University Economic Bulletin
Vol. 21, No. 1, 2026
Journal homepage: https://ue-bulletin.com.ua/en
Received: 23.12.2025. Revised: 11.04.2026. Accepted: 12.05.2026. Published: 03.07.2026.

UDC 347.734:336.71:004.8
DOI: 10.69587/ueb/1.2026.113

ISSN 2306-546X
ISSN 2414-3774

# Transformation of the institution of banking secrecy amid digitalisation and strengthened financial monitoring

**Svitlana Kushnir**
PhD in Economic Sciences, Professor
Zaporizhzhia National University
69011, 66 Universytetska Str., Zaporizhzhia, Ukraine
https://orcid.org/0000-0002-1410-1887

**Olexandr Pavlov***
Student
Zaporizhzhia National University
69011, 66 Universytetska Str., Zaporizhzhia, Ukraine
https://orcid.org/0009-0009-7171-6835

**Abstract.** This article aimed to provide a detailed theoretical and methodological foundation and evaluation of the institutional development of banking secrecy in response to the introduction of artificial intelligence technology, the rules of the Automatic Exchange of Information, the Common Reporting Standard, and the creation of central bank digital currencies. The methodological foundations were a dialectical method, methods of system-structure analysis of the financial markets, as well as the qualitative methods of case study on the history of the implementation of regulations on banking secrecy in Switzerland, as the main model for the development of banking confidentiality, as well as the experience of their implementation in Germany, Singapore, the United Kingdom and Ukraine. In order to make a comparative analysis of the process of intensification of the disclosure of transaction data by the subjects of the primary level of financial monitoring, objective systematisation of empirical data was conducted with the use of methods of graphical and table modelling. In the course of research, the established trend has been identified to transform the banking sector from the position of complete capital anonymity to the principles of the "glass client", under which the banking secrecy of the client turns from a means of legal secrecy to the technological protocol of regulated control of access to data. A stable trend was identified towards annual growth in the volume of automatic tax data exchange, amounting to 10-12% per year in Switzerland. This confirmed the erosion of offshore secrecy under the requirements of the Financial Action Task Force and the Organisation for Economic Co-operation and Development. The study substantiated the specific features of Ukrainian compliance under martial law, where the implementation of Resolution No. 65 of the National Bank of Ukraine and instant verification through the Diia ecosystem automatically discloses data to financial intelligence bodies without judicial authorisation. It was established that the launch of central bank digital currencies, such as the e-hryvnia and the digital franc, together with algorithms for continuous AI-based transactional scoring, de facto removes banking intermediation, turns privacy into a programmable option, and shifts legal protection towards cyber resilience and concepts of decentralised identity. The practical value of the findings lies in their possible use by the National Bank of Ukraine and commercial banks to optimise risk-based supervision algorithms, develop regulatory legal acts on the protection of a client's financial profile against cyberattacks, and build a balanced model of "digital trust"

**Keywords:** automatic exchange of information; Switzerland; risk-based approach; artificial intelligence; scoring

**Suggested Citation:**
Kushnir, S., & Pavlov, O. (2026). Transformation of the institution of banking secrecy amid digitalisation and strengthened financial monitoring. *University Economic Bulletin*, 21(1), 113-126. doi: 10.69587/ueb/1.2026.113.

*Corresponding author (pavlovalexander129@gmail.com)

## INTRODUCTION

In the contemporary global financial architecture, the institution of banking secrecy is undergoing its most extensive transformation in centuries. The traditional approach to the definition of banking secrecy as an absolute and uncontrollable guarantee of confidentiality of private banks is gradually fading under the influence of two global processes: the digitalisation of all spheres of life and a sharp increase in the intensity of financial monitoring. Currently, the bank itself is transforming from a "safe for secrets" to an institution of the state's control, which is required to adhere to the Know Your Customer (KYC) principle and verify the source of a customer's wealth to a greater extent than any other authority. Digitalisation not only provides greater opportunities to use banking services, but also creates new possibilities for using artificial intelligence of financial intelligence units to analyse financial flows, making it totally transparent. In the course of the worldwide struggle against money laundering, terrorist financing, and tax evasion, the privacy of clients is being replaced by financial security at the international level. For Ukraine, this issue is sharpened by the need to adapt national regulatory standards to the requirements of the European Union (EU) under martial law. This requires maximum transparency in capital movement without capitulating to the risks of a complete loss of trust among market participants. Analysis of recent studies and publications. The transformation of the legal and economic boundaries of financial confidentiality in the era of digitalisation is actively discussed in contemporary scholarship. A study by F.A. Siena (2022) analysed the paradigm shift in banking supervision in EU countries. The author demonstrated that the concept of absolute financial privacy has definitively lost its legitimacy, giving way to the principle of "managed transparency" in the interests of public law. Anderson emphasises that law enforcement bodies obtain unhindered access to accounts without the traditionally complex judicial procedures.

The issue of introducing regulatory technologies into anti-money laundering processes was examined by P. Tertychnyi *et al.* (2022). The scholars assessed the effectiveness of automated customer verification systems and noted that new digital compliance tools minimise the human factor, while at the same time turning commercial banks into direct instruments of state monitoring. According to their findings, banking secrecy is, in effect, transformed into an internal algorithm for data authorisation. The case of the transformation of the Swiss financial sector and the final dismantling of the system of anonymous accounts under the influence of the global standards of the Organisation for Economic Co-operation and Development (OECD) was analysed by S.S. Yeh (2023). The researcher focuses on the risks of capital outflow from Switzerland to jurisdictions with less stringent regulation following the introduction of the Common Reporting Standard (CRS) for the automatic exchange of information. S.S. Yeh argued that Swiss institutions were compelled to build new competitive advantages based not on secrecy, but on the technological security of assets.

The influence of artificial intelligence technologies on the detection of anomalous financial transactions was examined by M. Bakhshi *et al.* (2020). The authors described mechanisms of behavioural scoring that enable neural networks to monitor users' transactional activity continuously. It was substantiated that such comprehensive preventive control fully erodes the classical meaning of the confidentiality of a bank account. The specific features of implementing the concept of open banking, as well as the legal conflicts that arise when customer data is transferred to third parties through application programming interfaces (APIs), were studied by C. Amalia *et al.* (2022). The authors demonstrated that the integration of financial institutions with fintech companies blurs the traditional legal boundaries of responsibility for preserving secrecy. They proposed shifting the regulatory focus from restricting access to protecting personal data against cyber threats. The risks to individual privacy associated with the design and future launch of central bank digital currencies (CBDCs) were analysed by A. Jabbar *et al.* (2023). The authors critically assessed the architecture of distributed ledgers for digital money and argued that the issuer's direct control over each wallet de facto abolishes the institution of banking intermediation in relation to the preservation of confidentiality. A. Jabbar *et al.* also considered the prospect of new forms of "digital surveillance" by the state.

Despite the existence of substantial studies addressing the general issues of financial digitalisation and the legal aspects of financial monitoring, researchers have not yet given sufficient attention to a comprehensive assessment of the transformation of banking secrecy as a transition from a legal instrument of protection to a purely technological protocol for access management. The synergistic effect of the simultaneous introduction of artificial intelligence systems, CRS standards, and the integration of banks with state digital platforms under the legal restrictions of martial law remains insufficiently studied. This necessitates a rethinking of the very concept of financial privacy. This study aimed to analyse the transformation of the institution of banking secrecy under the influence of digitalisation, artificial intelligence, CBDCs, and strengthened financial monitoring.

