increasing threats facing the financial sector. One of the key international instruments governing cybersecurity is the General Data Protection Regulation (GDPR) implemented by the European Union. While primarily focused on data protection, the GDPR imposes stringent requirements on financial institutions regarding the handling of personal data, including obligations to implement appropriate security measures to protect against data breaches. The regulation mandates that institutions notify authorities and affected individuals in the event of a breach, ensuring transparency and accountability. The EU’s Network and Information Systems (NIS) Directive also plays a significant role in cybersecurity, setting out security requirements for essential services, including financial services. This directive aims to enhance the overall level of cybersecurity across the EU by requiring organizations to take measures to prevent and respond to cyber incidents. Similarly, the European Union's Cybersecurity Act establishes a framework for strengthening cybersecurity across the union, including the establishment of a certification framework for information and communications technology (ICT) products, services, and processes, which impacts financial institutions (Sadat Bidgoli, 2023).

National regulations play a crucial role in shaping the cybersecurity practices of financial institutions. In the United States, the Gramm-Leach-Bliley Act (GLBA) requires financial institutions to implement safeguards to protect the confidentiality and security of customers' personal financial information. The GLBA mandates that institutions conduct regular risk assessments, implement security measures, and provide customers with privacy notices. The Dodd-Frank Act, passed in the wake of the 2008 financial crisis, includes provisions that enhance the ability of regulators to oversee and enforce cybersecurity practices in financial institutions. The act also established the Consumer Financial Protection Bureau (CFPB), which has the authority to regulate data security standards for consumer financial products. Additionally, agencies such as the Federal Reserve and the Securities and Exchange Commission (SEC) play a significant role in enforcing cybersecurity standards for financial institutions. The SEC, for example, has issued guidance on the disclosure of cybersecurity risks and incidents by publicly traded companies, including financial institutions. These regulations work together to create a comprehensive framework for ensuring that financial institutions adopt effective cybersecurity measures to protect their systems and data (Grzybowski, 2019).

Financial institutions are also subject to sector-specific regulations that tailor cybersecurity requirements to the unique risks of the financial industry. The Basel III guidelines, established by the Basel Committee on Banking Supervision, provide a comprehensive framework for managing financial risk, including cybersecurity risk. These guidelines emphasize the importance of effective risk management practices and require institutions to have robust systems in place to protect against cyber threats. The Federal Financial Institutions Examination Council (FFIEC) has developed the Cybersecurity Assessment Tool, which helps financial institutions assess their cybersecurity posture and identify areas for improvement. The tool is designed to help institutions understand the evolving threat landscape and implement appropriate risk management strategies. Compliance with these sector-specific regulations is essential for ensuring that financial institutions are adequately prepared to face cybersecurity challenges (Sadat Bidgoli, 2023).

Compliance with cybersecurity regulations is not optional for financial institutions; it is a legal requirement. Institutions must adhere to a complex web of regulations, both at the national and international levels, to avoid legal consequences, including fines and penalties. Compliance involves implementing robust security protocols, conducting regular audits, and ensuring that employees are trained in cybersecurity best practices. Institutions must also be prepared to report any cybersecurity incidents promptly and transparently to the relevant authorities. The failure to comply with these regulations can result in significant legal and financial penalties, as well as reputational damage. The ever-changing nature of cybersecurity risks means that financial institutions must continuously update their security practices to remain compliant with evolving regulations. Regular risk assessments, system upgrades, and staff training are critical components of maintaining compliance with the regulatory frameworks that govern cybersecurity in the financial sector (Beijerman, 2018).

