Legal 500
Country Comparative Guides 2025

Romania
Fintech

Contributor

VD Law Group

Sergiu-Traian Vasilescu

Managing Partner | sergiu.vasilescu@vdlawgroup.com

Luca Dejan

Partner | luca.dejan@vdlawgroup.com

Bogdan Rotaru

Partner | bogdan.rotaru@vdlawgroup.com

This country-specific Q&A provides an overview of fintech laws and regulations applicable in Romania.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Romania: Fintech

1. What are the regulators for fintech companies in your jurisdiction?

In Romania, fintech companies operate under the supervision of several regulatory authorities, depending on the nature of their business activities.

As of February 2025, the primary regulators in the field of fintechs are:

a. National Bank of Romania (BNR) – which is the main regulatory body for financial institutions, including fintech companies that engage in banking activities, electronic money issuance, and payment services.

Companies wishing to provide such services must obtain proper authorizations from the BNR and comply with the applicable banking and financial legislation. The BNR ensures that these entities operate within the legal framework and meet prudential requirements, including capital adequacy, risk management, and consumer protection rules;

b. Financial Supervisory Authority (ASF) – opposed to the BNR, the ASF oversees non-banking financial markets, including insurance, crowdfunding, private pensions, and capital markets.

Fintech firms involved in investment services, crowdfunding, digital insurance solutions, or other financial instruments fall under ASF's jurisdiction and, depending on the type of service provided, these companies may need to apply for licensing or registration with the ASF and comply with its regulatory requirements.

c. Romanian Authority for Digitalization (RAD) – while this authority is not a financial regulator per se, RAD plays a role in shaping the digital financial landscape, overseeing aspects relevant to fintech, such as digital identity, cybersecurity, and open data initiatives.

Thus, Fintech companies operating with digital platforms, or offering Know Your Customer (KYC) services, blockchain solutions, or AI-driven financial products may need to follow ADR guidelines related to digital infrastructure and security standards.

2. Do you foresee any imminent risks to the growth of the fintech market in your jurisdiction?

We do not foresee imminent risks to the growth of the fintech sector that are unique to Romania. While fintech continues to significantly influence global markets, it is essential to maintain vigilant supervisory oversight to address potential challenges effectively.

Romanian regulators are actively engaged in developing optimal legislative solutions to keep pace with the complex technological and economic advancements affecting the financial sector. Unlicensed or non-licensable projects often attempt to exploit regulatory gaps; however, Romania has consistently implemented appropriate measures, enacting or adapting regulations across all pertinent areas of the fintech market.

Consumer vulnerability, linked to the maturity level of the Romanian financial market, presents another significant concern. Authorities have undertaken substantial efforts to address knowledge disparities and collaborate with European Union agencies to enhance consumer education and protection.

In the cryptocurrency market, risks appear to be diminishing as the sector is receiving increased regulatory attention, with legislative acts like the Digital Operational Resilience Act (DORA) and notably, the Markets in Crypto-Assets Regulation (MiCAR), becoming applicable from 17th January 2025 and 30th December 2024, respectively.

Regarding concerns about payment fraud and the effectiveness of Strong Customer Authentication (SCA), forthcoming legislation, including the proposed Payment Services Directive 3 (PSD3) and the Payment Services Regulation, is anticipated to strengthen both European Union and Romanian defenses against such risks.

In summary, while challenges persist, Romania's proactive regulatory measures, consumer protection efforts, and investment in technological infrastructure collectively contribute to a favorable environment for the continued growth of the fintech sector.

3. Are fintechs required to be licensed or registered to operate in your jurisdiction?

Fintech companies operating in Romania may be required

to obtain a license or register with the relevant authorities, depending on the nature of their business.

Thus, entities engaged in regulated financial services—such as payment processing, electronic money issuance, lending, investment services, or insurance—must secure the appropriate authorization before commencing operations.

As explained above, the primary regulatory bodies overseeing these activities are the National Bank of Romania (BNR) and the Financial Supervisory Authority (ASF).

For example, fintech companies providing payment services or issuing electronic money must obtain a license from the BNR, in accordance with Law No. 209/2019 on payment services, which transposes the Revised Payment Services Directive (PSD2 – Directive (EU) 2015/2366) into Romanian law.

Similarly, those offering (i) investment-related services fall under the regulatory scope of the ASF, as per Law No. 126/2018 on markets in financial instruments, which implements the MiFID II Directive or (ii) digital insurance products are also subject to licensing under Law No. 236/2018 on insurance distribution, aligned with the Insurance Distribution Directive (IDD – Directive (EU) 2016/97).