## MATERIALS AND METHODS

This study used a qualitative design, theoretical and methodological analysis, and institutional modelling of the legal and economic transformation of the financial sector. The research type was combined, consisting of a theoretical foundation and an in-depth analysis of the concept of confidentiality, as well as an applied assessment of the implementation of technological and regulatory mechanisms. The object of the study was the process of transformation of the institution of banking secrecy under the influence of total digitalisation and stricter financial monitoring requirements. The research covered all legal and economic aspects of relations between commercial banks, their clients and the state's supervisory institutions for issues of

disclosure and protection of information about transactions. The source base was formed through purposive sampling of official reports and standards issued by international organisations, in particular the Financial Action Task Force (FATF, 2025) and the Swiss Financial Market Supervisory Authority (FINMA, 2025). Among Ukrainian legal acts, the study considered Resolution of the Board of the National Bank of Ukraine No. 65 (2020), as well as specialised academic periodicals published between 2019 and 2025, including studies by Z.M. Dovhan & Y.M. Halitseiska (2021) and V. Krasovskyi (2024). The study applied a qualitative case-study method to examine the experience of Switzerland and Ukraine. The choice of Switzerland is justified by its status as a historical benchmark of banking confidentiality, whose forced transition to the Automatic Exchange of Information (AEOI) (2020) and the Common Reporting Standard (CRS) (2025) reflects the global dismantling of offshore anonymity. The choice of Ukraine is determined by the exceptional pace of digitalisation in its banking system, its unique experience of instant customer verification through the Diia (n.d.) ecosystem, and the specific features of implementing a risk-based approach under martial law. The research tasks were carried out in stages using a set of mutually complementary methods. In particular, historical-legal and dialectical methods were used to identify patterns in the evolution of banking secrecy from the classical paperbased model to the digital model. Comparative analysis was applied to compare international regulatory practices, as well as the level of privacy in traditional bank accounts and central bank digital currency (CBDC) wallets. Systemic and structural analysis served as a tool for examining the influence of artificial intelligence (AI) technologies and Open Application Programming Interfaces (APIs) on the formation of the "glass client" model and for assessing the degree of integration between banks and state registers. At the final stage of the study, theoretical generalisation and the abstract-logical method were used to formulate the authors' conclusions on the contours of the future architecture of "digital trust".

## RESULTS AND DISCUSSION

Historically, banking secrecy emerged as an instrument for protecting private property and commercial information. However, in the 21st century, a paradigm shift can be observed: from absolute anonymity to "justified transparency". The experience of Switzerland is particularly illustrative in this context. The country, which made banking secrecy part of its national code as early as 1934, was forced, under pressure from the Organisation for Economic Co-operation and Development and the United States of America (USA), to dismantle the system of numbered accounts and move towards the CRS (Meier *et al*., 2023). This indicates that the digital era leaves no room for "grey zones". Banking secrecy now protects the client from unauthorised access by third parties, such as hackers and competitors, but it is fully open to tax and law enforcement authorities within the limits of the law. The transformation of conceptual approaches to the essence of banking secrecy is clearly visible when its classical and digital models are compared. Under the 20th-century classical paradigm, the main priorities were absolute anonymity for the client and preventing outside interference in clients' capital. Today, the digital model has moved in the other direction, to transparency and a relentless anti-money-laundering fight. Accordingly, the access to the information has changed: the information was revealed by criminal cases under the court decision before, while today in banking, it is disclosed under CRS and on request (Meier *et al*., 2023). The technological basis of control has evolved from paper-based documentation and the subjective human factor to the introduction of AI algorithms, Big Data tools, and end-to-end blockchain monitoring (FINMA, 2025). This has led to a fundamental change in the role of the financial institution itself: the bank has been transformed from a custodian of secrecy and a trusted representative of the client into a primary financial monitoring entity that de facto performs the functions of a state agent. This evolution is most clearly reflected in the change in the Swiss standard, where legendary anonymous numbered accounts and strict criminal liability for data disclosure have been replaced by full reporting by financial institutions to the Swiss Federal Tax Administration. For a deeper understanding of these processes, it is worth analysing precisely how digitalisation has changed the technical possibility of preserving secrecy. In the past, information was stored in paper archives, access to which required a physical visit and lengthy legal procedures. Today, however, every transaction generates a digital footprint that is available to the regulator in real time. The introduction of Big Data systems enables banks to score clients not once a year, but continuously, by analysing behavioural anomalies that automatically trigger the disclosure of information within the framework of financial monitoring.

When considering the case of Switzerland, it should be noted that the transformation of the institution of confidentiality began not because of technical failures, but as a result of strong external political pressure. For a long time, the Swiss Confederation uncompromisingly defended Article 47 of the Federal Act on Banks and Savings Banks, which provided for criminal liability and actual imprisonment for the disclosure of client data (Mahdi *et al*., 2024). However, by 2024-2025, the situation had changed, and the country had become one of the leaders in implementing the standard of automatic exchange of information. According to official data from the Swiss Federal Tax Administration, the number of financial accounts covered by AEOI procedures has been growing steadily by 10-12% annually, covering data on more than 3.6 million accounts held in partner states. This has, in effect, eliminated classical offshore anonymity (Exchange of information with 104 countries…, 2023). Analysis of the Swiss experience demonstrates that the removal of banking secrecy has led to massive restructuring of the redistribution of cross-border capital. During the period of sharp change, the outflow of "undeclared" offshore funds of the small and medium

private Swiss banks from the total of 15-18% of assets was observed. At the same time, the market underwent forced consolidation. The largest conglomerates, such as UBS, were able to offset this outflow by reorienting themselves towards the lawful onshore segment and capital management in Asia. According to regulatory reports, the assets under management (AuM) of the merged UBS giant after the acquisition of Credit Suisse exceeded USD 5.7 trillion. This confirms the shift from a strategy of "asset concealment" to a strategy of "technological management and transparent security" (FINMA, 2025).

An important quantitative indicator of the uncompromising nature of the new compliance era has been the unprecedented financial sanctions imposed on financial institutions for violations of financial monitoring rules and tax agreements. A striking example is the long-running investigations by the US Department of Justice and the Swiss regulator FINMA into Credit Suisse, which resulted in total penalties of more than USD 2.5 billion for assisting in the concealment of assets from taxation. Even UBS, the market leader, was compelled, in similar international cases, including claims brought by the French tax authorities, to pay final penalties and compensation amounting to 1.8 billion EUR (FINMA, 2025). This particular amount of financial losses shows that the preservation of clients' "grey" secrets is no longer profitable for banks. To maintain a high degree of objectivity of the research, the Swiss experience should also be supplemented by a review of other global regulatory models, for example, of different approaches to the narrowing of banking secrecy. The United States has built a unique model in which banking confidentiality is fully subordinated to national security interests through the mechanisms of the Financial Crimes Enforcement Network (FinCEN). Under the Anti-Money Laundering Act of 2020 (n.d.) and the Corporate Transparency Act of 2019 (2019), FinCEN obtained unhindered digital access to companies' beneficial ownership information and banks' transactional activity. The US model has transformed banks into direct intelligence informants: where transactions exceeding USD 10,000 or any suspicious activity are detected, a bank is required to submit a Suspicious Activity Report automatically. Any attempt to conceal client data is punishable by multi-billion-dollar fines and exclusion from dollar clearing, which makes the US model the most aggressive form of capital deanonymisation in the world. While the US model focuses on state financial control, the experience of the EU demonstrates the dismantling of banking secrecy under the influence of market digitalisation and consumer rights protection. The implementation of Directive (EU) 2015/2366 (2015) established the mandatory nature of the concept of open banking. According to a study by M. Polasik *et al.* (2024), European legislation compelled traditional banks to open up access, free of charge, to their clients' accounts and transaction histories for third parties, namely technology-based fintech companies, through application programming interfaces (Open APIs). Thus, the monopoly of banks over financial secrecy in the EU was eliminated by law in favour of market competition and the creation of "transparent client" ecosystems.

The analysis of empirical data on the practical implementation of the AEOI standard (2020) in Switzerland made it possible to identify stable trends towards the globalisation of financial control and to reveal the hidden mechanisms of capital de-shadowing. The data presented by E. Baselgia (2023) demonstrate stable exponential growth across all three key descriptors: geographical coverage, the volume of transactional data and the number of institutions involved. The results of the analysis of automatic financial information exchange indicators show the consistent strengthening of international tax transparency and the expansion of the institutional scope of the AEOI mechanism. Between 2019 and 2025, the number of Switzerland's partner states involved in automatic data exchange increased from 75 to 110, representing a total growth of 46.7%. The most intensive expansion of the cooperation network was observed in 2019-2021, when the indicator increased by 28%. This points to the active adaptation of the international regulatory architecture to transparency standards after the completion of the transitional stages of CRS implementation. At the same time, there is a general increase of 22.6% from 3.1 million to 3.8 million for the total of transferred financial records related to non-resident bank accounts (Exchange of information with 75 countries…, 2019; Exchange of information with 110 states…, 2025).

