Enhancement of the risk-based approach in Anti-Money Laundering (AML) through digital transformation. A case from Romania

FORESIGHT ERASMUS+

Catalin Ploae, Ph.D.
Bucharest University of Economic Studies

INTRO

If there was ever a need for a reminder, the COVID-19 catastrophe served as such that criminal ingenuity flourishes in chaotic situations by playing on people's concerns. Unreliable face masks, fake medications, and dubious medical supplies were widely advertised as miracle treatments for the coronavirus by dishonest individuals looking to make a fast buck. As people's circumstances deteriorated, organized crime intervened to provide a "helping hand" to individuals who were in financial difficulty. Companies with no track record in health were awarded significant government contracts. Criminals saw an opportunity where other people saw a worldwide public health and economic calamity.

The money involved moves via the established financial system, which is a characteristic of this illegal activity and nearly all financial and economic crime. The companies who carry out those transactions are in a strong position to get first-hand information about what is going on. Because of this, banks and other financial institutions are required to follow **anti-money-laundering and countering the funding of terrorism (AML/CFT) regulations** to identify who is paying whom and why, and to notify the appropriate authorities if necessary. Financial institutions, which act as the worldwide financial system's gatekeepers, are the first line of defense against this illicit activity. They cannot, however, do this work on their own; they require assistance from authorities to comprehend what risks they face, what criminal groups and typologies are widespread in their system, and how they are to carry out their responsibilities. They require a guiding, and sometimes strong, hand. In this context, financial sector regulators play a critical role. They guarantee that the financial sector understands and successfully executes its AML/CFT duties by off-site monitoring and on-site visits, giving guidance and, when appropriate, enforcing with consequences proportional to the breach.

The "global public bads" of organized crime, corruption, and terrorism all disproportionately affect emerging civilizations, especially the citizens of fragile and conflict-ridden nations. Small enterprises must pay security money when organized crime is rife; patients must buy doctors for care where corruption is rampant; and where terrorist organizations and warlords are in charge, even going to school requires bravery. Therefore, to **preserve and protect the integrity of the global financial system**, the entire ecosystem has to address and directly fight these negative phenomena and to attack them on the back end by **following the money.**

As already mentioned, in order for financial and other related institutions to mitigate the money laundering risks (which can result in reputational damage, financial losses, and regulatory sanctions), AML regulations have been implemented globally, requiring financial institutions to establish AML programs that comply with local laws and regulations.

The effectiveness of traditional AML programs has been limited by their reliance on manual processes, which are time-consuming, error-prone, and unable to keep pace with the evolving risks and threats. **Digital transformation provides an opportunity to enhance the risk-based approach in AML by leveraging emerging technologies such as artificial intelligence (AI), machine learning (ML), and blockchain.**

WHAT IS THE RISK-BASED APPROACH?

As we have mentioned in the Intro to this lecture, financial institutions must identify, assess, and manage money laundering risks to comply with local laws and regulations and protect themselves from reputational damage, financial losses, and regulatory sanctions.

Financial institutions and other institution that are required by law to comply to AML/CFT regulations must develop a programme against Money Laundering (ML) and the Financing of Terrorism (TF). These institutions are best placed to assess ML/TF risk(s) they may reasonably face in conducting business, having regard to their business (size, nature and complexity),having in the same time the flexibility to construct their risk management frameworks for the purpose of developing risk-based systems and controls, proportionate to the ML/TF risk(s) faced and mitigation strategies in the manner most appropriate to the structure of clients/customers and the products and/or the interface services provided to clients/customers and the jurisdictions.

The starting point of any risk-based approach framework on addressing ML/FT is considered to be the first recommendation of FATF (the Financial Action Task Force which is the global money laundering and terrorist financing watchdog, as it sets international standards that aim to prevent these illegal activities and the harm they cause to society):

- FATF Recommendation 1- Assessing risks and applying a risk-based approach

“Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions. Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks”.