Conversely, certain fintech business models that do not directly fall under existing financial regulations may not require specific licensing or registration. However, these companies must still comply with Law No. 129/2019 on anti-money laundering and counter-terrorism financing, which imposes obligations on businesses facilitating financial transactions.

Additionally, with the increasing regulation of crypto-assets at the European level, Romania is preparing for the implementation of Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCAR). This regulation, which became fully applicable from 30 December 2024, introduces licensing requirements for crypto-asset service providers, ensuring greater regulatory oversight in this sector.

Given the evolving legal framework, fintech companies are advised to conduct thorough regulatory assessments to determine the exact licensing or registration obligations applicable to their business model.

4. What is a Regulatory Sandbox and how does it benefit fintech start-ups in your jurisdiction?

A Regulatory Sandbox is a framework that allows fintech companies to test innovative products, services, or business models in a live environment while operating under regulatory supervision.

This setup provides a safe space for companies to experiment with new solutions, ensuring they comply with legal requirements and maintain consumer protection standards.

In Romania, although a formal Regulatory Sandbox has not yet been fully implemented, the National Bank of Romania (BNR) has introduced the Fintech Innovation Hub, a platform designed to facilitate dialogue between fintech innovators and regulatory authorities. Through this initiative, companies can seek guidance on compliance matters and regulatory expectations, helping them navigate the complexities of financial regulation before launching their products into the market.

Similarly, the Financial Supervisory Authority (ASF), which regulates non-banking financial sectors such as insurance, capital markets, and private pensions, has established the Fintech Hub, which serves as a resource for fintech businesses operating in these areas and provides support in understanding the applicable regulatory framework.

In our view, participating in a Regulatory Sandbox can provide several key benefits to fintech companies:

- Clearer Regulatory Understanding;
- Reduced Initial Cost;
- Faster Time to Market;
- Managing Risks Safely;
- Networking and Collaboration Opportunities.

5. How do existing securities laws apply to initial coin offerings (ICOs) and other crypto assets, and what steps can companies take to ensure compliance in your jurisdiction?

In Romania, the regulatory landscape for Initial Coin Offerings (ICOs) and other crypto – assets is evolving, with existing securities laws potentially applicable depending on the specific characteristics of the offering.

The Romanian Financial Supervisory Authority (ASF) and the National Bank of Romania (BNR) have not issued comprehensive regulations specifically addressing ICOs or crypto assets. However, general provisions of Romanian securities law, aligned with European Union directives, may apply if the crypto assets exhibit features akin to traditional financial instruments.

To determine whether an ICO or crypto asset falls under

the scope of securities regulation, Romanian authorities may assess factors such as the rights conferred to investors, the expectation of profits, and the degree of decentralization. If the tokens offered grant rights similar to shares or bonds, such as profit-sharing or decision-making powers, they are more likely to be classified as securities.

Companies looking to launch an ICO or operate with crypto assets in Romania should follow several essential steps to ensure compliance with applicable regulations:

- **Legal Evaluation** – Conduct a detailed analysis to determine whether the token qualifies as a security under Romanian law. This assessment should focus on the token's characteristics, the rights it grants to holders, and whether it resembles traditional financial instruments such as shares or bonds.
- **Regulatory Consultation** – Engage in discussions with the Financial Supervisory Authority (ASF) and the National Bank of Romania (BNR) to clarify any regulatory obligations as early communication with these authorities can help navigate potential licensing requirements and ensure compliance with the legal framework.
- **Documentation and Disclosure** – If the token is classified as a security, prepare and submit the necessary documentation, including a prospectus, in accordance with Romanian securities regulations.
- **AML and KYC Compliance** – Implement strict anti-money laundering (AML) and know-your-customer (KYC) procedures to align with both national and EU regulations.
- **Ongoing Regulatory Obligations** – Establish internal processes to meet continuous compliance requirements, such as periodic reporting to regulatory authorities. Staying up to date with legislative changes and ensuring adherence to evolving regulations is crucial for long-term operational stability.

6. What are the key anti-money laundering (AML) and Know Your Customer (KYC) requirements for cryptocurrency exchanges in your jurisdiction, and how can companies implement effective compliance programs to meet these obligations?

In Romania, cryptocurrency exchanges are subject to Law No. 129/2019 on the prevention and combating of money laundering and terrorist financing, which aligns with the EU's AML directives, but the specific provisions concerning cryptocurrency exchanges are currently suspended until the Romanian Government enacts a dedicated procedure detailing their implementation.