The trend mentioned above testifies to a deeper integration of different jurisdictions' financial systems and to a more efficient use of tools for controlling cross-border capital flows. Moreover, the number of financial institutions covered by reporting requirements has increased from ~7,500 to 9,500, or 26.7%, during the same period (Exchange of information with 110 states…, 2025). This suggests that banking reporting requirements are expanding not only to banking institutions, but also to investment funds, trusts, insurance companies, and so on, which significantly limits opportunities to use alternative financial intermediaries to evade monitoring and information exchange. It needs to be noted that the identified trends have direct macroeconomic and legal consequences. First of all, the increase in automatic exchange of information resulted in a cumulative growth of the national tax receipts of the partner countries, according to the report of the State Secretariat of International Finance (SIF, 2025). The receipt of financial intelligence on foreign assets enabled fiscal authorities to use voluntary disclosure mechanisms, including capital amnesties, and to carry out additional assessments of tax liabilities. Second, the shift from a request-based system to the CRS has fundamentally increased the effectiveness of detecting and preventing financial crime. Regulatory AI algorithms are now able to conduct end-to-end retrospective analysis of transactions, identifying complex schemes of capital splitting, cross-border money laundering and the financing of illegal activities as early as the transaction-structuring stage. Changes in AEOI indicators in Swiss practice are shown in Table 1.

**Table 1.** Dynamics of Switzerland's AEOI indicators

| Year | Number of partner countries for exchange | Growth rate of geographical coverage compared with 2019 (%) | Number of account records transmitted (million) | Growth rate of data volume compared with 2019 (%) | Number of participating financial institutions |
|---|---|---|---|---|---|
| 2019 | 75 | - | 3.1 | - | ~7,500 |
| 2021 | 96 | +28.0 | 3.3 | +6.4 | ~8,200 |
| 2024 | 104 | +38.7 | 3.7 | +19.3 | ~9,000 |
| 2025 | 110 | +46.7 | 3.8 | +22.6 | ~9,500 |

**Source:** developed by the authors based on Exchange of information with 75 countries… (2019), E. Baselgia (2023), SIF (2025), Exchange of information with 110 states… (2025)

The indicators presented demonstrate the transition from a model focused on banking confidentiality to a model of systematic international information exchange, in which the key priorities are tax transparency, interstate cooperation and digital control over cross-border financial flows. In Ukraine, this process is being synchronised with European standards. The accession of the State Tax Service of Ukraine to the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information of the OECD (2014) means that the banking secrecy of Ukrainian residents abroad and non-residents in Ukraine has ceased to be an obstacle to tax control. Digitalisation has introduced open banking into banking practice. The use of open APIs allows clients to transfer their data to third-party services in order to obtain better financial offers. However, this creates a paradox: on the one hand, clients voluntarily "dismantle" their own secrecy for the sake of convenience; on the other hand, the bank remains responsible for the security of this data. Thus, the contemporary transformation of the institution of banking secrecy shifts the emphasis from nondisclosure to access management. A separate aspect is the strengthening of financial monitoring in Ukraine under martial law and digitalisation. The risk-based approach introduced by the National Bank of Ukraine (NBU, n.d.b) requires banks to block automatically any transactions that do not correspond to a client's financial profile. In this case, banking secrecy is automatically disclosed to the State Financial Monitoring Service without judicial involvement. According to data from the Structured Financial Messaging System (SFMS, 2024), analytical processing of large volumes of suspicious transactions made it possible to identify and block financial flows of illegal origin amounting to more than UAH 7.3 billion in equivalent value. This was accompanied by the transfer of more than 1,100 summarised case materials to law enforcement agencies. Quantitative analysis of these data indicates a shift in the compliance system from retrospective recording to preventive blocking, where the bank de facto becomes the first censor by implementing a model of "presumption of transparency".

In the academic literature, the concept of the "glass client" is used as a metaphor for the increased digital transparency of financial behaviour under conditions of open banking, AEOI and expanded compliance. However, it should be borne in mind that the term is more of an analytical construct than a unified regulatory definition. As D. Lyon (2018) and S. Zuboff (2019) noted, its meaning fits logically into the broader discussion of the datafication of financial services and the reduction of information asymmetry between the client, the bank and the regulator. In this context, R. Alt *et al.* (2018) distinguish between two interpretative approaches. The optimistic viewpoint considers full transparency, which is being achieved via digital means, to be a tool for lowering the costs of financial transactions, raising the efficiency of scoring and reducing information asymmetries in financial markets. Conversely, the critical approach points to the dangers of the emergence of a "digital panopticon" in the sphere of banking activity, where there is a constant control over the actions and patterns of movement of clients' money, which eventually threatens the loss of privacy and the possibility of influencing client behaviour via risk-assessment systems using algorithms (Lyon, 2018). In this regard, the concept of the "glass client" falls within the framework of the broader theory of surveillance capitalism and algorithmic control, and is not an independent category within the theory of banking law. Within the framework of Big Data technologies and predictive analytics, a financial institution is able to identify previously imperceptible connections between counterparties that were previously inaccessible to human observation. This changes the very nature of monitoring: banking secrecy ceases to be a protective shield and is transformed into a tool to select transactions that meet certain standards of legitimacy. Of particular note is the role of AI, which is implemented in compliance systems of large banks. In the Ukrainian market, more than 85% of first- and secondtier banking institutions have optimised their processes through leading technology platforms, such as SAS Anti-Money Laundering (AML) and NICE Actimize (FINMA, 2025). Algorithms are programmed not only to analyse the transaction amount, but also the place of its occurrence, the time of its occurrence, the device used by the client, the time of logging in from a specific device and even user habits (e.g. data-entry speed, usual money transfer paths). As S. Zuboff (2019) claims, the use of such platforms as SAS AML allows the financial institutions to cut down the number of false positives by 35-40%, while improving the accuracy of identification of complex schemes of shadow capital splitting by 22%. Such a level of control renders the classical banking secrecy practically inapplicable in the internal systems of the bank and, therefore, in the regulatory bodies that have the right to view such aggregated data.

Within the scope of tightened financial monitoring in Ukraine, attention should also be drawn to banking systems integration with the state registers and Diia (n.d.) ecosystem. This makes it possible to conduct remote identification and verification (e-KYC) within minutes. However, the downside of this convenience is the concentration of vast amounts of confidential information in digital clouds. The transformation of the institution of banking secrecy is manifested here in the fact that legal protection shifts from the very fact of "having an account" to the "protection of personal data against leakage" (Mahdi *et al*., 2024). In other words, in this case, the state no longer promises the client that it will not analyse their accounts; instead, it promises that third parties will not be able to use this data because of technical weaknesses in the system. The introduction of advanced digital tools into banking practice has not merely automated operational processes, but has fundamentally changed the physical and legal nature of data confidentiality. The evolution of technology creates specific challenges for the classical institution of banking secrecy, forcing regulators to balance financial transparency with cybersecurity (FINMA, 2025). The study results suggest that the influence of digital technologies has brought about structural changes in banking secrecy and monitoring systems. Distributed ledger changes the traditional pattern of a closed banking system to an open one by ensuring full transaction visibility and real-time transaction traceability, especially concerning crypto assets connected with illegal transactions. The use of cloud infrastructure for the storage and maintenance of banking databases blurs the traditional approach to the division of banking secret protection and maintenance between financial institutions and technology providers. The spread of biometric authentication reduces the possibility of anonymous account management and strengthens the personalisation of financial transactions (Jain *et al*., 2011). At the same time, the development of open banking and API integrations deepens interaction between banks and fintech services, thereby improving the efficiency of financial services while complicating the determination of the boundaries of responsibility for data protection (Alt *et al*., 2018). The role of technologies in the development and transformation of the concept of banking secrecy is summarised in Table 2.