Therefore, in line with FATF recommendation 1 (and other relevant recommendations and interpretative notes) and the relevant legislation and rules, financial institutions and DNFBPs are required to adopt a risk-based approach. They should involve senior management in the managing of their risks and using their knowledge of the Licensed Party to develop systems that uniquely address the specific risks that they face, especially in respect of allocation of additional resources to areas of high risk.

FATF frequently uses the words risk, danger, vulnerability, and consequence when outlining how countries should put AML/CFT requirements into practice. These words signify:

- Threat, susceptibility, and consequence are three variables that might be considered as influencing **risk.** An attempt is made to identify, analyse, and comprehend ML/TF risks in an ML/TF risk assessment, which is a product or process based on a methodology that has been approved by the parties associated with Licensed Parties and acts as the first step in resolving them. Making judgements about risks, vulnerabilities, and outcomes is ideal for a risk

assessment. The extent and gravity of a risk depend on the possibility that ML or TF activity will occur as well as the effects or harm that will result from that occurrence. Therefore, it would be deemed "high risk" when threats and vulnerabilities coexist and have the potential to have major negative effects or damages.

- A **threat** is an individual or group of individuals, thing, or action that has the potential to harm, for instance, the state, society, economy, etc. This covers criminals, terrorist organizations and their financiers, as well as past, current, and potential ML or TF actions. One of the risk-related aspects mentioned above is threat, and in most cases, it serves as a crucial beginning point for comprehending ML/TF risk.
- The inherent qualities of a system or structure (such as flaws in controls, processes, or procedures) that leave it vulnerable to abuse or exploitation by criminal elements for ML, TF, or both are known as v**ulnerabilities**. A system is more appealing to money launderers and those who fund terrorism when it has flaws.
- **Consequence** refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequences of ML or TF may be short or long term in nature and also relate to populations, specific communities, the business environment, or national or international interests.

An institution required by law to comply to AML/CFT regulations must be able to show that it has considered the business's exposure to ML/TF risks (including the clients/customers, goods, interface services, and countries). The Business Risk Assessment must be in writing, approved by top management, and reviewed on a regular basis—at the very least annually.

The type, amount, and extent of risks that a licensed party is ready to subject itself to in order to progress its business operations should be defined and documented by obliged entities. Since this might affect an institution's profitability and/or regulatory requirements, senior management's involvement and approval are crucial to the process.

The risk assessment process typically involves the following steps:

- ✓ **Identify and categorize customers:** Financial institutions must identify and categorize their customers based on their risk level. This can be done using various factors, such as customer type, geography, business activity, and transaction volume.
- ✓ **Assess and rate risks:** Once customers have been categorized, financial institutions must assess and rate the money laundering risks associated with each category. This can be done using various factors, such as the source of funds, the purpose of the transaction, and the customer's background.
- ✓ **Determine risk appetite**: Financial institutions must determine their risk appetite and establish risk tolerance levels for different categories of customers. This ensures that risks are managed in a consistent and appropriate manner.
- ✓ **Develop risk mitigation strategies:** Finally, financial institutions must develop risk mitigation strategies to address identified risks. This may include enhanced due diligence, transaction monitoring, and internal controls.

The results of a risk assessment can be used for a variety of reasons, including:

- Identify gaps or opportunities for improvement in AML/CFT policies, procedures and processes;
- Make informed decisions about risk appetite and implementation of control efforts, allocation of resources, technology spend;
- Assist management in understanding how the structure of a business unit or business line’s AML/CFT compliance programme aligns with its risk profile;

- Develop risk mitigation strategies including applicable internal controls and therefore lower a business unit or business line's residual risk exposure;
- Ensure senior management are made aware of the key risks, control gaps and remediation efforts;
- Assist senior management with strategic decisions in relation to commercial exits and disposals;
- Ensure regulators are made aware of the key risks, control gaps and remediation efforts across the obliged entities;
- Assist management in ensuring that resources and priorities are aligned with its risks.

Following the risk assessment, a risk management framework is required to be set-up, that involves implementing controls and procedures to mitigate identified risks. Effective risk management requires a combination of policies, procedures, and controls that are designed to prevent, detect, and report suspicious activity.