Despite this suspension, it is highly advisable for any cryptocurrency exchange to establish and follow a comprehensive KYC/AML compliance program that includes customer identification and verification, a risk-based approach to assessing transactions, continuous monitoring of suspicious activities, proper record-keeping, and clear internal procedures for reporting suspicious transactions.

Additionally, exchanges should ensure regular staff training on AML obligations, conduct independent audits to assess compliance effectiveness, and proactively implement these measures to mitigate risks and facilitate a smooth transition once the regulatory framework is fully enforced.

7. How do government regulations requiring licensing or regulatory oversight impact the operations of cryptocurrency and blockchain companies in your jurisdiction, and what strategies can be employed to navigate these varying requirements?

Currently, the regulatory oversight for cryptocurrency and blockchain companies in Romania does not have a major impact on their operations, largely due to the unclear and evolving legal landscape in this field.

As of now, companies that offered crypto-assets or began providing crypto-asset related services prior to the applicability of the Market in Crypto-Assets Regulation (MiCA) on December 30, 2024, are not subject to specific licensing requirements under Romanian law. However, this does not apply to e-money or asset-referenced tokens, which have been regulated since June 30, 2024, in accordance with the said regulation.

For companies that commenced crypto-asset related activities after MiCA became applicable, compliance with MiCA's provisions is mandatory, but it remains unclear which specific authorities in Romania will be responsible for overseeing these activities.

While the new legislative proposal to grant the National Bank of Romania the authority to oversee asset-referenced tokens and crypto-asset services is a step toward clarification, the full impact of these changes will only be felt once the regulatory framework is formally enacted.

Therefore, while the regulatory environment is evolving, it does not yet impose significant burdens on companies,

as the legal and regulatory guidelines are still under development.

8. What measures should cryptocurrency companies take to comply with the governmental guidelines on tax reporting and obligations related to digital assets in your jurisdiction?

To ensure full compliance with Romania's tax regulations, cryptocurrency companies must first establish a rigorous accounting system to track each transaction involving cryptocurrencies, including purchases, sales, exchanges, and conversions to fiat currency. This includes ensuring that all transactions are logged with accurate timestamps and transaction values in both cryptocurrency and Romanian Leu (RON). In addition, companies should determine their tax obligations based on the business model, such as whether they qualify as microenterprises or small businesses, as the applicable tax rates can vary significantly. For example, microenterprises benefit from a flat tax rate of 1% of revenue, provided they have at least one full-time employee.

Another critical step is to ensure compliance with VAT obligations, particularly if the company is providing cryptocurrency-related services such as exchange, trading, or ICO facilitation. These activities may trigger VAT registration requirements, and companies should ensure that they issue VAT-compliant invoices.

Companies involved in crypto mining or trading should track the cost basis of their assets, particularly given the fluctuating value of cryptocurrencies – proper valuation of crypto holdings at the time of sale or conversion is crucial for accurately determining taxable gains.

Lastly, timely filing of all required tax documents is essential. This includes submitting annual tax returns, financial statements, and any applicable documentation regarding income from cryptocurrency transactions. Given the possibility of audits, companies should also maintain records of their compliance efforts, including correspondence with tax authorities, any tax advisory reports, and documentation of internal controls used to ensure accuracy in tax filings.

By implementing these specific measures, cryptocurrency companies in Romania can better navigate the tax framework, ensure compliance, and minimize the risk of penalties or legal challenges related to their business operations.

9. How can blockchain companies address data privacy and protection regulations in your jurisdiction, while ensuring transparency and security on decentralized networks?

Blockchain companies operating in Romania must comply with the General Data Protection Regulation (GDPR) and local Romanian data protection laws, just like any other company handling personal data. This includes obligations such as keeping detailed records of data processing activities, drafting clear and comprehensive privacy and cookie policies, and ensuring that users are fully informed about how their data is handled.

In the context of blockchain's public and immutable nature, companies must consider how personal data is managed on the network. Blockchain is inherently transparent, meaning that transactions and data can often be visible to anyone with access to the network. To ensure compliance with GDPR, blockchain companies must provide mechanisms that allow users to control what personal data is recorded on the blockchain, especially if the blockchain is designed to store personal information. Users should have the option to decide which personal details are visible, ensuring that sensitive information is not unnecessarily exposed.

Furthermore, blockchain companies should implement processes to allow individuals to exercise their rights under GDPR, such as the right to access, rectification, or erasure of personal data.

While the nature of blockchain makes “erasure” a more complex issue due to its permanent, decentralized records, companies should still have procedures in place to manage personal data in a way that respects the rights of individuals. This could include leveraging cryptographic techniques that allow for data to be anonymized or pseudonymized, thus minimizing the risks of exposing identifiable information on the blockchain.