**Table 2.** The impact of digital technologies on components of banking secrecy

| Technological solution | Impact on confidentiality | Result for financial monitoring | Practical examples and implementation tools |
|---|---|---|---|
| Blockchain & distributed ledger technology | Transparency of transactions in public networks | Possibility of tracking "dirty" crypto-assets up to the point at which they are converted into fiat currency | Use of Chainalysis KYT and Elliptic analytical platforms to label and block tokens with a criminal history |
| Cloud computing | Storage of data on third-party servers operated by providers | Need to delimit access between the bank and major IT companies | Migration of banking Big Data to Amazon Web Services clouds; risks of data compromise through vulnerabilities in third-party software |
| Biometric ID | Replacement of passwords with fingerprints and Face ID | Impossibility of anonymous account management through nominees | Remote identification systems such as Apple Face ID and Android Biometric, as well as state e-KYC algorithms within the Diia ecosystem |
| Open API | Third-party applications' access to account balances | Blurring of responsibility for preserving the secrecy of transactions | Integration of bank accounts with fintech services through PSD2 API protocols; data leaks at the processing stage by third-party personal finance management applications |

**Source:** developed by the authors based on Directive (EU) 2015/2366 (2015), FINMA (2025), Diia (n.d.)

As Table 2 shows, the digital technologies have systematically modified classical components of banking secrecy and gradually shifted it from the field of the protective function to the control through transparency and algorithmic monitoring. As for the impact on financial monitoring, the situation is ambiguous: on the one hand, the ability to identify and track risky transactions has been upgraded; on the other hand, the boundaries between liability have become less clear and new cyber and compliance risks have increased. It is also worth considering in greater detail the issue of combating tax evasion, which became the main driver of reforms in Switzerland. Forced to accept the fact that the US Department of Justice, as well as the European Commission, had to charge Swiss banks with multi-billion-dollar fines for the fact that they helped foreigners hide their assets. This led to a radical overhaul of national legislation and the adoption of the government's White Money Strategy. This was confirmed through tighter requirements set out in the Federal Act on Combating Money Laundering and Terrorist Financing in the Financial Sector and the corresponding regulations of the State Secretariat for International Finance (SIF, 2025). According to this strategy, Swiss banks should accept only such funds for which there is an undisputable confirmation of tax payment in the client's home country. This differs radically from the situation 20 years ago, when the origin of funds was rarely checked unless the amount was linked to obvious criminal activity. In the current regulations of the FINMA (2025), there is a provision that financial organisations shall carry out tax control for each of the foreign client's assets from origin to destination. Thus, the burden to justify the fiscal security of the funds falls on the account holder, under the threat of immediate blocking of the account and reporting a suspicious transaction to relevant authorities.

In the Ukrainian context, the strengthening of financial monitoring has its own specific features, linked to

adaptation to FATF standards and the requirements of the International Monetary Fund. The introduction of the institution of politically exposed persons (PEPs) and the establishment of lifelong status for them constitute a direct limitation of banking secrecy for a specific category of citizens, as regulated by the SFMS (2024) and Law of Ukraine No. 361-IX (2025). For such persons, the idea of confidentiality of transactions is not relevant: for them, the bank is required to carry out additional checks for each of their transactions, regardless of amounts. This sets a precedent for the segmentation of banking secrecy, as in this case, the secrecy will be "selective", depending on the person's social and political status. In this way, the implementation of the risk-oriented approach has resulted in radical changes to the classical banking secrecy, as the absolute and uniform legal norm turned into a flexible control tool. In the modern regulatory framework of compliance control, the concept of deepening the client base segregation has been implemented; the level of secrecy of information and the level of the provision of information depend directly on the risk group of the client. The differentiation of the level of banking secrecy in contemporary financial monitoring practice is based on the risk-based approach. For low-risk clients, who are characterised by transparent sources of income and standard financial behaviour, basic identification procedures and periodic data updates are applied, while transaction monitoring is largely limited to detecting atypical transactions that exceed established thresholds. For medium-risk clients, KYC requirements are strengthened, involving regular verification of information and selective checks on the origin of funds when non-standard financial activity is detected. For high-risk clients, including PEPs and citizens from countries with high money laundering and terrorist financing risk, an increased level of due diligence is provided, which implies constant monitoring of clients, an expanded list of documents that confirm the source of funds, and an expanded scope of transaction control (Table 3).

**Table 3.** Levels of client verification intensity within financial monitoring

| Client category | Level of secrecy disclosure | Frequency of data updates | Need to confirm the source of wealth |
|---|---|---|---|
| Low risk | Basic level: Identification | Once every 3-5 years | Only when limits are exceeded |
| Medium risk | Standard level: KYC | Once every 2 years | Selectively, at the bank's request |
| High risk: PEPs | Enhanced level: Enhanced Due Diligence | Annually and lifelong | Mandatory for all transactions |

**Source:** developed by the authors based on SFMS (2024), Law of Ukraine No. 361-IX (2025)

According to Table 3, the financial monitoring practice is based on the risk-oriented approach for the segregation of levels of confidentiality of information. For the clients that are low risk, the following approach is applied: simplified identification, periodic update of data, and selective control of anomalous transactions. For medium-risk clients, the enhanced KYC procedure is applied, which includes the periodic updating of the client's information, as well as selective checking of the origin of funds in the case of anomalous activities. The next important aspect is the digitalisation of the process of reporting suspicious transactions. In Ukraine, due to the automation of data exchange between banks and the State Financial Monitoring Service on the basis of updated electronic protocols, the average time required to process and transmit information on critical financial risks has been reduced from several days to real-time or a few hours (SFMS, 2024). This enabled the regulator to respond preventively to suspicious financial flows before capital was fully split and moved into the shadow economy. A special place in the contemporary transformation of banking secrecy is occupied by the so-called "Travel Rule" developed by FATF (2025). This rule requires financial institutions, including virtual asset service providers, to collect and transmit the personal data of both the sender and the recipient when transactions are carried out. For the banking sector, this means the complete dismantling of the remaining elements of anonymity, even in cross-border transfers, which were previously regarded as one of the most protected areas of confidentiality. Digitalisation makes it possible to automate this process: each transaction is accompanied by a "digital passport", which makes banking secrecy transparent to the network of correspondent banks and state regulators worldwide.

Under martial law in Ukraine, the institution of banking secrecy has been subject to additional restrictions arising from national security needs. The NBU significantly expanded its powers to monitor the accounts of persons associated with the aggressor state and introduced mechanisms for the immediate blocking of assets. A comparative analysis of the dynamics of sanctions compliance demonstrates a radical shift in the paradigm. Before 2022, asset-blocking mechanisms based on decisions of the National Security and Defence Council were used as an exceptional instrument, while the legal regime of banking secrecy protected the accounts of most foreign residents until a court judgment was issued. The number of blocked entities was limited to isolated cases, and the volume of frozen funds had no systemic effect on the liquidity of the sector. After 2022, while the country is under martial law, banking secrecy has turned into an instrument of sanctions policy. Banks must not only store information, but also proactively search for a match in the sanctions lists. That is why the continuous accounting of all client assets by law enforcement and security bodies can be considered. Compared to the pre-war figure, in 2022-2025, according to regulatory data, the number of subjects with blocked accounts according to codes relating to terrorism financing and connections with the aggressor state has grown 15 times, and the amount of preventively frozen assets and associated funds amounted to billions of the national currency (SFMS, 2024).