4. Challenges in Managing Cybersecurity Risks in Financial Institutions

The complexity of managing cybersecurity risks in financial institutions arises from the ever-changing nature of cyber threats. Financial systems are highly interconnected, making them more vulnerable to cyberattacks, which are constantly evolving in sophistication and scale. Cybercriminals continuously develop new tactics to bypass security measures, often exploiting previously unknown vulnerabilities. As financial institutions adopt new technologies to streamline their operations, the attack surface expands, providing additional points of entry for hackers. This dynamic and unpredictable landscape makes it difficult to create a cohesive cybersecurity strategy that remains effective over time. Institutions are often left scrambling to address new threats as they emerge, struggling to maintain a balance between keeping up with technological advancements and safeguarding against the latest forms of cyberattacks. Furthermore, the integration of multiple technologies, such as cloud services, mobile banking platforms, and artificial intelligence, into financial operations complicates risk management. Each technology comes with its own set of security challenges, and managing these disparate elements in a unified cybersecurity strategy requires significant coordination, expertise, and resources (Crum & Merlo, 2020).

Another significant challenge faced by financial institutions in managing cybersecurity risks is the tension between adopting new technologies and ensuring adequate security measures. The financial sector is under constant pressure to innovate in order to remain competitive and meet the growing expectations of customers for fast, efficient, and convenient services. However, the rapid adoption of new technologies often outpaces the development of corresponding security measures. For instance, mobile banking applications, while enhancing customer convenience, are also prone to security vulnerabilities, such as weak

encryption protocols or flaws in authentication systems. Blockchain technology, although offering promising advancements in financial transactions, has raised concerns regarding the security of smart contracts and the potential for cyberattacks on decentralized systems. This tension between innovation and security is not unique to financial institutions but is particularly acute in the sector due to the sensitive nature of the data involved. Financial institutions are compelled to strike a delicate balance between implementing cutting-edge technologies and maintaining rigorous security standards to protect customer data and assets (Beijerman, 2018).

The shortage of skilled cybersecurity professionals is another pressing issue facing financial institutions. The increasing complexity of cybersecurity threats requires a specialized workforce capable of implementing and managing sophisticated security systems. However, the demand for cybersecurity experts far exceeds the supply, particularly in the financial sector, where the stakes are higher. This shortage of qualified professionals creates significant gaps in the cybersecurity strategies of many financial institutions. With fewer experts available, organizations may struggle to adequately address emerging risks or respond to incidents in a timely manner. Additionally, the lack of skilled personnel often leads to overburdened staff, increasing the likelihood of human error or oversight in security protocols. Financial institutions may be forced to allocate resources to other areas, such as business development or customer service, leaving cybersecurity as a lower priority. The cybersecurity skills gap has become a critical challenge, and its resolution is essential for improving the resilience of financial institutions against cyber threats (Sadat Bidgoli, 2023).

Jurisdictional issues present another significant challenge in managing cybersecurity risks for financial institutions operating across borders. The global nature of financial markets means that institutions often have operations, clients, and data spread across multiple jurisdictions. Each jurisdiction has its own set of cybersecurity laws and regulations, which can differ significantly in terms of scope, enforcement, and penalties. This lack of uniformity creates difficulties for financial institutions in establishing a consistent cybersecurity strategy that complies with all applicable laws. For example, an institution operating in both the European Union and the United States must navigate the complexities of the EU's General Data Protection Regulation (GDPR) and the U.S. Gramm-Leach-Bliley Act (GLBA), which may have conflicting requirements. In addition to legal discrepancies, cross-border data transfers present security risks, as institutions must ensure that data is securely handled in accordance with local laws, especially when data is transferred between countries with differing data protection standards. The absence of a harmonized global cybersecurity framework further complicates efforts to mitigate risks effectively, requiring financial institutions to invest in legal counsel and compliance officers to ensure they meet all regulatory obligations (Grzybowski, 2019).

The evolving nature of cyber threats means that current legal frameworks often struggle to keep up with new risks. While existing regulations and standards provide a foundation for cybersecurity management, they are often reactive rather than proactive. Cybercriminals are quick to exploit vulnerabilities, and financial institutions must constantly adapt their security measures to stay ahead. This dynamic threat landscape requires legal frameworks to be flexible and adaptable, but many existing regulations are slow to evolve. For example, the legal framework surrounding the use of emerging technologies, such as artificial intelligence and machine learning, in financial services is still in its infancy. As these technologies become more integrated into financial systems, they may introduce new vulnerabilities that current laws are ill-equipped to address. The gap between the speed of technological innovation and the pace of legal adaptation poses a significant challenge in effectively managing cybersecurity risks in the financial sector (Bytyci & Phillips, 2017).