10. How do immigration policies, such as the U.S.'s H-1B and L-1 visas, impact the ability of fintech companies to hire international talent in your jurisdiction?

Immigration policies in Romania, although different from the U.S.'s H-1B and L-1 visas, still provide mechanisms for fintech companies to attract international talent. Romania offers several visa options for foreign professionals, with one of the most notable being the EU Blue Card. This permit is designed for highly skilled workers, allowing them to work in Romania in a wide

range of industries, including fintech. It is particularly advantageous for non-EU citizens, granting them residence and the right to work, provided they meet certain criteria regarding qualifications and salary thresholds.

For fintech companies, hiring international talent requires obtaining work permits and residence visas, which can vary in terms of complexity depending on the applicant's skill level and nationality. For example, the Romanian government has established a fast-track procedure for highly skilled workers, especially those in fields such as software development, engineering, and blockchain technologies. The process generally involves proving the necessity of hiring foreign talent, along with demonstrating the specialized nature of the position.

Companies may also leverage the "Highly Skilled Worker" visa for employees with specialized knowledge or expertise, where the Romanian authorities have created specific pathways for those who can fill gaps in local labor markets.

However, while Romania's immigration policies are more flexible than those in some other European Union countries, challenges still exist, including ensuring the company adheres to specific compliance regulations on salaries, tax reporting, and employment conditions.

11. What are the key regulatory and compliance requirements that a fintech must address when entering the market in your jurisdiction, and how can the company ensure adherence to all applicable laws and regulations?

When entering the Romanian market, a fintech company must ensure compliance with various regulatory and legal requirements to operate legally and securely. If the business model involves providing financial services such as payments, lending, or issuing electronic money, obtaining the necessary authorization from the National Bank of Romania (BNR) or the Financial Supervisory Authority (ASF) may be required.

However, if the fintech operates under an EU license, passporting may allow it to provide services in Romania without additional authorization, though notification to the relevant authorities is still necessary.

Data protection is another critical aspect, as fintechs must comply with the General Data Protection Regulation (GDPR) and Romanian data protection laws. This includes ensuring the security of customer data, implementing appropriate consent mechanisms, and appointing a Data Protection Officer (DPO) if necessary.

Fintech companies operating in Romania must also comply with labor laws and workforce regulations, ensuring that employment contracts, benefits, and working conditions meet national legal standards. This includes proper registration of employees, adherence to working hour regulations, and compliance with tax and social security contributions.

From a financial standpoint, fintechs must comply with Romanian tax laws, including corporate income tax, VAT (if applicable), and payroll taxes for employees. The company must ensure accurate financial reporting and meet any relevant fiscal obligations. Engaging with a local tax expert or accounting firm is advisable to navigate the complexities of Romanian tax regulations efficiently.

12. How should a fintech approach market entry strategy in your jurisdiction, considering factors such as target customer demographics, competitive landscape, and potential partnerships with banking and other financial institutions?

Entering the Romanian fintech market isn't just about ticking off regulatory checkboxes—it's about understanding the people, the landscape, and how to fit into an ecosystem that's growing fast but still has its unique challenges.

First, let's talk about customers. Romania has a strong digital adoption rate, especially among younger generations who are mobile-first and expect seamless, intuitive financial services. There's also a growing wave of SMEs looking for smarter banking, lending, and payment solutions. However, financial inclusion remains a gap, particularly in rural areas where traditional banking services are limited. A fintech that can balance high-tech with accessibility—whether through easy-to-use apps, alternative lending models, or better financial education—can tap into an underserved yet promising market.

Then there's the competition. It's a mix of everything—global fintechs, homegrown startups, and traditional banks stepping up their digital game. Some of the big banks have already integrated fintech-like experiences into their apps, so standing out means either doing something new or doing something better.

Now, let's talk partnerships. Romanian banks used to be cautious about working with fintechs, but things are

changing. Open banking (thanks to PSD2) has opened doors for collaboration, and banks are starting to realize that fintechs can be partners, not just competitors. Getting a strong local bank or payments provider on board can provide credibility, speed up compliance processes, and help with customer acquisition

So, what's the best way to enter the market? First, get regulatory alignment sorted early—navigating authorizations, GDPR, and tax compliance from the start avoids headaches down the road. Second, focus on digital marketing—Romanian consumers respond well to social media and influencer-driven campaigns, so a strong online presence is key. Finally, build trust. Financial services run on credibility, and in a market where many still lean on traditional banking, proving reliability, security, and real value will be essential for long-term success.