Another important aspect is the development of systems for the automated exchange of tax information under the CRS standard, following Ukraine's official accession in August 2022 to the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information (Ukraine joined the Multilateral Competent…, 2022). The Ukrainian tax authorities receive data on the account balances of Ukrainian residents in more than 100 countries worldwide, including Switzerland, Luxembourg and Cyprus. This means that "external" banking secrecy has effectively ceased to exist for Ukrainians as a means of concealing income. The digital platforms of the tax service automatically compare the data received with citizens' declarations, making any discrepancies grounds for initiating proceedings (Ukraine joined the Multilateral Competent…, 2022). In analysing Switzerland's experience during this period, attention should be paid to the activities of FINMA (2025). This authority has received unprecedented powers to inspect banks' internal compliance systems. Whereas in the past a Swiss banker could refuse to provide information to law enforcement bodies by referring to the criminal provision on the disclosure of secrecy, today refusal to provide data to the regulator is itself a criminal offence. Digitalisation has also created new challenges related to cybersecurity. Since banking secrecy is no longer a "secret" from the state, the main risk has shifted towards unauthorised access by hacker groups. The transformation of the institution in this direction lies in the fact that banks now report not only suspicious client transactions, but also any attempts to compromise their databases. Thus, client confidentiality is no longer determined by the "silence" of a bank employee, but by the reliability of the encryption and the response speed to cyber attacks. Today, the notion of banking secrecy is partially replaced by the broader term "financial privacy in the digital environment", encompassing not only balance data but also the metadata, digital signatures, and interaction history with financial software.

The issue of "open banking" and its influence on the erasure of secrecy also deserves special consideration. Under Directive (EU) 2015/2366 (2015), Ukraine is actively implementing, and banks provide third-party service providers with the opportunity to access clients' accounts with consent from such a client. That is why, in the case of open banking, the banking secrecy has an attribute of "shared use". Upon agreeing with the financial aggregator or payment service provider, the client removes data from the sphere of banking secrecy and places it in the context of commercial processing of personal data. Digitalisation is therefore an agent of the process of destruction of the bank monopoly over information on clients. To comprehend the scale of these changes in Ukraine, it is necessary to analyse the Regulation of the Board of the National Bank of Ukraine No. 65 (2020). This document essentially became the "manifesto of digital transparency", defining the transition from formal control to a risk-based approach. The regulation provides for the continuous monitoring of not only the content of the transaction, but also the purpose of the operation and its conformity to the client's financial profile. Owing to the introduction of automated analytical algorithms, any transaction that appears illogical to the system or lacks documentary confirmation of the origin of funds automatically causes banking secrecy to give way to the bank's obligation to notify the State Financial Monitoring Service. A specific feature of the current stage is that the right to confidentiality now directly depends on the client's ability to explain promptly every step taken in the digital space and to provide electronic evidence of the legitimacy of transactions. Thus, Resolution of the Board of the National Bank of Ukraine No. 65 (2020) has transformed banking secrecy from a "legal veil" into an "intelligent filter", where the client's level of privacy is directly proportional to their level of financial transparency.

One of the most radical challenges to the institution of banking secrecy in the coming decade is the introduction of CBDCs, such as the e-hryvnia in Ukraine, the digital euro in the EU and the digital franc in Switzerland. Unlike traditional non-cash money held on the balance sheets of commercial banks, CBDCs constitute a direct liability of the monetary regulator (About e-hryvnia, the digital currency…, n.d.; ECB, n.d.; Will the Swiss franc…, n.d.). However, the state's level of access to transactional data is not universal and varies flexibly depending on the architectural model and the technological principle on which the platform is built (BIS, 2023). Different models may involve direct access by the central bank to information, access through financial intermediaries within a two-tier architecture, or limited access based on the principle of privacy by design. In its analytical materials, the BIS (2023) notes three main models of CBDC confidentiality as mechanisms of implementation of the financial privacy transformation process:

1) Account-based model: this involves full user identification, where each transaction is strictly linked to a digital profile;

2) Token-based model: this focuses on verifying the authenticity of the digital token itself rather than the identity of the person, making it possible to ensure a higher level of pseudonymity for retail payments;

3) Tiered anonymity: this is the most balanced option and is being actively tested in the digital euro project. It provides full confidentiality and no monitoring for small everyday offline payments, while large transactions remain subject to standard KYC/AML procedures.

The scale of the global trend is confirmed by the fact that more than 130 countries, representing over 98% of global GDP, are currently researching, testing or have already launched their own CBDCs (ECB, n.d.). The largest retail pilot in the world is China's e-CNY, with transactions under its testing already exceeding hundreds of billions of yuan. This demonstrates the technical capacity of the state to exercise centralised real-time oversight of capital flows (Tan *et al.*, 2025). In turn, the NBU became one of the first regulators in the world to begin practical testing, having implemented the e-hryvnia pilot project

as early as 2018 by issuing a limited volume of tokens to test retail payments (NBU, n.d.a). The current concept for the introduction of the e-hryvnia defines it as a payment instrument, the functioning of which will be realised within a two-tier scheme with commercial banks as identification agents. Consequently, CBDCs do not necessarily mean that financial privacy is completely abolished; it only means a different character of financial privacy: instead of classical banking secrecy that is provided by commercial financial institutions as a protection tool, there is a regulated, techno-logically configured regime of transaction data access where anonymity can be controlled by an adjustable parameter in the software code. The transformation of the institution of financial confidentiality becomes most evident when the traditional banking system is compared with different architectural configurations of central bank digital currencies. Where in traditional banking, access to confidential information is always subject to certain legal procedures, in a CBDC regime, the level of transparency of transactions is solely determined by the technical parameters of the platform. A comparison of CBDC models is presented in Table 4.

**Table 4.** Comparative analysis of access to data in traditional banking and different CBDC models

| Characteristic | Traditional accounts | Direct CBDC model, based on elements of e-CNY | Intermediated/hybrid CBDC model, based on the e-hryvnia concept | Limitedaccess/ privacybydesign model, based on the digital euro |
|---|---|---|---|---|
| Data custodian | Commercial bank | Central bank as a monetary regulator | Distributed architecture: commercial bank and central bank | Decentralised local devices/ protected central bank register |
| Data request procedure | Official request or court decision | Direct monitoring in the central ledger | Request through an intermediary bank; automated AML screening | Automatic disclosure only when limits are exceeded or investigations are initiated |
| Level of anonymity | Relative, protected by banking law | Minimal, with full transparency for the issuer | Controlled, with identification through financial agents | Tiered anonymity: full anonymity for small offline amounts |
| Role of the state | External observer and supervisory authority | Direct operator and verifier of transactions | Co-operator and architect of monitoring rules | Technological guarantor of compliance and confidentiality protection |

**Source:** developed by the authors based on BIS (2023), H. Tan *et al.* (2025), ECB (n.d.), NBU (n.d.a)

The findings on models of access to financial data make it possible to identify several basic approaches. In the traditional regime, the data is stored separately in commercial banks; the state is a third party that wants to get to the information and can only obtain it within the procedures established by the law. In the CBDC model, data are concentrated in the centralised register of the central bank, which turns it into the direct operator of transactions and substantially reduces the level of transactional anonymity. In the hybrid regime, commercial banks continue to be the main providers of information about clients and providers of KYC, while the central bank takes care of the issuance of the cryptocurrency and provides the final clearing procedure. With the limited-access mode, the client is given the opportunity to make pseudonymous transactions within a limited amount (for offline transactions), and the regulatory mechanism starts functioning only if the threshold is crossed. This is how modern approaches to the design of central bank digital currencies look. The transformation of banking secrecy under strengthened financial monitoring is also reflected in a change in the philosophy of interaction with the client. There is also a noticeable gradual move from "presumption of confidentiality": if, before, the bank had to prove that it was lawful to provide confidential data, the client now must prove the legitimacy of his funds to remain within the circle of clients who are granted the right to service. The globalisation of supervision has meant that, through FATF and CRS standards, an individual's financial profile becomes part of the global information domain of tax and intelligence authorities. The algorithmisation of compliance means that decisions on information disclosure are increasingly made not by a human being, but by a neural network. This excludes the subjective factor, but creates risks for certain categories of clients.

