THE IMPACT OF EU LEGISLATIVE REGULATIONS ON ACCELERATING THE DIGITALIZATION OF BANKING SERVICES

Mugurel Petre PODARU [a]*, Răzvan Cătălin DOBREA [a], Dragoș-Daniel DENDRINO [a], Loredana Gabriela DINULESCU [a]

[a] Bucharest University of Economic Studies, Romania

ABSTRACT

The digital transformation of the European banking sector results from the connection between technological advancements and regulatory interventions aimed at ensuring financial stability, consumer protection, and the promotion of innovation. This article examines the convergent impact of key regulations on the banking business model, technological infrastructure, and customer relationships. The PSD2 Directive has laid the groundwork for the development of open banking, prompting financial institutions to reposition themselves in relation to new actors within the fintech ecosystem. The eIDAS Regulation has contributed to establishing a trusted framework for the use of electronic identity and trust services, thereby facilitating process automation and digital onboarding. The requirements imposed by the Basel III Accord have accelerated the adoption of advanced technological solutions for managing systemic risks and enhancing the resilience of financial institutions. The GDPR Regulation has introduced new standards for data governance, with significant implications for the collection, storage, and use of personal information. Moreover, the proliferation of regulatory sandbox environments has provided an experimental framework that supports the testing and validation of financial innovations in a controlled setting, fostering a flexible and adaptive approach to regulation. The paper proposes an integrative perspective on these factors, highlighting the role of regulation as a strategic driver of digital transformation in banking.

KEYWORDS: *Basel III, digital banking, eIDAS, GDPR, PSD2.*

DOI: 10.24818/IMC/2025/01.05

1. INTRODUCTION

The digital transformation of the banking sector is one of the most profound and rapid shifts in recent decades, reshaping business models, operational infrastructures, and client engagement practices. In an environment marked by emerging technologies and rising customer expectations, financial institutions must adapt quickly to remain competitive. This transformation is not driven solely by market dynamics or technological innovation, but also by regulatory actions aimed at balancing innovation, financial stability, and consumer protection.

Within this framework, a set of key European regulations—such as the revised Payment Services Directive (PSD2), the eIDAS Regulation, the Basel III standards, the General Data Protection Regulation (GDPR), and regulatory sandbox initiatives—has played a pivotal role in shaping the digital banking landscape.

* Corresponding author. E-mail address: *mugur.podaru@yahoo.com*

These instruments have influenced not only banks' internal systems and processes but also their strategic approaches to digitalization and collaboration with fintech players.
This paper examines how these regulations both accelerate and discipline the digital transformation of banking. Using a conceptual and analytical perspective, it explores the interplay between regulatory policies and digital innovation, providing insights into the regulatory role in the financial sector's evolution.
The paper is organized in five parts: a review of the relevant literature; an analysis of the key regulations and their industry impact; a discussion of the challenges and opportunities they create; a bibliometric assessment of the five regulations; and concluding remarks with directions for future research.

2. LITERATURE REVIEW

2.1 PSD2

The revised Payment Services Directive (PSD2) was introduced as a legal foundation for opening customer banking data to authorized third-party providers, with the customer's explicit consent (Pestovska, 2021).
The original Payment Services Directive (PSD) was adopted by the European Union in 2007 with the objective of creating a single market for payments across Europe. It established rules and guidelines for the provision of payment services, simplified cross-border payment processing within the EU, promoted innovation, and encouraged competition by facilitating the entry of new players into the payments market. It also provided the legal basis for the creation of the Single Euro Payments Area (SEPA)**.**
The revised version, known as PSD2, was proposed in 2013, adopted in 2015, and fully implemented in 2018. Among its main objectives were:

- further standardizing and improving the efficiency of EU payment systems;
- fostering innovation in the payments sector, particularly by opening it to non-bank entities;
- enhancing transparency in payment methods, including mobile and online payments;
- harmonizing fees and lowering the cost of payment services;
- strengthening transaction security.

The original PSD aimed primarily to create a uniform legal framework for payment services in the EU while providing the legislative basis for SEPA. These measures were deemed essential for building a single market for payment services, a key component of the EU's internal market. By contrast, facilitating the development of e-commerce played only a marginal role in shaping the initial PSD policies. Consequently, although the Directive applies to many online payment scenarios, it offers limited solutions to the specific issues of these transactions—many of which emerged after 2007 (Donnelly, 2016).
One of PSD2's most disruptive provisions is the requirement for banks to grant authorized third-party providers (TPPs) access to customer account data through APIs, with customer consent. This fostered a digital ecosystem based on:

- integrating fintech companies into banking infrastructure;
- unbundling traditional financial services into interconnected digital components;
- accelerating innovation in Payment Initiation Services (PISP) and Account Information Services (AISP)**.**

"PSD2 transformed banks from exclusive intermediaries into providers of open digital infrastructure" (Barbu et al., 2021).
To comply with PSD2 requirements. banks have had to invest in:

- secure API platforms aligned with European standards (e.g., Berlin Group);
- robust electronic identification and Strong Customer Authentication (SCA)**;**
- agile innovation processes to compete with emerging fintech firms (Șoitu, 2019).