13. What are the primary financial and operational risks associated with entering the market in your jurisdiction, and how can the fintech effectively mitigate these risks to ensure a smooth transition and sustainable growth?

Expanding into Romania as a fintech comes with its fair share of risks, but nothing that can't be tackled with the right approach.

On the financial side, regulatory compliance is one of the biggest hurdles. While Romania follows EU laws like PSD2 and GDPR, the way they're implemented locally can sometimes be unclear or change unexpectedly. Getting caught up in licensing or AML issues can cause major delays, so working with local legal experts from day one is a must. Then there's the currency factor—since Romania still uses the leu (RON), exchange rate fluctuations could impact pricing and profitability, especially for cross-border fintechs.

Operationally, winning over Romanian customers takes time. While younger, urban consumers are eager to embrace fintech solutions, trust is still a big factor—people tend to stick with traditional banks unless they're convinced a new service is secure and reliable. Clear communication, transparency, and local partnerships can help bridge this gap. Competition is another reality. The market is growing, but digital payments, lending, and personal finance platforms already have strong players, so standing out means offering something truly different or better.

The key to making it work? Get compliance sorted early, hedge against currency risks, find the right funding channels, build trust with customers, and stay ahead of the competition through innovation and security. If a fintech can navigate these challenges, Romania offers plenty of opportunities for sustainable growth.

Yes, Romania allows certain business functions to be outsourced to offshore locations, but there are regulatory restrictions and compliance requirements that fintechs need to consider, especially when handling financial services, customer data, and IT infrastructure.

14. Does your jurisdiction allow certain business functions to be outsourced to an offshore location?

Yes, Romania allows certain business functions to be outsourced to offshore locations, but there are regulatory restrictions and compliance requirements that fintechs need to consider, especially when handling financial services, customer data, and IT infrastructure.

When outsourcing operational tasks like customer support, software development, or back-office processing, fintechs must ensure that the arrangement does not violate GDPR (for data protection) or financial regulations set by the National Bank of Romania (BNR) or the Financial Supervisory Authority (ASF). Any outsourcing of regulated functions—such as payment processing or risk management—must be reported to the regulators, and in some cases, prior approval is required.

For fintechs dealing with sensitive financial data, outsourcing to non-EU countries is more complex. Under GDPR, any data transfer outside the EU must either be to a country with an adequate level of data protection (as determined by the EU Commission) or be covered by safeguards like Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).

In short, outsourcing is possible, but fintechs need to carefully navigate data protection laws, regulatory oversight, and cybersecurity requirements. Many companies choose nearshoring (to EU or EEA countries) instead of full offshore outsourcing to simplify compliance and reduce legal risks.

15. What strategies can fintech companies use to effectively protect their proprietary algorithms and software in your jurisdiction, and how does patent eligibility apply to fintech innovations?

Protecting proprietary algorithms and software in Romania—and the EU in general—requires a mix of

intellectual property strategies, since fintech innovations don't always fit neatly into patent law. Unlike in the U.S., where software patents are more common, EU and Romanian laws don't typically allow patents for pure software or algorithms unless they form part of a broader technical invention.

Instead, fintechs rely heavily on copyright law, trade secrets, and contractual protections. In Romania, software is automatically protected under copyright law from the moment it's created, meaning no formal registration is required. However, this only protects the specific code, not the underlying idea or functionality.

For fintech companies looking to protect unique functionalities or algorithms, trade secrets become crucial. Keeping proprietary technology confidential through NDAs (non-disclosure agreements), internal security measures, and controlled access helps prevent unauthorized use. Additionally, registering trademarks for fintech platforms and services can help secure branding and market presence.

If a fintech innovation involves a technical process or hardware integration—for example, a new cryptographic method or an AI-driven fraud detection system—it might qualify for patent protection, but this requires proving that the software contributes to a technical problem with a technical solution. Patent applications must go through the Romanian State Office for Inventions and Trademarks (OSIM) or the European Patent Office (EPO) for broader EU protection.

16. How can a fintech company safeguard its trademarks and service marks to protect its brand identity in your jurisdiction?

Protecting a fintech company's trademarks and service marks in Romania is not just a legal formality—it's a crucial step in securing brand identity and ensuring that no one else can take advantage of the reputation and trust the company builds. The most effective way to achieve this is through trademark registration, which grants exclusive rights over the company's name, logo, slogan, or any other distinctive sign that sets it apart in the financial market. Without this protection, there's always a risk that competitors or bad actors could create confusingly similar brands, potentially misleading customers or diluting the company's presence.