The transition to preventive algorithmic risk analysis in banking law and the neutralisation of the human factor were examined by T. Gatla (2024). At the same time, the emphasis shifts towards cyber protection: banking secrecy is transformed into a technical standard of encryption. Switzerland's experience in 2024-2025 demonstrates an interesting trend: despite full transparency for tax authorities, the country remains attractive to capital because of its legal stability. In Ukraine, however, the transformation of this institution should be accompanied not only by stronger control, but also by greater responsibility on the part of state bodies for the use of the information obtained. An important element of the analysis is the role of cryptocurrencies and decentralised finance. The introduction of new anti-monopoly and anti-money-laundering directives has, in effect, equated crypto exchanges with banks in matters of reporting. Digitalisation has made it possible to create specialised blockchain analytics tools, such as Chainalysis, Elliptic and Crystal Blockchain, which deanonymise transactions much more effectively than classical banking requests (FATF, 2025; FINMA, 2025). Through heuristic analysis algorithms, address clustering and artificial intelligence technologies, these analytical platforms enable state regulators and compliance officers to track the full chain of

movement of digital assets, label "dirty" wallets and identify the ultimate beneficial owners of transactions in decentralised networks, even where mixers or privacy-enhancing protocols are used (Zuboff, 2019). This leads to the emergence of the phenomenon of "absolute transactional transparency", in which traditional legal barriers of banking confidentiality are neutralised by the directly open architecture of the distributed ledger.

Stronger financial monitoring contributes to bringing the economy out of the shadows; however, excessive control may force part of the capital into unregulated segments. The legal specificity of Ukraine lies in the expansion of the list of entities, including the National Anti-Corruption Bureau of Ukraine and the Bureau of Economic Security of Ukraine, that have the right to obtain data without a court decision. The digitalisation of the procedure for providing such responses minimises time costs, but requires strict access auditing. The final stage of the transformation is the transition to the concept of self-sovereign identity (SSI), whereby the client owns their own data in a digital wallet and grants the state temporary access for verification purposes (Schardong & Custódio, 2022).

A separate aspect of the transformation of banking secrecy is the introduction of AI systems into the architecture of automated sanctions and penalty imposition. In conditions where financial information becomes fully digital, state bodies are able to integrate the databases of the tax service and court decision registers directly with banking systems. The analysis shows that in the USA and the EU, commercial banks are required to carry out automated screening of transactions against sanctions lists, including those of the US Office of Foreign Assets Control and the consolidated EU sanctions regimes (Kim & Yang, 2024). For this purpose, fuzzy matching algorithms are integrated, making it possible to identify hidden links despite deliberate changes in the spelling of names or company titles. However, such mechanisms operate exclusively through internal bank compliance systems as filtering barriers, rather than in the form of direct automatic blocking of transactions by state structures.

In the Ukrainian context, the NBU and the State Financial Monitoring Service have built a centralised system of automated financial monitoring. Modern banking systems implement algorithmic mechanisms for the automatic generation and transmission of suspicious transaction reports (STRs), which are integrated with state registers and compliance systems. This enables rapid response, including the automatic blocking or temporary restriction of transactions when deviations from the client's financial profile are detected. In this context, digitalisation transforms banking secrecy from a classical legal institution for protecting information into a technically regulated access mechanism, where the priority is the speed of data exchange between participants in financial monitoring. At the same time, banks are moving away from a reactive model of confidentiality protection towards proactive analysis of client behaviour, in which artificial intelligence algorithms play a key role in identifying risky transactions. As a result, within open banking ecosystems, the client's control over their own financial secrecy is substantially reduced because data is transmitted automatically between participants in the financial infrastructure.

The transformation of banking secrecy is also closely linked to the ethical dilemma of "digital surveillance". In contemporary legal scholarship, several approaches have emerged regarding the relationship between financial security and privacy. As S. Karakushi (2025) noted, this dilemma intensifies the theoretical debate on the limits of legal intervention in the digital rights of market participants. The first approach, the securitisation approach, dominates regulatory practice and asserts the unconditional priority of transparency in combating criminalisation. The second, the libertarian-legal approach, emphasises that privacy is a fundamental human right, and that its violation undermines market trust. The third, integrative approach argues that a direct opposition between "privacy and security" is an oversimplification, since in practice this involves a multi-level system of risks in which the technical security of data transmission channels is a prerequisite for preserving the legal privacy of the subject. When a bank's algorithms classify a transaction as a deviation from the norm, banking secrecy becomes an obstacle for the client themselves, as institutions often refuse to disclose the logic behind the decision, referring to the confidentiality of their internal methodologies. This creates a need to revise legislation towards stronger consumer protection, so that digitalisation does not lead to arbitrariness by automated systems (Karakushi, 2025).

In the Ukrainian context, where trust in state institutions is still being formed, the transformation of banking secrecy must be accompanied by reciprocal transparency on the part of state bodies. The model of the "transparent client" will be viable only if strict liability is introduced for data leaks or the misuse of data. The Swiss experience shows that, even with full transparency for tax authorities, banking secrecy remains as a form of protection against commercial espionage and private interference. This defines a new standard: the banking secrecy of the future is not about concealing income, but about protecting a digital identity against unauthorised access by third parties. Finally, attention should be paid to the development of cybersecurity systems as the new protective layer of banking secrecy. In a world where data is transmitted instantly, secrecy no longer means that nobody knows something; it means that nobody can break into it. The regulatory basis for this transformation in the EU has been provided by the Digital Operational Resilience Act (DORA) (2025) and the Cyber Resilience Act (CRA) (2024), which establish strict requirements for the reliability of software code and the protection of channels for exchanging financial information. The need for such regulation is confirmed by the rapid increase in cyberattacks on banking institutions in Ukraine and EU countries during 2022-2025, which has turned cyber incidents into the main threat of unauthorised disclosure of

confidential data. The legal concept of secrecy is gradually being absorbed by the technical concept of cyber resilience. This requires the legislator to move towards regulating not only the "right of access", but also the "quality of protection" of that access at the level of software code and encryption. The technological resilience of issuers' infrastructure is becoming a basic legal criterion for the functioning of new payment architectures (Parashchenko & Dosuzha, 2025).

The final stage in the transformation of the institution of banking secrecy is the transition to the concept of "digital trust", which is replacing classical banking anonymity. This transition is made concrete through the architectural mechanisms of open banking and API access technologies. The legal framework of Directive (EU) 2015/2366 (2015) clearly establishes the principles of mandatory client consent and data access minimisation, whereby the user receives tools for role-based management of their own financial profile. In a world where financial transactions are becoming part of the global Internet of Things, banking secrecy is effectively turning into a service for managing access to data. This gives rise to new legal constructs in which the bank's responsibility lies not in concealing information from the state, but in ensuring the integrity and immutability of the client's financial profile. Thus, digitalisation has substantially changed the meaning of banking secrecy: automated data exchange and the development of financial monitoring have significantly increased the transparency of financial transactions and narrowed the boundary between banking confidentiality and tax reporting. At the same time, control is increasingly exercised through algorithmic data analysis systems, which improves the effectiveness of detecting risky transactions. Under such conditions, the value of banking secrecy is gradually shifting from the concealment of information to the provision of an appropriate level of cyber protection, personal data protection and legal guarantees for data processing. The results of the comparative analysis, therefore, indicate the transformation of banking secrecy from a model of absolute confidentiality to a model of regulated access to financial information. Despite a common development trajectory, these changes in Switzerland are taking place on the basis of established legal traditions and a developed financial infrastructure, whereas in Ukraine, they are largely driven by the needs of financial monitoring and national security under martial law.