These obligations triggered deep digital transformation, driving banks to adopt cloud infrastructures**,** DevOps practices**, and** modular architectures (PwC, 2019).
PSD2 also introduced strict authentication and payment data protection requirements aligned with GDPR. Banks therefore integrated solutions such as: biometric authentication, transaction tokenization and behavioral analytics to prevent digital fraud (Waliullah et al., 2025).
"PSD2 not only enabled new digital services but also imposed a solid security framework, reshaping how the digital banking experience is designed" (EBA, 2020).

2.1.1 Challenges for the banking system in implementing PSD2

1. **Expanded cybersecurity exposure**
   The implementation of open APIs increases the attack surface for hackers, compelling banks to make significant investments in cybersecurity (Trend Micro, 2019, p. 3).
2. **Lack of uniform API standards**
   Although initiatives such as the NextGenPSD2 standard exist, uneven adoption of APIs across countries and financial institutions results in incompatibilities and integration difficulties (Hideez, 2025).
3. **High infrastructure and compliance costs**
   Deploying Strong Customer Authentication (SCA), ensuring data protection, and integrating APIs require substantial investments in IT infrastructure, staff training, and consultancy services (Utimaco, 2024).
4. **Limited customer awareness and trust**
   Many customers are unaware of the benefits of open banking and remain reluctant to share financial data with third-party providers (TPPs) (Utimaco, 2024).
5. **Business model disruption**
   Banks are no longer the sole gatekeepers of account access. The shift toward open banking forces them to rethink revenue streams and client relationships (Infopulse, 2019).

2.2 eIDAS Regulation

The Regulation on Electronic Identification, Authentication and Trust Services — Regulation (EU) No. 910/2014, commonly known as eIDAS — establishes the legal framework for electronic identification within the EU internal market. Its goal is to create a uniform legal basis for secure electronic collaboration across the EU and to strengthen the trust of individuals, legal entities, and public authorities in electronic transactions (Hölbl et al., 2023).
According to the European Commission (2020), eIDAS solutions are intended to enable efficient and secure digital interaction through the following technologies:

- Electronic signature (eSignature) – allows citizens to sign legal documents and electronic messages without printing.
- Qualified Website Authentication Certificate – assures citizens that the websites and applications they use are trustworthy and secure.
- Electronic timestamp (eTimestamp) – provides proof of actions such as ticket purchases for events.
- Electronic seal (eSeal) – ensures the authenticity of documents or tickets (e.g., for sporting events) and prevents forgery.
- Electronic identification (eID) – enables citizens to open a bank account in another Member State using their national ID.
- Electronic Registered Delivery Service – guarantees the secure exchange of data and provides proof of dispatch and receipt.

The eIDAS Regulation entered into force on 1 July 2016 and repealed Directive 1999/93/EC. Its purpose is *"to enhance trust in electronic transactions by establishing a common foundation for secure electronic interactions between citizens, businesses, and public authorities."*

eIDAS defines three levels of electronic signatures:

- Simple electronic signature – electronic data logically attached to other data;
- Advanced electronic signature (AdES) – uniquely linked to the signer and enabling identification;
- Qualified electronic signature (QES) – legally equivalent to a handwritten signature and issued by a qualified trust service provider (ENISA, 2021).

Trust Service Providers (TSPs) are accredited entities that provide services such as qualified electronic signatures, eSeals, timestamps, and website authentication. They must comply with strict requirements on security, data integrity, and periodic auditing (Biedermann et al., 2024). For example, a qualified eTimestamp guarantees the exact time of a digital transaction with full legal validity, while an eSeal is primarily used by legal entities to certify the authenticity of issued documents (ETSI, 2022).

Despite its achievements, research highlights persistent challenges:

- Incomplete interoperability between Member States;
- Technical and legal complexity of implementing qualified signatures in the private sector;
- Limited adoption in the public sector due to institutional constraints (Hölbl et al., 2023).