The risk management process typically involves the following steps:

- Design policies and procedures: Financial institutions must design policies and procedures that reflect their risk appetite and tolerance levels. These policies and procedures should cover areas such as customer due diligence, transaction monitoring, and reporting suspicious activity.
- Implement internal controls: Financial institutions must implement internal controls to ensure that policies and procedures are followed and that risks are managed effectively. This may include segregation of duties, dual controls, and regular reviews.
- Monitor transactions: Financial institutions must monitor transactions for suspicious activity using automated systems and manual processes. This includes reviewing transaction patterns, identifying anomalies, and investigating any red flags.
- Report suspicious activity: Finally, financial institutions must report suspicious activity to the relevant authorities in a timely and accurate manner. This helps to prevent money laundering and other financial crimes.

Risk assessment and management are critical components of an effective AML program. By identifying, assessing, and managing money laundering risks, financial institutions can comply with local laws and regulations, protect themselves from reputational damage, financial losses, and regulatory sanctions, and prevent money laundering and other financial crimes. The risk assessment process involves identifying and categorizing customers, assessing and rating risks, determining risk appetite, and developing risk mitigation strategies. The risk management process involves designing policies and procedures, implementing internal controls, monitoring transactions, and reporting suspicious activity. By implementing these processes effectively, financial institutions can better manage money laundering risks and protect their business.

DIGITAL TRANSFORMATION IN PREVENTING AND COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

Technology is transforming the way financial institutions approach anti-money laundering (AML) compliance. Emerging technologies such as artificial intelligence (AI), machine learning (ML), and Data Mining (DM) are enabling financial institutions to automate compliance processes, improve risk assessment and management, and enhance customer due diligence.

The health crisis generated by the COVID-19 pandemic has spurred business at national, regional and global levels to seek new solutions to respond to the uncertain context. For many economic sectors and businesses, digital transformation has been one such solution, capable of helping to revive business and foster sustainable growth.

Digital transformation is more an operational issue than a technology issue. Digital transformation is not about machines, it is about people. If digitisation is the process of taking analogue information available on paper and translating it into a digital format so that it can be stored, processed and transmitted on a computer, and digitisation is the use of digital technologies and information to automate operations and processes within an organisation, then digital transformation is about embracing cultural change on a large scale to take full advantage of digital technologies. This involves customer-facing organisational changes and is therefore a process that requires continuous recalibration of both businesses, operating and interaction models with customers and stakeholders, and the competencies held by organisations. For many organisations, the start of such a sustained process is a return on investment.

At the same time, financial-crime incidents and failings have been on the rise throughout the pandemic, according to the Financial Action Task Force, the leading international standards-setting body for financial crime we have already referred to.

In this context, it is noted that the anti-money laundering landscape is also undergoing a period of considerable change as financial institutions face significant disruption to traditional risk management methodologies and approaches.

Anti-money laundering continues to be a key area of concern for regulators around the world, including in Romania. For example, the United Nations Office on Drugs and Crime (UNODC) recently estimated that between 2% and 5% of global gross domestic product, somewhere between USD 800 billion and USD 2 trillion therefore, is laundered/recycled on a global scale. The increasing sophistication of crimes such as fraud, cybercrime, human trafficking, slavery, environmental crime, online exploitation of children and organised property crime requires even greater efforts to combat financial crime. There is therefore an urgent need for the industry to explore and implement innovative technological solutions that can address these complexities and risks.

We need also to consider the huge increase of the payment services sector. Payments services were long offered to companies and individuals by banks, but in the past 20 years dedicated and specialized providers greatly expanded the market. In 2020, global payments revenues reached $1.9 trillion. During the past decade, individuals and e-commerce merchants have increasingly adopted payments services. About half the recent growth has been in consumer-to-business and business-to-consumer payments. In North America and Europe, electronic payments are expanding very fast, at twice the GDP growth rates in these regions; in Asia, the expansion is happening even faster. The explosion in the number of electronic transactions is part of the e-commerce and m-commerce booms and the shift away from cash payments. Digital-payments mechanisms include

cards but also recent payments innovations, such as digital wallets. This shift to digital payments is expected to continue.