The transformation of the institution of banking secrecy amid large-scale digitalisation and strengthened financial monitoring is a subject of intense debate in contemporary legal and economic scholarship. The findings of this research correspond with, and in some respects substantially complement, the studies of other specialists. The issue of the technological transformation of compliance and the neutralisation of traditional confidentiality through automatic data exchange systems was examined in detail by V. Krasovskyi (2024). In his study, the author demonstrated that the full automation of tax control and the integration of unified reporting standards effectively eliminate classical banking anonymity, turning financial institutions into direct agents of fiscal services. The present study confirms these conclusions, but extends the analysis by emphasising that, in the Ukrainian context, this process is further accelerated by security challenges, which create a specific balance between fiscal pressure and national security. The development trajectory of artificial intelligence systems in the architecture of financial supervision was analysed in detail in the study by U. Turksen *et al*. (2024). The authors focused on the risks of algorithmic errors, where neural networks independently classify transactions as suspicious and restrict clients' access to assets without adequate human oversight. When these findings are compared, it should be noted that the present study also identified the problem of "invisible" monitoring and the arbitrariness of automated systems. However, this study proposes a specific legal response to this dilemma through a transition to the concept of SSI, under which the client retains the right to temporary and role-based management of access to their own data. Finally, the concept of "digital trust" and the implementation of the open banking architecture were examined by Z.M. Dovhan & Y.M. Halitseiska (2021). Open APIs were considered exclusively as a technological tool for intensifying the financial services market. By contrast, the findings of the present study demonstrate the deeper legal nature of this phenomenon, showing that the framework of Directive (EU) 2015/2366 (2015) transforms the right to secrecy into a technical protocol for the dynamic management of user consent, where the bank's responsibility lies in ensuring the immutability of the client's digital profile. The study of open banking by D.A. Zetzsche & L. Anker-Sørensen (2022) also confirmed the need to maintain a balance between user data sovereignty and the efficiency of the financial system. Thus, the comparison carried out in this study confirms its scholarly novelty, which lies in the integrated consideration of the legal, technological and ethical factors shaping the transformation of banking secrecy.

## CONCLUSIONS

The study confirmed that the contemporary transformation of the institution of banking secrecy is an irreversible process driven by the shift towards global digital transparency. In the new reality, banking secrecy has definitively lost its original status as the client's absolute right to anonymity and has become a complex regime of restricted access to personal data. The global trend towards deoffshorisation and the active implementation of automatic information exchange standards have made financial assets transparent to regulators. The Swiss experience shows that even the most closed jurisdictions have had to yield to the requirements of international financial security. The transformation of the regimes of the classical confidentiality regime in the European space demonstrates the gradual transition of banking secrecy to the service of the interests of collective fiscal transparency without the destruction of the legal framework for combating commercial espionage. The results of the comparative analysis demonstrate a historical shift from the "right to secrecy" to the "right to protected

and regulated access". Digitalisation, the introduction of AI technologies and fuzzy matching, Big Data analytics and open banking models have enabled supervisory authorities and compliance services to analyse a client's financial profile in real time. It was found that, in the Ukrainian context, this process is reinforced by the integration of banking systems with state registers and the Diia ecosystem, which ensures unprecedented speed in verification and the automatic generation of STRs for the State Financial Monitoring Service. At the same time, this requires the implementation of strict standards of liability for data leaks. The strengthening of financial monitoring has led to a fundamental change in the role of banking institutions, which have been transformed from trusted representatives of the client into active participants in compliance control. Against the background of the spread of EU regulatory frameworks, this paradigm shift creates new ethical dilemmas related to the risks of "digital exclusion", arbitrariness by automated systems and the opacity of banks' internal scoring methodologies. For the stability of Ukraine's financial system, it is important to maintain a multi-level balancing of the national security of interest, which has been significantly strengthened by the challenges of martial law, with the fundamental right of citizens to privacy. In the future, banking secrecy will most likely be absorbed in the techno-legal concept of cyber resilience and transition to standards DORA and CRA in the context of a growing number of cyberattacks against the financial sector. With the development of the architectural models of the CBDCs, such as the e-hryvnia and the digital euro, the traditional banking secrecy will develop in the direction of the concept of SSI and in the direction of the service of dynamic control over the provision of API-access for the customer within the framework of the principles of GDPR and PSD2. Further research in this area should focus on developing optimal legal mechanisms to protect consumers of financial services from errors in AI algorithms used in banking compliance, as well as on harmonising Ukrainian cyber resilience legislation with the criteria of the DORA Regulation.

## ACKNOWLEDGEMENTS

None.

## FUNDING

None.

## CONFLICT OF INTEREST

None.

## REFERENCES

[1] About e-hryvnia, the digital currency of the National Bank of Ukraine. (n.d.). Retrieved from https://bank.gov.ua/en/payments/e-hryvnia.
[2] Alt, R., Beck, R., & Smits, M.T. (2018). FinTech and the transformation of the financial industry. *Electronic Markets*, 28(3), 235-243. doi: 10.1007/s12525-018-0302-x.
[3] Amalia, C., Gianne Poetry, E., Kono, M.K., Kusuma, D.A., & Kurniawan, A. (2022). Legal issues of personal data protection and consumer protection in open API payments. *Journal of Central Banking Law and Institutions*, 1(2), 323-352. doi: 10.21098/jcli.v1i2.19.
[4] Automatic Exchange of Information. (2020). Retrieved from https://www.oecd.org/en/publications/automatic-exchange-of-information_7655bed0-en.html.
[5] Bakhshi, M., Nematbakhsh, M., Mohsenzadeh, M., & Rahmani, A.M. (2020). Data-driven construction of SPARQL queries by approximate question graph alignment in question answering over knowledge graphs. *Expert Systems with Applications*, 146, article number 113205. doi: 10.1016/j.eswa.2020.113205.
[6] Baselgia, E. (2023). *The compliance effects of the automatic exchange of information: Evidence from the Swiss tax amnesty*. Retrieved from https://surl.li/dvuzgh.
[7] BIS. (2023). *Central bank digital currencies: Ongoing policy perspectives*. Retrieved from https://www.bis.org/publ/othp65.pdf.
[8] Common Reporting Standard. (2025). Retrieved from https://www.oecd.org/en/publications/2025/04/consolidated-text-of-the-common-reporting-standard-2025_e478bc04.html.
[9] Corporate Transparency Act of 2019. (2019, October). Retrieved from https://www.congress.gov/bill/116th-congress/house-bill/2513.
[10] Cyber Resilience Act. (2024). Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.
[11] Digital Operational Resilience Act (DORA). (2025). Retrieved from https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.
[12] Diia. (n.d.). Retrieved from https://diia.gov.ua/.
[13] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC. (2015, November). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex %3A32015L2366.
[14] Dovhan, Z.M., & Halitseiska, Y.M. (2021). Open-banking as a trend in the development of financial technologies. *Innovative Economy*, 5-6, 111-116. doi: 10.37332/2309-1533.2021.5-6.16.
[15] ECB. (n.d.). *Digital euro*. Retrieved from https://www.ecb.europa.eu/euro/digital_euro/html/index.eu.html.