According to Hölbl et al. (2023, p. 8), *"Notified solutions are often inflexible, and integrating identification services into digital platforms remains difficult due to the lack of fully uniform standards."*

To meet evolving needs, eIDAS 2.0 was adopted in 2024 through Regulation (EU) 2024/1183, introducing the European Digital Identity Wallet (EUDI Wallet) for secure storage and sharing of identity credentials, driver's licenses, diplomas, and other key documents (European Commission, 2024). In banking, one of the most visible applications of eIDAS is online onboarding—the process by which a bank verifies a client's identity remotely using technology. This process, which relies heavily on electronic signatures, is critical to accessing financial services and products. Because each Member State retains the right to regulate electronic signatures nationally, the qualified electronic signature (QES) remains the most secure option, offering the highest guarantees of authenticity and integrity.

2.2.1 Challenges for the Banking System in Implementing eIDAS

1. **Interoperability gaps**
   eIDAS aims for mutual recognition of electronic identities across EU Member States, yet technical heterogeneity and diverse administrative requirements still hinder full interoperability. *"Standardization will be key to ensuring EU-wide interoperability"* ().
2. **EUDI Wallet adoption and security risks**
   Banks will be required to accept European Digital Identity Wallets (EUDIWs) for Strong Customer Authentication (SCA) by December 2027, but they will not directly control the security of cryptographic keys, creating risks when dealing with third-party providers (Hartsema, 2025).

2.3 Basel III Accord

The Basel III regulations, developed by the Basel Committee on Banking Supervision (BCBS), aim to strengthen banks' capital bases, improve risk management, and enhance resilience to financial shocks (Wikipedia, 2025). In the context of accelerated digital transformation, these standards have forced banks to integrate advanced IT technologies to meet increasingly stringent requirements for reporting and data security.

The rollout of Basel III Endgame, with a compliance deadline of July 2025 for systemically important institutions, raises significant technological and data-management challenges.

According to Arcesium (2024), the new standards mandate operational stress testing and expansion of data infrastructure, thereby accelerating the need to modernize legacy IT systems and support regular reporting.

The growing volume of data and the complexity of calculating risk-weighted assets (RWA**)** call for flexible and scalable platforms.
Banking digitalization, including cloud migration, artificial intelligence, and distributed ledger technologies (DLT), exposes financial institutions to operational, reputational, and cyber risks (Jones, 2024; FinTech Magazine, 2024).
BCBS warns that these new technological "nodes" can amplify systemic risk and recommends stronger IT governance and tighter oversight of external providers (BCBS, 2024; FinTech Magazine, 2024).
The broad adoption of fintech solutions supports Basel III compliance. Advanced analytics, process automation, and AI enable real-time monitoring of capital and liquidity (Finance on Point, 2024). Blockchain and data analytics facilitate transparent and secure audits, aligning with regulatory demands for transparency and operational resilience.
Implementing Basel III in a digital environment is driving structural reform: building stronger banks within an automated ecosystem.
Modernizing IT is not merely a technological upgrade but a core element of regulatory compliance and competitiveness.
While digital transformation improves efficiency, it also requires major investment in digital governance, cybersecurity, and data infrastructure.
Basel III penalizes inefficient capital use, prompting banks to digitalize key business processes such as: Digital customer onboarding (KYC, AML), Automated credit scoring and CRM integration with profitability analytics for products and clients.
These processes help optimize capital allocation and reduce risk exposure.
Basel III also requires much more detailed and frequent reporting on capital, liquidity (LCR, NSFR), exposures, and risks. To meet these demands, banks have invested heavily in: Automated ERP and MIS systems, RegTech solutions using AI and machine learning for real-time reporting and Big-data infrastructures to integrate and analyze large financial datasets.
As Arcesium (2024) notes, digitalization has become *"a prerequisite for Basel III Endgame compliance, not merely a technological option."*
Basel III did not prescribe digital transformation, but its regulatory pressure has made such transformation inevitable.
In practice, banks that fail to invest in technology cannot effectively manage Basel III's requirements for capital, risk, and transparency.
Digitalization is no longer a competitive advantage; it is a condition for survival in an increasingly tightly regulated banking system (BCBS, 2024).

2.3.1 Challenges for the Banking Sector in Implementing Basel III

1. **Higher capital requirements**
   Basel III Endgame is expected to increase Common Equity Tier 1 (CET1) requirements by about **16 %** and risk-weighted assets by **20 %** for large banks (Deloitte, 2024).
2. **Regulatory fragmentation**
   Different jurisdictions (EU, United States, United Kingdom) have varied timelines and approaches, potentially creating competitive disadvantages and operational uncertainty.
3. **Complex reporting and infrastructure demands**
   Compliance requires sophisticated data-reporting systems, IT-infrastructure upgrades, and integration of stress-testing tools (EY, 2023).
4. **Asymmetric impact on smaller institutions**
   While global systemically important banks (G-SIBs) can better absorb these changes, smaller banks and non-bank financial entities may face significant difficulties (Wharton, 2023).