5. The Role of Financial Supervisory Bodies in Cybersecurity

Financial supervisory bodies play a crucial role in overseeing and guiding financial institutions in managing cybersecurity risks. These regulatory authorities, both at the national and international levels, are responsible for ensuring that financial institutions comply with cybersecurity standards and take appropriate measures to protect against cyber threats. In many countries, regulatory bodies such as the Federal Reserve in the United States and the European Central Bank (ECB) have established frameworks and guidelines to promote cybersecurity resilience in the financial sector. These organizations provide oversight and set the expectations for institutions to implement robust cybersecurity strategies, conduct regular risk assessments, and ensure that systems are regularly updated to address emerging threats. By establishing clear guidelines and

monitoring compliance, financial supervisory bodies help to create a standardized approach to cybersecurity risk management across the sector, ensuring that institutions take the necessary steps to protect their operations and data (Sadat Bidgoli, 2023).

Regulatory guidance and frameworks issued by supervisory bodies provide the essential framework for financial institutions to follow in their cybersecurity efforts. For example, the ECB's Cyber Resilience Oversight Expectations set out clear guidelines for financial institutions to follow in developing and maintaining cybersecurity frameworks. These expectations include measures for identifying, assessing, and managing cybersecurity risks, as well as guidelines for incident reporting, recovery, and communication with stakeholders. Similarly, regulatory bodies often provide frameworks for financial institutions to assess their own cybersecurity posture, such as the Federal Financial Institutions Examination Council's Cybersecurity Assessment Tool in the U.S. These frameworks enable institutions to evaluate their readiness to face cyber threats and identify areas for improvement. By offering detailed and structured guidance, supervisory bodies help financial institutions establish cybersecurity measures that are aligned with regulatory requirements and industry best practices (Crum & Merlo, 2020).

Collaboration between financial regulators, financial institutions, and other industry stakeholders is essential to enhancing cybersecurity resilience. Many regulators encourage collaboration through information-sharing initiatives, where institutions can share threat intelligence and best practices for mitigating cybersecurity risks. By working together, financial institutions and regulators can identify emerging threats, strengthen defenses, and improve incident response strategies. Industry bodies, such as financial industry associations and cybersecurity consortiums, also play a key role in promoting collaboration and facilitating the exchange of knowledge and resources. This collaborative approach allows financial institutions to benefit from a collective understanding of the threat landscape and work together to enhance the sector's overall resilience to cyberattacks. Regulatory bodies also facilitate this collaboration by hosting workshops, seminars, and conferences to raise awareness about cybersecurity risks and foster dialogue between industry players. Ultimately, a coordinated approach that involves regulators, institutions, and industry bodies can help ensure that the financial sector is better prepared to face the evolving challenges of cybersecurity (Beijerman, 2018).

6. Future Directions and Recommendations

The legal landscape surrounding cybersecurity in financial institutions is rapidly evolving in response to emerging technologies and the increasingly complex nature of cyber threats. One of the most significant future trends in cybersecurity regulation is the growing incorporation of artificial intelligence (AI) and machine learning (ML) into security frameworks. AI-based security systems have the potential to revolutionize how financial institutions detect and respond to threats. These systems can analyze vast amounts of data in real-time, identifying patterns of suspicious activity and predicting potential threats before they manifest. As AI becomes more integrated into financial systems, it will likely become a key component of legal frameworks, requiring regulators to establish guidelines for the ethical use of AI in cybersecurity and address concerns regarding accountability, transparency, and privacy. Blockchain technology is another area that is expected to play a larger role in cybersecurity regulation. Blockchain's decentralized nature and its ability to provide secure, transparent transaction records make it an attractive tool for improving data integrity and reducing fraud in financial systems. However, the adoption of blockchain also introduces new regulatory challenges, particularly around data privacy and cross-border transactions. Real-time risk monitoring is another emerging trend that is likely to shape future cybersecurity regulation. Financial institutions will need to implement more sophisticated tools to continuously monitor their systems for vulnerabilities and threats, requiring regulatory frameworks to address the standards and practices for such monitoring (Grzybowski, 2019).