In Romania, trademarks are registered with the State Office for Inventions and Trademarks (OSIM), and once granted, they provide nationwide legal protection. If a fintech plans to expand beyond Romania, it's wise to register the trademark with the European Union Intellectual Property Office (EUIPO) as well, which ensures coverage across all EU countries.

Before applying, it's essential to conduct a trademark availability search to make sure the chosen mark isn't already in use, as disputes over pre-existing trademarks can lead to costly legal battles and even forced rebranding. Once registered, the trademark is valid for 10 years and can be renewed indefinitely, as long as it continues to be actively used.

However, registration alone isn't enough. Fintechs need to actively monitor for potential infringements, as unauthorized use of a brand can cause serious reputational and financial damage. This means keeping an eye on new business registrations, domain names, and even social media accounts that might be attempting to mimic or profit from the company's brand.

Beyond trademark registration, fintechs should also take additional steps to protect their brand identity. Securing relevant domain names early prevents cybersquatting, while reserving social media handles ensures consistency across digital platforms.

17. What are the legal implications of using open-source software in fintech products in your jurisdiction, and how can companies ensure compliance with open-source licensing agreements?

Using open-source software in fintech products can feel like hitting the jackpot—powerful, flexible, and cost-effective, ready to speed up development and innovation. But in a highly regulated industry like financial services, it's not as simple as just plugging in free code and moving on. There are legal strings attached, and if a fintech doesn't handle them properly, those “free" tools could end up costing a lot more than expected.

The biggest issue comes down to licensing obligations. Not all open-source licenses are created equal. Some, like MIT, Apache, or BSD, are quite permissive, letting companies use and modify the code freely without too many restrictions. Others, like GPL or AGPL, come with a catch—if a fintech builds a product using code under these licenses, it may be required to open-source its own proprietary software, something most companies would rather avoid. The worst-case scenario? A fintech unknowingly uses GPL-licensed software in a core product, only to find out later that it has to make its entire platform public. That's the kind of mistake that can kill a business.

Beyond licensing risks, there's also the issue of security and compliance. Financial services deal with highly sensitive customer data, and regulators—whether it's the National Bank of Romania (BNR) or European authorities enforcing GDPR and cybersecurity laws—expect fintechs to have full control over the integrity and security of their software. Open-source components, while incredibly useful, can sometimes contain hidden vulnerabilities or outdated code that expose platforms to cyber threats. If a fintech isn't carefully vetting the software it integrates, it could open the door to security breaches, regulatory fines, and reputational damage.

So how can a fintech stay on the right side of the law while still benefiting from open-source innovation? First, it needs to know exactly what it's using. That means carefully reviewing licenses before integrating any open-source component into proprietary software. Second, having an internal open-source policy—essentially, a rulebook that outlines what's acceptable and what's not—can help developers make smart decisions from the start. Third, fintechs should use automated tools like Software Composition Analysis (SCA) to scan their codebases and identify any risky dependencies before they become a problem.

At the end of the day, open-source software is an incredible asset, but it needs to be handled with care. Fintechs that take a proactive approach—understanding licensing, maintaining strong security practices, and keeping compliance in check—can harness the best of open-source while avoiding legal and operational nightmares.

On a different note, we may point out that to date there has been no national licensing requirement for providers of services related to crypto-assets. Although based on the AML5 package crypto-exchanges and crypto-wallets platforms were required a licence, Romania has not yet enacted the secondary legislation that would have made this effective. If this situation will continue, these crypto-assets service providers (or CASPs) will be not be subject to authorisation until MiCAR applies to them (i.e. 31 December 2024).

We strongly recommend that all market participants offering or planning to offer services related to crypto-assets falling under MiCA seek advice and prepare their compliance accordingly, bearing in mind that all requirements should be met by the end of this year at the latest.

18. How can fintech startups navigate the complexities of intellectual property ownership when collaborating with third-party developers or entering into partnerships?

Establishing a proper intellectual property (IP) ownership framework in partnerships or collaborations with third-party developers is a crucial but sometimes tricky area for fintech startups. When working with external developers or entering partnerships, it's important to clearly define who owns what from the outset. Without a solid agreement, IP disputes can arise later, which could lead to delays, unexpected costs, or even the loss of ownership over key technology.

The first step is always to have clear, detailed contracts in place. These should outline the ownership of any software, algorithms, code, and other innovations that result from the partnership or collaboration. It's also vital to specify who has the right to use or modify the intellectual property, especially if the fintech is relying on third-party developers for critical parts of its platform.