2.4 General Data Protection Regulation (GDPR)

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data, known as the General Data Protection Regulation (GDPR)**,** came into force on 25 May 2018, establishing a unified EU-wide framework for the processing and safeguarding of personal data.

In the banking sector — where personal data processing is massive and continuous — GDPR has profoundly influenced digital processes, IT architectures, and customer relations (Zetzsche et al., 2017, 2019).

GDPR forced banks to adopt digital technologies that comply with key principles such as data minimization**,** data portability**,** security, and the right to be forgotten. This led to:

- investments in advanced Personal Information Management Systems (PIM**S)**;
- implementation of encryption**,** pseudonymization, and access-control technologies;
- automated IT audits and privacy-by-design mechanisms in digital banking applications (Voigt & Von dem Bussche, 2017).

"Without flexible and integrated IT architectures, financial institutions cannot meet GDPR's requirements to provide access, modification, or deletion of data at the user's request" (EDPB, 2020).

GDPR also accelerated the shift toward data-protection-centric digital banking.

Banks had to revise how they collect consent across mobile apps**,** internet banking, and marketing communications, leading to:

- customer-facing privacy dashboards;
- automation of consent withdrawal and data management processes;
- adoption of ethical AI, featuring explainable logs and avoiding opaque automated decisions (Wachter et al., 2017).

Moreover, GDPR introduced a strict 72-hour breach notification requirement, putting pressure on banking IT infrastructures and cybersecurity practices.

Banks responded by deploying:

- modern Security Information and Event Management **(**SIEM) systems;
- robust incident-response and continuous testing procedures;
- closer collaboration between Data Protection Officers (DPOs)**,** IT teams, and compliance units.

"Banks must move beyond mere privacy policies toward a comprehensive data-governance architecture" (Kuner et al., 2020).

2.4.1 Challenges for the Banking Sector in Implementing GDPR

1. **Complex consent management**
   Banks must obtain explicit, informed, and specific consent from clients. Even minor inconsistencies, without serious security breaches, can result in significant fines. Financial institutions struggle to track personal data across complex, non-integrated systems (Feroot, 2025).
2. **Expanded liability through case law**
   Recent rulings of the Court of Justice of the EU (CJEU) allow individuals to claim compensation for loss of control over their data even without an actual damage (Feldman et al., 2025).
3. **Reputational and strategic implications**
   Beyond regulatory fines, GDPR compliance has become a competitive advantage, as privacy breaches can severely damage an institution's reputation (Laney, 2024).

3. RESEARCH METHODOLOGY

Rationale for the Bibliometric Method

Bibliometric analysis is a quantitative method for evaluating scientific literature, used to identify thematic relationships among key concepts in published articles.
The choice of this method is justified by:

- its relevance for exploring the structure of knowledge and major research directions;
- its ability to visualize connections between concepts across diverse domains (legal, technological, financial);
- its objectivity, based on co-occurrence frequencies of terms;
- its usefulness in supporting an academic study by facilitating the selection of relevant literature.

3.1. Bibliometric Analysis of the Impact of GDPR on the Banking Sector

The General Data Protection Regulation (GDPR) is one of the most significant legislative instruments of the European Union, with direct implications for the management of personal data. The sectors most affected include banking, fintech, IT, and digital services, where large volumes of personal data are processed.
To capture research trends and thematic interdependencies generated by the application of GDPR, a **bibliometric analysis** was conducted.

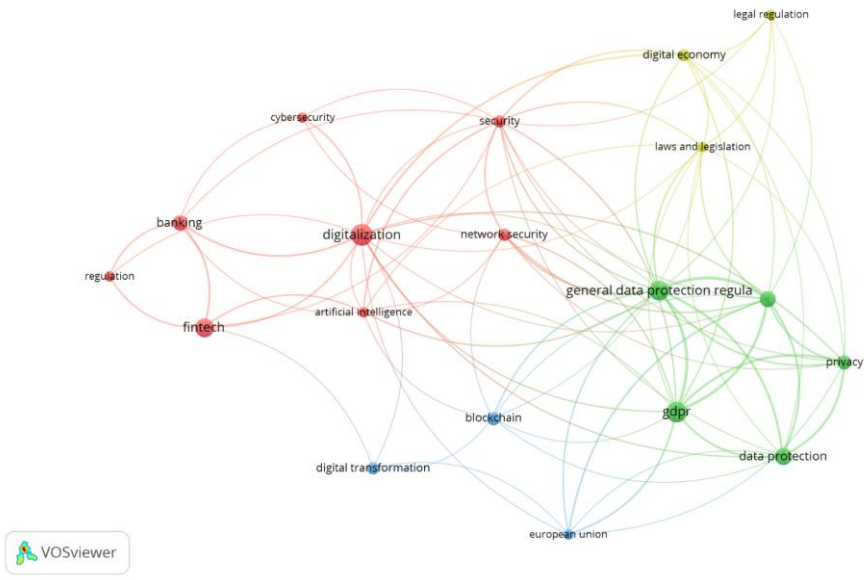

Figure 1. GDPR bibliometric graph

Source: The graph was generated by the authors using VOSviewer**,** based on a CSV type file exported from the Scopus database. The dataset was generated in May 2025 by searching for documents with the keywords *GDPR* and *banking*, yielding a total of 120 documents.