In order to strengthen legal frameworks for managing cybersecurity risks, several recommendations can be made. First, regulators should enhance existing regulations by updating them to better address emerging technologies, such as AI and blockchain, and the specific risks associated with these technologies. It is essential that legal frameworks remain flexible to accommodate the rapid pace of technological change while ensuring that security and privacy standards are met. Second, enforcement mechanisms should be strengthened to ensure compliance with cybersecurity regulations. This can include increasing penalties for non-compliance, enhancing the capacity of regulatory bodies to conduct audits and investigations, and improving transparency in reporting cybersecurity incidents. Third, international cooperation must be prioritized to address the challenges posed by cross-border cybersecurity risks. With financial institutions operating across multiple jurisdictions,

regulatory bodies should work together to harmonize cybersecurity standards, share threat intelligence, and collaborate on incident response. International treaties or agreements could facilitate this cooperation, ensuring that institutions comply with consistent security standards regardless of where they operate (Beijerman, 2018).

Finally, the need for continuous adaptation of legal and regulatory frameworks cannot be overstated. Cybersecurity is an ongoing challenge that requires a dynamic and forward-looking approach. Legal frameworks must evolve in response to new technologies, emerging threats, and changing geopolitical landscapes. This will involve continuous engagement with industry stakeholders, regular updates to regulations, and proactive measures to anticipate future risks. Financial institutions, regulators, and industry bodies must work together to foster a culture of cybersecurity resilience, where legal and regulatory responses are agile and capable of addressing the evolving nature of cyber threats (Bytyci & Phillips, 2017).

7. Conclusion

In conclusion, the importance of a robust legal framework for managing cybersecurity risks in financial institutions cannot be overstated. As technology continues to shape the financial sector, the need for effective cybersecurity regulation becomes even more critical. This article has discussed the growing cybersecurity threats faced by financial institutions, the legal frameworks currently in place, and the challenges associated with managing these risks. It has also highlighted the need for continuous adaptation of legal structures to stay ahead of emerging technologies and evolving threats. Strengthening enforcement mechanisms, enhancing international cooperation, and updating legal frameworks to address new risks are essential steps in improving cybersecurity resilience in the financial sector. Ultimately, a forward-looking and collaborative approach will be crucial in ensuring that the financial industry can navigate the complex landscape of cybersecurity while protecting sensitive data and maintaining trust (Crum & Merlo, 2020).

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Beijerman, M. (2018). Conceptual confusions in debating the role of NGOs for the democratic legitimacy of international law. Transnational Legal Theory, 9(2), 147-173.

Bytyci, F., & Phillips, D. L. (2017). State-building and the making of democracy: Kosovo in comparative perspective. Journal of Balkan and Near Eastern Studies, 19(1), 68-86.

Crum, B., & Merlo, S. (2020). Democratic legitimacy in the post-crisis EMU. Journal of European Integration, 42(3), 399-413.

Grzybowski, J. (2019). The paradox of state identification: De facto states, recognition, and the (re-)production of the international. International Theory, 11, 241–263.

Sadat Bidgoli. (2023). An analysis of the challenge of legitimacy of Ashraf Ghani's government. Iranian History Journal, 16(2), 225-246.

Beijerman, M. (2018). Conceptual confusions in debating the role of NGOs for the democratic legitimacy of international law. Transnational Legal Theory, 9(2), 147-173.

Crum, B., & Merlo, S. (2020). Democratic legitimacy in the post-crisis EMU. Journal of European Integration, 42(3), 399-413.

Grzybowski, J. (2019). The paradox of state identification: De facto states, recognition, and the (re-)production of the international. International Theory, 11, 241–263.