We are thus living in the age of digitisation - especially among financial institutions - one of the sources of data and information relevant to preventing and combating money laundering and terrorist financing. The rapid evolution of technology is leading to an explosion in the number and volume of transactions, the growth of electronic payment methods and the development of cryptocurrencies. The introduction of new technologies implies an increased sophistication of criminal money laundering methods. The inability to adequately identify, assess and mitigate the risk of money laundering and terrorist financing, including the fundamentals of risk identification (customer identification/verification and transaction monitoring) is an obstacle to efficiency in the area of AML/CFT. This outlines the current context in which the implementation and use of new technologies can provide the greatest added value.

The added value of the new technologies is to support the highly judicious work of the analyst working in a financial intelligence unit, an analyst who functions and operates according to internationally established principles and standards in relation to preventing and combating money laundering and terrorist financing. The financial intelligence analysis work carried out in a financial intelligence unit involves the same steps as the analysis work carried out in intelligence services, namely collection, collation, integration, analysis and dissemination. In this context, we stress that the Financial Intelligence Unit is the main provider of specialised financial intelligence products to law enforcement authorities and other structures with competences in the field of preventing and combating money laundering and terrorist financing.

Until the Big Data revolution that has its starting point in the early 2000s, the approach to detecting money laundering has been to analyse the evidence provided by audit trails and the wider context of the activity of the entity or person concerned. Such investigative techniques focused primarily on detecting suspicious patterns in the available data to identify money laundering activities. Traditionally, BSA/AML systems have followed a time-intensive manual processing approach. Today, the total number of transactions has grown exponentially and the volume of bank data has also increased significantly. Hence the need for traditional anti-money laundering methods to be backed up by some automated tools to extract suspicious money laundering patterns. As the volume of data is growing, traditional statistical techniques and human capabilities are outdated in their ability to identify patterns in huge data sets. The development of technology (through the advent of machine learning and the use of algorithms) and the growth of the digital economy have changed the way data is exploited for further analysis. Money laundering in large industrial centres is becoming increasingly complex and the sheer volume of data far exceeds what investigators can realistically understand and analyse.

In this context, it should be noted that the entire AML/CFT ecosystem is marked by profound transformations and challenges generated by the increasing complexity of economic activity and the number and volume of financial transactions. Thus, we note that large financial institutions have millions of customers with thousands of transactions per second on different channels such as internet, telephone, ATMs, etc. The data collected by these institutions is heterogeneous and large. This is the operating environment in which financial institutions face a number of key challenges in the fight against financial crime, such:

- Complex AML regulatory requirements as well as a broader scope for AML compliance (the regulatory framework in most jurisdictions places financial institutions at the forefront of the fight against financial crime, with increasingly rigorous compliance requirements for monitoring non-traditional customer profiles, which can pose increased risks to banks);

- **Innovations in financial crime**: The financial crime landscape is constantly changing, with criminals finding new ways to commit crimes through new technologies, channels or products, e.g. mobile banking, digital currencies, etc.;
- **Technological and regulatory system limitations;**
- **Increased compliance costs.**

Thus, extracting money laundering transactions from millions of transactions is difficult and requires a large amount of computing power, the main challenges from this perspective being:

- **Large volume of data**: Every second, millions of customer transactions take place through different touch points such as ATM, phone, TV, etc. The detection system works on three levels: transaction, account and customer level. Whenever a transaction takes place, it is not possible to use all three levels of data, as it will be necessary to retrieve this data from large databases, which is time-consuming. Also, this data is large in size and therefore the application of statistical calculations is difficult.
- **Imbalance in terms of class labels**: in the US for example, out of 700,000 transactions, only 0.05-0.1% are labelled as suspicious. Thus, the data has a very high level of class imbalance, which poses problems for classification algorithms.
- **Mislabelling:** Machine learning algorithms are trained on datasets where suspicious transactions are detected. In practice, it is not possible to check every case that was suspicious. Money laundering is an extreme case of financial fraud, while there are many small cases that are not labelled. This poses problems for machine learning algorithms during training and motivates the need for robust methods that can handle mislabelling.