The analyzed graph (figure 1), depicts a co-occurrence map of keywords from the literature on GDPR and its impact on the digital–financial environment.
It contains **four main thematic clusters**:

- **Green cluster (legal–regulatory)**: Focused on terms such as *GDPR*, *general data protection regulation*, *privacy*, *data protection*, *laws and legislation*. This forms the conceptual core of the European regulatory framework.

- **Red cluster (technological–banking)**: Includes terms such as *digitalization*, *fintech*, *banking*, *cybersecurity*, *artificial intelligence*, reflecting concerns related to implementing GDPR in the digital infrastructure of the banking system.
- **Yellow cluster (digital economy and legislation)**: Concentrates terms such as *digital economy* and *legal regulation*, highlighting the link between the legislative framework and macroeconomic transformations.
- **Blue cluster (emerging technologies and EU policies)**: Brings together concepts such as *blockchain*, *digital transformation*, and *European Union*, suggesting the influence of EU directives on emerging technologies.

The analysis highlights GDPR as a central node in the scientific literature, connecting areas such as cybersecurity, the digitalization of financial services, privacy protection, and legal regulation. These interconnections point to a clear trend of convergence between technology and law in an increasingly digitalized European context.

The bibliometric method proves to be an essential tool for mapping this complex ecosystem and for identifying future directions for research and regulation.

3.2 Conceptual Relation in the Context of eIDAS bibliometric map

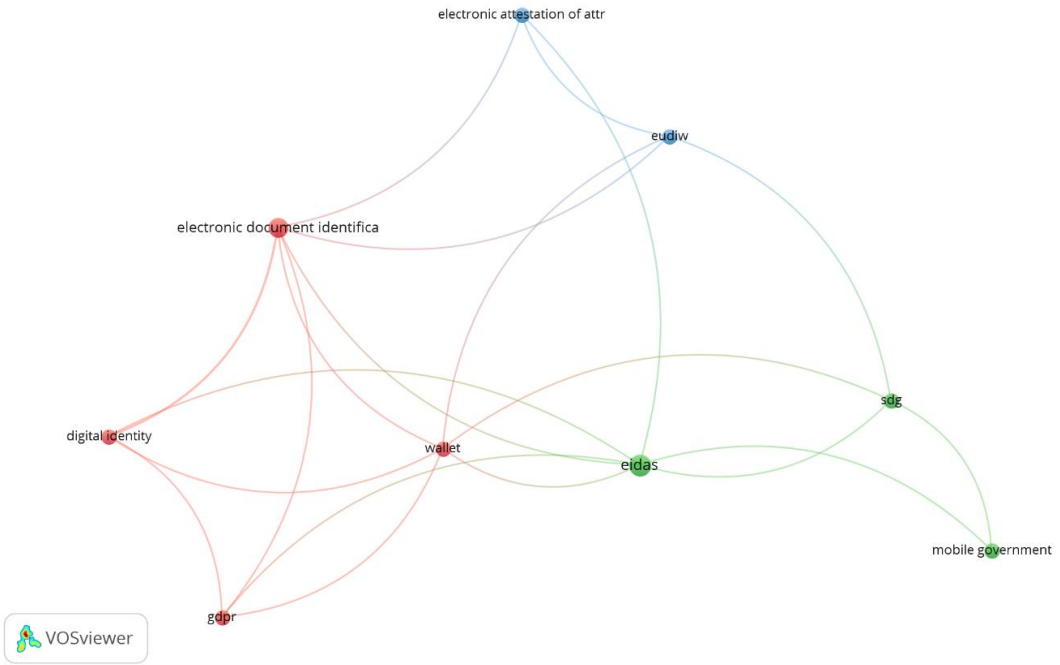

Figure 2. eIDAS bibliometric graph

Source: The graph was created by the authors using VOSviewer, based on a CSV file exported from the Scopus database. The dataset was generated in May 2025 by searching for documents with the keywords *eIDAS* and *banking*, yielding a total of 120 documents

The presented network map (figure 2) illustrates the co-occurrence of key terms in the scientific literature on digital identity and EU regulations in the era of public-sector digitalization.