For instance, if a startup hires a developer to build a key piece of software, the contract should include a "work-for-hire" clause, ensuring the fintech retains full ownership of the IP. If the third party is contributing original code, the fintech should request that developers sign an IP assignment agreement to transfer ownership of the code to the company.

Another key consideration is the potential use of open-source software within the product. If this is part of the development process, the startup should ensure they understand and comply with any licensing requirements, as discussed earlier.

When entering into partnerships, it's also important to address joint ownership of any IP created together. In this case, both parties should agree on how the IP will be used, commercialized, and protected. They should also define how any future profits or rights related to that IP will be split.

19. What steps should fintech companies take to prevent and address potential IP infringements, such as unauthorized use of their technology or brand by competitors?

To prevent and address potential IP infringements, fintech companies need to take a proactive approach by both protecting their intellectual property (IP) and being prepared to address any infringements that may arise.

First and foremost, fintechs should register their

trademarks, patents, and copyrights with the relevant authorities, such as the State Office for Inventions and Trademarks (OSIM) in Romania or the European Union Intellectual Property Office (EUIPO).

Next, fintechs should monitor the market and keep an eye on competitors, especially when it comes to the use of their brand and technology. This can include regularly checking domain names, social media platforms, and industry-related developments to spot potential infringements early. Automated tools or IP monitoring services can help track unauthorized use of a brand or technology.

In case of infringement, acting swiftly is crucial. The first step is often sending a legal notice to the infringing party, clearly outlining the violation and requesting that they stop using the IP. If this doesn't resolve the issue, the company can escalate the matter by filing a complaint with relevant authorities, such as the taking civil or criminal legal action through the courts.

Additionally, fintechs can take steps to safeguard their technology by keeping critical innovations confidential through non-disclosure agreements (NDAs) and limiting access to proprietary information within the organization.

Finally, fintechs should ensure their employees and partners are aware of the importance of IP protection and their role in preventing misuse. Training and education about IP rights and confidentiality can help develop a culture of respect for the company's intellectual property.

20. What are the legal obligations of fintechs regarding the transparency and fairness of AI algorithms, especially in credit scoring and lending decisions? How can companies demonstrate that their AI systems do not result in biased or discriminatory outcomes?

When it comes to AI algorithms, especially in areas like credit scoring and lending decisions, fintechs have a legal duty to ensure that their systems are transparent, fair, and non-discriminatory. In the EU, regulations like the GDPR emphasize the need for clear communication about how AI is used and the impact it has on individuals. Customers should know when decisions are being made by AI and understand how those decisions are being reached.

Under GDPR, there's a specific prohibition against relying solely on automated decisions in situations that have a significant impact on the individual, like credit scoring or lending. Fintechs must ensure that human oversight is involved, particularly for decisions that could affect someone's financial standing. This means a human must always be part of the process, either to review or validate the automated decisions, providing the customer with an opportunity for manual review or challenge.

To meet fairness requirements, fintechs need to make sure their AI systems don't unintentionally lead to biased or discriminatory outcomes. For example, AI used for credit scoring mustn't base decisions on factors like race or gender. Regular audits are essential to catch any potential biases, and fintechs need to ensure that their algorithms are trained on representative data that accurately reflects different demographic groups.

To show that their AI systems are fair, fintechs can take a few steps: they can document the design and development process, making sure to explain how the AI works and how fairness is incorporated; use explainable AI techniques so customers and regulators can understand how decisions are made; and create dispute resolution options so people can challenge decisions if they feel they've been treated unfairly.

21. What are the IP considerations for fintech companies developing proprietary AI models? How can they protect their AI technologies and data sets from infringement, and what are the implications of using third-party AI tools?

When fintech companies develop proprietary AI models, protecting both the technology and the data behind them is absolutely essential. For a lot of fintechs, patents are one way to protect their innovations, especially if they've come up with a new algorithm or method. But getting a patent is not always straightforward—AI models often don't meet the strict criteria for patenting. That's where trade secrets come into play. Keeping the details of the AI system confidential, using NDAs, and limiting access to the model are often the best way to protect valuable technology.

But there's another aspect to consider when using third-party AI solutions: while these tools can speed up development, they also come with potential risks. Relying on third-party AI solutions means you may be exposing your proprietary tech and data to outside vendors, which could undermine your confidentiality and trade secrets. The licensing terms of these tools also need to be examined closely. If the third-party AI is restricted in certain ways, it could limit your ability to use the technology or even patent the resulting product. Plus, if the third-party software isn't adequately licensed, there's

a chance that you could unintentionally infringe on someone else's IP.