A fitted solution to these challenges, offered by the banking and financial industry is through **Data Mining (DM) techniques,** which are used to identify causalities and correlations between different variables, analyse huge data sets to identify patterns and create customer profiles to identify suspicious activity.

Data analysts, no matter how skilled and competent, simply cannot understand the aggregate data available from money laundering activities using traditional approaches. This is where data mining techniques can help. Data mining techniques can enable these analysts to have the ability to process the data and make informed decisions about the likelihood that a particular transaction or series of transactions may have been the subject of the money laundering offence and therefore should be appropriately flagged as a risk factor by anti-money laundering compliance teams for further investigation.

The traditional evidence-based approach, which focuses on collecting data from internal controls, external audits and whistle-blower communications via hotlines to detect money laundering activities, simply does not have the tools to adapt to the complexity of these transactions. A more effective method is therefore to use data mining (such as through statistical methods, artificial intelligence, pattern recognition, neural networks, etc.) and various analytical approaches to discover knowledge and patterns in the dataset. In this sense, data mining can be seen as assembling large masses of data that can then be analysed to make informed decisions about a phenomenon, in this case money laundering transactions.

As a corollary to understanding data mining for detecting money laundering activities, data pre-processing is of critical importance to make inferences from the data. Context is therefore important. To make the most of the data, analysts need to understand the broader context of the sector where money laundering activities are suspected. Considerable attention needs to be paid to the preparation for data extraction and the subsequent processes for making inferences from the data.

As mentioned earlier, the AML/CFT ecosystem can also benefit from the unprecedented development of artificial intelligence and its applications. **Artificial intelligence (AI)** is the science that

mimics human thinking skills to perform tasks that typically require human intelligence, such as pattern recognition, making predictions, recommendations or decisions. Artificial intelligence uses advanced computational techniques to obtain information from different types, sources and qualities (structured and unstructured) of data information to "autonomously" solve problems and perform tasks. We discuss **machine learning**, a sort of artificial intelligence that "trains" computer systems to learn from data, spot patterns, and make judgments with little to no human involvement, in the context of creating tools to prevent and combat money laundering. Applications for machine learning are helpful for finding anomalies and outliers, as well as for locating and deleting duplicate data to enhance data quality and analysis. As an advanced kind of machine learning, **Deep Learning (DL)** uses artificial neural networks (brain-inspired algorithms) with many layers to learn from vast amounts of data in a very independent manner. DL algorithms repeat a job while making tiny adjustments each time to enhance the result, enabling the computer to handle complicated issues without the need for human interaction.

Where can machine learning add value?

Primarily in the process of **customer identification and verification.**

Secondly, in **business relationship monitoring and behavioural and transactional analysis** via unsupervised and supervised machine learning algorithms (which allow for faster, real-time analysis of data in line with relevant CSB/CFT requirements in place) and alert scoring which helps to focus on patterns of activity and issue notifications or the need for increased due diligence.

Third, in the process of **identifying and implementing regulatory updates** (machine learning techniques with natural language processing, cognitive computing capability and robotic process automation can scan and interpret large volumes of unstructured regulatory data sources on a continuous basis to identify, analyse and then automatically select applicable requirements for the organisation or to implement new or revised regulatory requirements so that regulated entities comply with relevant regulations).

Fourth, in **automated data reporting**, through the use of standardised reporting templates using automated digital applications (data pooling tools) that provide supervisors with the underlying granular data of regulated entities in blocks of data.

The need for digitisation and advanced and efficient use of data is evident globally within the AML/CFT ecosystem. A recent survey conducted by the Financial Action Task Force (FATF) through the application of the Digital Transformation Questionnaire among its members revealed, based on respondents' answers, that greater use of new technologies by AML/CFT supervisors could contribute to the effectiveness of the sector by improving supervisory capabilities.