The analysis reveals several thematic clusters, each reflecting a major research direction or policy/technology focus.

1. **Red cluster – Digital identity and data-protection regulations**
   Terms such as *digital identity*, *GDPR*, *wallet*, and *electronic document identification* are closely interconnected.

This cluster highlights the interaction between digital identification and personal-data protection within the EU legislative framework.
The strong link to *wallet* underscores the current strategic focus on European digital wallets, which integrate identity, authentication, and secure document storage.

2. **Green cluster – Regulation and digital governance**
   Terms like *eIDAS, SDG (Sustainable Development Goals)*, and *mobile government* define a core area centered on European regulations for electronic identification and their contribution to public-service digitalization and the achievement of sustainable development goals**.**
3. **Blue cluster – Technical infrastructures and European interoperability**
   Keywords such as *EUDI Wallet* and *electronic attestation of attributes* point to the growing interest in the technical standardization of electronic attestations and in cross-border interoperability within the European Digital Identity Wallet initiative.
4. **Central positioning of "eIDAS"**
   The *eIDAS* node functions as a linking hub across all three clusters, underlining its pivotal role in the EU's digital-identity ecosystem.
   It connects both with technical terms (*wallet*, *attestation*), normative terms (*GDPR*), and strategic terms (*SDG*), reflecting the multidimensional complexity of this legislative framework.

3.3 Conceptual Relationships in the Context of PSD2 bibliometric map

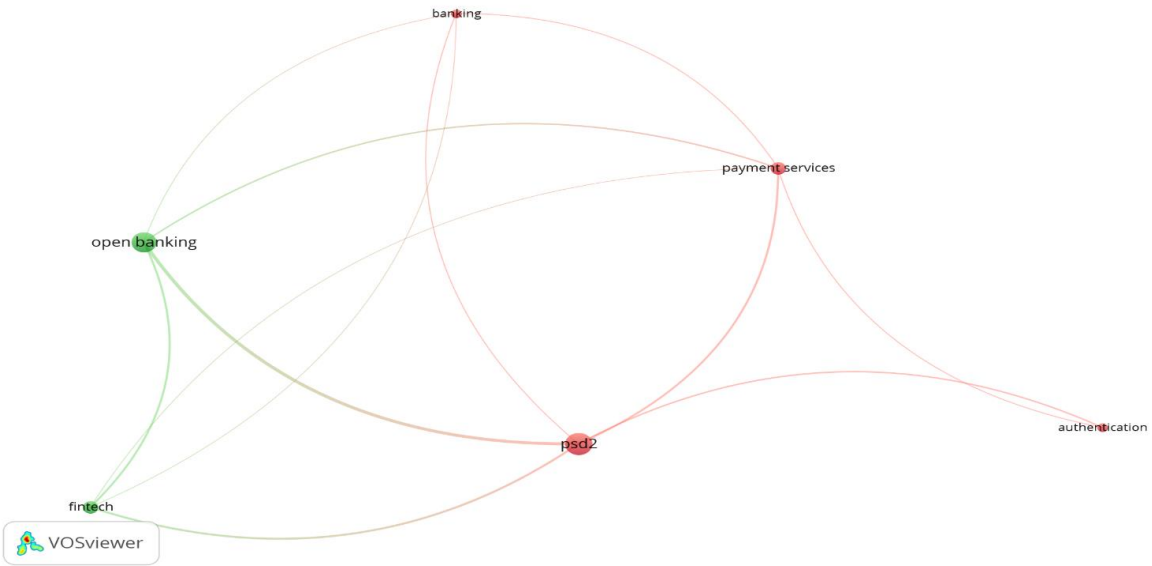

Figure 3. PSD2 bibliometric map

Source: The graph was created by the authors using VOSviewer, based on a CSV type file exported from the Scopus database**.** The dataset was generated in May 2025 by searching for documents with the keywords *PSD2* and *banking*, yielding a total of 75 documents.

The revised Payment Services Directive **(PSD2)** adopted by the European Union (2018) has profoundly transformed how financial institutions interact with customer data, payment services, and emerging technologies. This regulation laid the foundation for the concept of open banking and encouraged the rise of fintechs as competitive players in the financial market.
To examine current research directions and conceptual interdependencies, a bibliometric co-occurrence analysis of keywords was applied.
Two main clusters stand out:

- **Red cluster (PSD2 and regulation)**: Includes terms such as *psd2*, *payment services*, *authentication*, and *banking*. This cluster reflects concerns related to legal compliance, security, and the infrastructure of traditional banking.
- **Green cluster (innovation-oriented)**: Contains *open banking* and *fintech*, indicating the emergence of new financial actors and the structural changes driven by digitalization.