[16] Exchange of information with 104 countries on around 3.6 million financial accounts. (2023). Retrieved from https://www.admin.ch/en/nsb?id=98028.
[17] Exchange of information with 110 states on approximately 3.8 million financial accounts. (2025). Retrieved from https://www.sif.admin.ch/it/scambio-automatico-informazioni-sai.
[18] Exchange of information with 75 countries on around 3.1 million financial accounts. (2019). Retrieved from https://www.admin.ch/en/nsb?id=76625.
[19] FATF. (2025). *Methodology for assessing technical compliance with the FATF recommendations and the effectivenesss of AML/CFT/CPF systems*. Paris: Financial Action Task Force.
[20] FINMA. (2025). *Annual report 2025*. Retrieved from https://report.finma.ch/2025/en/downloads.
[21] Gatla, T. (2024). AI-driven regulatory compliance for financial institutions: Examining how AI can assist in monitoring and complying with ever-changing financial regulations. *SSRN Electronic Journal*, 12(3), 607-611. doi: 10.2139/ssrn.4856649.
[22] Jabbar, A., Geebren, A., Hussain, Z., Dani, S., & Ul-Durar, S. (2023). Investigating individual privacy within CBDC: A privacy calculus perspective. *Research in International Business and Finance*, 64, article number 101826. doi: 10.1016/j.ribaf.2022.101826.
[23] Jain, A.K., Ross, A.A., & Nandakumar, K. (2011). *Introduction to biometrics*. New York, NY: Springer Science & Business Media.
[24] Karakushi, S. (2025). Balancing security and privacy: Analyzing the effectiveness of EU digital surveillance laws in criminal proceedings. *International Journal of Law and Societal Studies*, 2(1), 110-119. doi: 10.61424/ijlss.v2i1.445.
[25] Kim, S., & Yang, S. (2024). Accuracy improvement in financial sanction screening: Is natural language processing the solution? *Frontiers in Artificial Intelligence*, 7, article number 1374323. doi: 10.3389/frai.2024.1374323.
[26] Krasovskyi, V. (2024). Common Reporting Standard as a model for tax information exchange: Mechanism of operation and implementation status in Ukraine. *Law and Innovative Society*, 1(22), 10-20. doi: 10.37772/2309-9275-2024-1(22)-1.
[27] Law of Ukraine No. 361-IX "On the Prevention and Combating of Money Laundering, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction". (2025, January). Retrieved from https://zakon.rada.gov.ua/laws/show/361-20#Text.
[28] Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Cambridge: Polity.
[29] Mahdi, M.N., Walshe, R., Farrell, S., & Pandit, H.J. (2024). Comprehensive review and future research directions on ICT standardisation. *Information*, 15(11), article number 691. doi: 10.3390/info15110691.
[30] Meier, H.B., Marthinsen, J.E., Gantenbein, P.A., & Weber, S.S. (2023). Swiss bank (customer) secrecy and the international exchange of information. In *Swiss finance* (pp. 159-250). Cham: Springer. doi: 10.1007/978-3-031-23194-0_4.
[31] NBU. (n.d.a). *About the e-hryvnia – the National Bank's digital currency*. Retrieved from https://bank.gov.ua/ua/payments/e-hryvnia.
[32] NBU. (n.d.b). *Financial monitoring*. Retrieved from https://bank.gov.ua/ua/supervision/monitoring.
[33] OECD. (2014). *Multilateral competent authority agreement on automatic exchange of financial account information*. Paris: Organisation for Economic Co-operation and Development.
[34] Parashchenko, O.K., & Dosuzha, A.Ye. (2025). Legal regulation of digital finance in the EU and Ukraine: A comparative analysis. *Analytical and Comparative Jurisprudence*, 2(6), 266-272. doi: 10.24144/2788-6018.2025.06.2.42.
[35] Polasik, M., Butor-Keler, A., Widawski, P., & Keler, G. (2024). Evaluating the regulatory approach to open banking in Europe: An empirical study. *Financial Law Review*, 34(2), 59-90. doi: 10.4467/22996834FLR.24.007.20612.
[36] Resolution of the Board of the National Bank of Ukraine No. 65 "On Approval of the Regulation on Financial Monitoring by Banks". (2020, May). Retrieved from https://zakon.rada.gov.ua/laws/show/v0065500-20#Text.
[37] Schardong, F., & Custódio, R. (2022). Self-sovereign identity: A systematic review, mapping and taxonomy. *Sensors*, 22(15), article number 5641. doi: 10.3390/s22155641.
[38] SFMS. (2024). *Annual report 2023*. Kyiv: State Financial Monitoring Service of Ukraine.
[39] Siena, F.A. (2022). The European anti-money laundering framework – at a turning point? The role of financial intelligence units. *New Journal of European Criminal Law*, 13(2), 216-246. doi: 10.1177/20322844221105406.
[40] SIF. (2025). *2025 activity report*. Retrieved from https://www.sif.admin.ch/dam/en/sd-web/NLoWaSssFgVh/SIF-Tatigkeitsbericht_2025_EN.pdf.
[41] Tan, H., Kwon, J., Peng, W., & Xin, B. (2025). The co-effects of technology innovation and digital infrastructure on central bank digital currency: A DSGE analysis. *Research in International Business and Finance*, 75, article number 102783. https://doi.org/10.1016/j.ribaf.2025.102783.
[42] Tertychnyi, P., Godgildieva, M., Dumas, M., & Ollikainen, M. (2022). Time-aware and interpretable predictive monitoring system for Anti-Money Laundering. *Machine Learning with Applications*, 8, article number 100306. doi: 10.1016/j.mlwa.2022.100306.

[43] The Anti-Money Laundering Act of 2020. (n.d.). Retrieved from https://www.fincen.gov/resources/statutes-and-regulations/anti-money-laundering-act-2020.
[44] Turksen, U., Benson, V., & Adamyk, B. (2024). Legal implications of automated suspicious transaction monitoring: Enhancing integrity of AI. *Journal of Banking Regulation*, 25, 359-377. doi: 10.1057/s41261-024-00233-2.
[45] Ukraine joined the Multilateral Competent Authority Agreement on the Automatic Exchange of Financial Account Information. (2022). Retrieved from https://tax.gov.ua/baneryi/crs/povidomlennya/609052.html.
[46] Will the Swiss franc soon only exist digitally? (n.d.). Retrieved from https://www.snb.ch/en/snb-explained/cbdc.
[47] Yeh, S.S. (2023). The anticorruption protocol to the United Nations convention against corruption beneficial owner rule. *Laws*, 12(6), article number 86. doi: 10.3390/laws12060086.
[48] Zetzsche, D.A., & Anker-Sørensen, L. (2022). Regulating sustainable finance in the dark. *European Business Organization Law Review*, 23, 47-85. doi: 10.1007/s40804-021-00237-7.
[49] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: PublicAffairs.

# Трансформація інституту банківської таємниці в умовах цифровізації та посилення фінансового моніторингу

**Світлана Кушнір**
Кандидат економічних наук, професор
Запорізький національний університет
69011, вул. Університетська, 66, м. Запоріжжя, Україна
https://orcid.org/0000-0002-1410-1887
**Олександр Павлов**
Студент
Запорізький національний університет
69011, вул. Університетська, 66, м. Запоріжжя, Україна
https://orcid.org/0009-0009-7171-6835

**Анотація.** Метою статті було комплексне теоретико-методологічне обґрунтування та оцінка еволюції інституту банківської таємниці під впливом інтеграції систем штучного інтелекту, норм Automatic Exchange of Information, Common Reporting Standard та проєктування цифрових валют центральних банків. Методологічну основу дослідження становило поєднання методів діалектичного пізнання, системно-структурного аналізу фінансових ринків та якісного кейс-стаді регуляторних практик Швейцарії як історичного еталона конфіденційності, а також адаптаційних процесів у банківських системах Німеччини, Сінгапуру, Великої Британії та України. Застосування компаративного підходу та методів графічно-табличного моделювання дозволило об'єктивно систематизувати емпіричні дані щодо інтенсифікації розкриття транзакційної інформації суб'єктами первинного моніторингу. У результаті дослідження доведено незворотний перехід банківського сектору від концепції абсолютної анонімності капіталу до моделі «скляного клієнта», де банківська таємниця трансформується з юридичного інструменту приховування інформації на технологічний протокол управління авторизованим доступом до даних. Виявлено стійку тенденцію щорічного зростання обсягів автоматичного обміну податковими даними (у Швейцарії на 10-12 % щороку), що підтвердило нівелювання офшорної таємниці під впливом вимог Financial Action Task Force та Organisation for Economic Co-operation and Development. Обґрунтовано особливості українського комплаєнсу в умовах воєнного стану, де реалізація Постанови Національного Банку України № 65 та миттєва верифікація через екосистему «Дія» автоматично розкривають дані перед фінансовою розвідкою без судових санкцій. Доведено, що запуск Central Bank Digital Currency (е-гривні, цифрового франка) та алгоритмів безперервного транзакційного скорингу штучним інтелектом де-факто усуває банківське посередництво, перетворюючи приватність на програмовану опцію та зміщуючи правовий захист у площину кіберстійкості та концепцій децентралізованої ідентичності. Практична цінність отриманих результатів полягає у можливості їх використання Нацбанком України та комерційними банками для оптимізації алгоритмів ризик-орієнтованого нагляду, розробки нормативно-правових актів щодо захисту фінансового профілю клієнта від кібератак та побудови збалансованої моделі «цифрової довіри»

**Ключові слова:** автоматичний обмін інформацією; Швейцарія; ризик-орієнтований підхід; штучний інтелект; скоринг