22. What specific financial regulations must fintechs adhere to when deploying AI solutions, and how can they ensure their AI applications comply with existing financial laws and regulations? Are there specific frameworks or guidelines provided by financial regulatory bodies regarding AI?

When deploying AI solutions, fintech companies must address a complex framework of financial regulations to ensure compliance and mitigate legal risks. Several key regulations apply, and fintechs should be particularly attentive to the EU's regulatory framework as well as local laws, depending on where they operate.

First and foremost, fintechs must comply with GDPR when using personal data to train or implement AI models. AI-driven systems that process personal data must respect data privacy, ensure transparency, and provide individuals with the right to opt-out or contest automated decisions, especially when those decisions significantly affect them, such as in credit scoring or lending.

In addition, MiFID II (Markets in Financial Instruments Directive II) and EMIR (European Market Infrastructure Regulation) in the EU set strict standards for financial market participants, ensuring that AI-driven applications for trading, investment advice, or asset management adhere to these rules. AI models in these areas need to ensure transparency, fairness, and accountability when making decisions that affect investors or market outcomes.

Another significant regulation is PSD2 (Payment Services Directive 2), which aims to open up payment services and ensure security for financial transactions. When implementing AI in payment systems or digital wallets, fintechs must meet the strong customer authentication requirements and ensure that AI doesn't undermine the security or privacy of financial transactions.

Financial regulatory bodies, like the European Central Bank (ECB) and the European Banking Authority (EBA), have recognized the growing role of AI and have started providing specific guidelines. For example, the EBA has released guidelines on outsourcing arrangements, which can impact how fintechs work with third-party providers of AI tools.

23. What risk management strategies should fintech companies adopt to mitigate potential legal liabilities associated with AI technologies?

To manage the legal risks tied to AI technologies, fintech companies need to take a practical, proactive approach that combines compliance with a focus on accountability and transparency.

First, it's crucial to conduct regular audits of AI models to check for biases and ensure fairness. Testing the systems periodically helps identify issues before they become legal problems, especially in sensitive areas like credit scoring or lending decisions. By staying on top of this, fintechs can avoid discrimination and stay compliant with laws.

Another key point is human oversight. AI shouldn't be running the show completely—especially when decisions significantly impact customers, like loan approvals. Having a human involved in reviewing key decisions helps ensure things are handled fairly and responsibly, as required by GDPR and other regulations.

Transparency is also vital. Fintechs should clearly document how their AI systems work—what data is used, how decisions are made, and why. It's important that customers understand how AI is affecting them, and this can prevent misunderstandings and legal disputes.

In short, fintechs need a comprehensive strategy that includes regular audits, human checks, clear communication, and adherence to regulations. By building these practices into the business, fintechs can significantly reduce the risk of legal issues while building trust with customers.

24. Are there any strong examples of disruption through fintech in your jurisdiction?

In Romania, the disruption has occurred in recent years as consumers become more comfortable using most efficient digital services where the transaction can happen instantly and without the limitations imposed by traditional banking services.

The most representative example of fintechs disrupting the traditional financial, payments and insurance system in Romania are contactless mobile payments service providers (Apple Pay or Google Pay) which are daily used by every smartphone holder and Revolut.

After the success of this project, many financial institutions begin to develop new initiatives around

alternative financing. Thus, the emergence of the project Revolut in Romania has pushed the traditional financial institutions to develop a digital strategy and new capabilities to remain relevant.

Nevertheless, as undeniable strike in the fintech industry was done by the cryptocurrencies' adoption as a conventional means of payment.

25. Which areas of fintech are attracting investment in your jurisdiction, and at what level (Series A, Series B, etc.)?

Nowadays one of the hottest topics in EU and in Romania also is around the crypto assets and crowdfunding industry, which since this year is fully effectively regulated at the EU level and it seems to become attractive for institutional investors. On the one hand, crowdfunding platform has managed to attract their own funding, in Romania and reportedly in the Moldavian Republic. On the other hand, they played an important role in funding Series A and Series B of startups active especially in open banking, digital assets, cloud payment services, generative AI, InsurTech, data simulators and finance management applications.

Recent venture capital reports indicate a clearly interest in particular in Series A investments as to Romanian fintech companies.

Contributors

Sergiu-Traian Vasilescu
Managing Partner
sergiu.vasilescu@vdlawgroup.com

Luca Dejan
Partner
luca.dejan@vdlawgroup.com

Bogdan Rotaru
Partner
bogdan.rotaru@vdlawgroup.com