The term **"**banking" occupies a central position, linking the two spheres and underscoring the dual challenge: complying with strict regulations while adopting new business models.
The concept of "authentication**"** is connected to both PSD2 and payment services, highlighting the importance of Strong Customer Authentication (SCA)**.**
The analysis shows that PSD2 is a central node in the scientific literature, generating connections in both regulatory and technological innovation domains.
The concept of open banking, supported by fintech companies, emerges as one of the main drivers of the European financial market's evolution.
The bibliometric method provides a clear visualization of these interactions and a solid foundation for exploring future challenges related to security**,** competition, and chalenges for traditional banking systems**.**

4. CONCLUSIONS

This study has demonstrated that the digital transformation of the European banking sector is a complex process resulting from the dynamic interaction between technological innovation and regulatory interventions, embodied in the key normative instruments analyzed: PSD2, eIDAS, Basel III, and GDPR**.**

These regulations have profoundly reshaped the operational infrastructure of financial institutions, their risk-management practices, and their customer relationships, creating significant opportunities for digitalization but also posing major challenges in terms of security, interoperability, and compliance**.**

In particular, the bibliometric analysis focused on the specialized literature dedicated to PSD2, eIDAS, and GDPR. For PSD2, the co-occurrence analysis revealed two main thematic clusters: one centered on regulation, security, and traditional banking infrastructure, and another oriented toward open innovation and the emergence of fintechs**.** The eIDAS bibliometric map highlighted the interdependencies between electronic identification**,** cross-border interoperability**,** and the development of the European Digital Identity Wallet (EUDI Wallet**)**, underlining the multidimensional complexity of electronic-identity regulation. Regarding GDPR, the analysis confirmed its central position in academic literature, structured around four thematic clusters linking privacy protection, the digitalization of financial services, data governance, and legal regulation, reflecting the convergence of regulation and digital transformation.

Looking forward, further research should examine the interaction between new European initiatives—such as eIDAS 2.0 and the EUDI Wallet—and emerging technologies, including artificial intelligence and blockchain, in order to identify opportunities and risks associated with digital banking in an evolving regulatory environment. In this context, the regulatory framework as an adaptive governance instrument remains central to the sustainable transformation of the European banking sector**.**

REFERENCES

Arcesium. (2024). How technology and data management are influencing banks' response to the Basel III Endgame. *Arcesium.com.* Retrieved June 2025, from https://www.arcesium.com/blog/technology-data-management-influence-banks-response-basel-iii-endgame

Barbu, C. M., Florea, D. L., Dabija, D., & Barbu, M. C. R. (2021). Customer experience in Fintech. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(5), 1415–1433. https://doi.org/10.3390/jtaer16050080

Basel Committee on Banking Supervision (BCBS). (2024, May 16). Basel Committee publishes report on the digitalisation of finance (press release). *Bis.org.* Retrieved June 2025, from https://www.bis.org/press/p240516.htm

Biedermann, B., Scerri, M., Kozlova, V., & Ellul, J. (2024). A Systematisation of Knowledge: Connecting European digital identities with Web3. *arXiv.org*. https://arxiv.org/pdf/2409.19032

Deloitte. (2024). Basel III Endgame Update: Implications and considerations. *Deloitte.wsj.com*. Retrieved June 2025, from https://deloitte.wsj.com/riskandcompliance/basel-iii-endgame-update-implications-and-considerations-acb80036

Donnelly, M. (2016). Payments in the digital market: Evaluating the contribution of Payment Services Directive II. *Computer Law & Security Review, 32*(6), 827–839. https://doi.org/10.1016/j.clsr.2016.07.003

European Union Agency for Cybersecurity. (2021). *Electronic Signatures and Infrastructures (ESI) – Standards*. Retrieved June 2025, from https://www.enisa.europa.eu

ETSI. (2022). *Electronic Signatures and Infrastructures (ESI); Overview of Standards and Architectures*. Retrieved June 2025, from https://www.etsi.org

European Banking Authority. (2020, June 4). *Opinion on obstacles to the provision of third-party provider services under PSD2*. Retrieved June 2025, from https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-opinion-obstacles-provision-third-party

European Commission. (2018). *Revised Payment Services Directive (PSD2)*. Retrieved June 2025, from https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366

European Commission. (2020). *Trust services and eID under eIDAS*. Retrieved June 2025, from https://ec.europa.eu

European Commission. (2024). *Digital Identity Wallet: Regulation (EU) 2024/1183*. Retrieved June 2025, from https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation

European Data Protection Board. (2020). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. Retrieved June 2025, from https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

EY. (2023). *As the Basel deadline nears, are banks up for the challenge?* Retrieved June 2025, from https://www.ey.com/en_mz/insights/banking-capital-markets/as-the-basel-deadline-nears-are-banks-up-for-the-challenge

Feroot. (2025). *The 10 most costly GDPR mistakes banks and financial institutions*. Retrieved June 2025, from https://www.feroot.com/blog/gdpr-mistakes-banks-financial-institutions/

Finance on Point. (2024). *The significance of Basel III and its impact on commercial banks*.

FinTech Magazine. (2024, May 20). *Basel Committee: Banking digitalisation creates 'risks'*. Retrieved June 2025, from https://fintechmagazine.com/articles/basel-committee-banking-digitalisation-creates-risks

Hartsema, J. (2025, June). *Why eIDAS 2.0 poses major hurdles for payment service providers*. Retrieved June 2025, from https://www.linkedin.com/pulse/why-eidas-20-poses-major-hurdles-payment-service-jim-hartsema-dbaqe/

Hideez. (2025). *PSD2, Dynamic Linking & FIDO Authenticators*. Retrieved June 2025, from https://hideez.com/blogs/news/psd2-banking-explained?srsltid=AfmBOooGlRYMPvFZzCVXufvX2NMUNpgXgA6u031Wwgey5Rw7UumC2e3b

Hölbl, M., Kežmah, B., & Kompara, M. (2023). eIDAS interoperability and cross-border compliance issues. *Mathematics, 11*(2), 430. https://doi.org/10.3390/math11020430

Infopulse. (2019). *Why PSD2 implementation is so important for banks*. Retrieved June 2025, from https://medium.com/@infopulseglobal_9037/why-psd2-implementation-is-so-important-for-banks-26f5d8931f55

Kuner, C., Cate, F., H., Millard, C., Svantesson, D., J. (2020). *Transborder data flows and data privacy law*. Oxford University Press.

Laney, D. (2024, June 12). *GDPR violations and fines: Trends, insights and compliance strategies*. Retrieved June 2025, from https://www.forbes.com/sites/douglaslaney/2024/06/12/gdpr-violations-and-fines-trends-insights-and-compliance-strategies/

Pestovska, Z., S. (2021). The (r)evolution of banking: Discussions and prospects. *Academy Review*. *1*(54). https://doi.org/10.32342/2074-5354-2021-1-54-4

PwC. (2019). *The future is open: How PSD2 will change the banking industry*. Retrieved June 2025, from https://www.pwc.ch/en/publications/2017/future-banking-psd2.pdf

Jones, H. (2024, May 16). *Digitalisation of banking creates new risks, says global watchdog*. Retrieved June 2025, from https://www.reuters.com/business/finance/digitalisation-banking-creates-new-risks-says-global-watchdog-2024-05-16/

Feldman, R., Fields, A., & Yifru, C. (2025, June 26). *Unintended consequences: How recent data protection rulings threaten Europe's digital future*. Retrieved June 2025, from https://www.reuters.com/legal/legalindustry/unintended-consequences-how-recent-data-protection-rulings-threaten-europes-2025-06-26/

Schwalm, S., Albrecht, D., & Alamillo, I. (2022). eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI. *Paper presented at Open Identity Summit 2022*. Copenhagen, Denmark.

Șoitu, L. (2019). *PSD2 – Oportunități și provocări pentru sectorul bancar.* Retrieved June 2025, from https://www.arb.ro/wp-content/uploads/5.PSD2-Oportunitati-si-Provocari-LS-ARB.pdf

Trend Micro. (2019). *When PSD2 opens more doors: The risks of open banking*. Retrieved June 2025, from https://www.trendmicro.com/en/research/19/i/when-psd2-opens-more-doors-the-risks-of-open-banking.html

Utimaco. (2024). *Exploring the impact of PSD2 on European payments*. Retrieved June 2025, from https://utimaco.com/articles/psd2-impact

Voigt, P., Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law, 7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Waliullah, M., George, Z. H., Hasan, T., Alam, K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 226-257. https://doi.org/10.63125/fh49az18

Acharya, V. V. (2023). *Basel III endgame was inevitable for large banks, but what about non-banks and smaller banks?* Retrieved June 2025, from https://wifpr.wharton.upenn.edu/blog/basel-iii-endgame-was-inevitable-for-large-banks-but-what-about-non-banks-and-smaller-banks/

Wikipedia. (2025, June). *Basel III*.

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2017). The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *University of Hong Kong Faculty of Law Research Paper*, 020. https://doi.org/10.2139/ssrn.3018214

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2019). From FinTech to TechFin: The regulatory challenges of data-driven finance. *University of Hong Kong Faculty of Law Research Paper*, 007. http://dx.doi.org/10.2139/ssrn.2959925