Among the benefits offered to supervisors by new technologies, respondents to this highly relevant survey mentioned the ability to supervise a larger number of entities, to identify and better understand the risks associated with different sectors, to monitor compliance with BSC/CFT standards in real time to allow for rapid intervention in case of non-compliance, to communicate more effectively with supervised entities, to store, process and report large sets of data, and last but not least to exchange information with other competent authorities. The same study also identified a number of private sector advantages for reporting entities, including the capacity to more effectively recognize, comprehend, and manage ML/FT risks as well as the capacity to process and analyze larger data sets more quickly and accurately, resulting in enhanced reporting quality for suspicious activity.

STUDY CASE: ROMANIAN FIU'S INTEGRATED INFORMATION ANALYSIS SYSTEM

In Romania, the supervision and control activities carried out in the field of AML/CFT are the main component of the institutional responsibility of the Financial Intelligence Unit of Romania – the National Office for Preventing and Combating Money Laundering (ONPCSB) that is to prevent money laundering, terrorist financing and the implementation of international sanctions. The Office's activity is to receive, analyse, process and disseminate financial information, supervise and control, in accordance with the law, reporting entities for the purpose of preventing and combating money laundering and terrorist financing. On the basis of protocols concluded by the Office with national competent authorities, public institutions and professional associations, the institution has on-line access to a number of relevant databases (managed by ANAF, ONRC, MJ, etc.) in order to obtain the necessary information in real time. This is why it is objectively considered that the financial intelligence activity occupies the largest share of the activities carried out at the level of the National Office for Preventing and Combating Money Laundering - Romania's financial intelligence unit.

The supervision and control activities have a number of pre-established objectives, including: - analysis and processing of information obtained from the Office's internal and external databases in order to identify entities that are vulnerable to the risk of money laundering and terrorist financing, by determining the degree of exposure to this risk.

Off-site surveillance is carried out by querying databases managed within the Office in order to identify potential non-compliance with legal obligations in the field of preventing and combating money laundering and terrorist financing by regulated authorities.

The financial analysis carried out within the institution, in all its components - **operational, strategic or statistical**, constitutes the framework for the information product delivered by the Office to internal or external institutional partners.

Operational analysis consists of processing and processing "first referral" data with the aim of quickly identifying information relevant to the national system for preventing and combating money laundering and terrorist financing. Operational analysis is the analysis of financial data and information with the aim of identifying indications of the commission of money laundering, predicate offences or terrorist financing. Thus, data and information held or obtained by the Office are subject to scrutiny for identification purposes:

- persons, assets and criminal groups involved in specific activities or transactions;
- links between persons involved in transactions and possible criminal proceeds, money laundering, predicate offences or terrorist financing.

The operational analysis function focuses on individual cases and specific objectives or selected information appropriate to the type and volume of information received and the intended use of the information after its communication. This process analyses and correlates data and information received by the Office from the financial and non-financial sector and accesses, on request or on a direct access basis, other information that provides a picture of the context in which the suspicious transactions took place, in order to draw conclusions that support the existence or absence of evidence of money laundering, terrorist financing or money laundering offences.

Strategic analysis focuses on 'macro' level data and seeks to pinpoint recurrent patterns of money laundering and terrorist financing. Strategic analysis is the process of developing knowledge by identifying trends and patterns in money laundering and/or terrorist financing utilizing data and information accessible at the Office level. This approach offers insight and a better understanding of various activities and behaviours. The Office or reporting entities utilize this information to identify

threats and vulnerabilities connected to money laundering and funding terrorism. Additionally, strategic analysis can aid in establishing goals and policies for the Office. Strategic analysis may produce a variety of outputs with varying levels of complexity and intent, including:

- ✓ Typologies: a systematic classification of a number of money laundering or terrorist financing schemes that appear to be constructed in a similar way or using similar methods;
- ✓ Trends: when a typology emerges for a particular event over a period of time, it can be classified as a trend;
- ✓ Patterns: recurring characteristics or features that help to identify a phenomenon/problem and serve as an indicator or model for predicting its future behaviour;
- ✓ Synthesis: the composition or combination of parts or elements so as to form a whole. Synthesis allows connections to be made to identify ideas and opportunities for detecting money laundering/terrorist financing operations;
- ✓ Geographical analysis: area of influence or location of the phenomenon;
- ✓ Behavioural analysis: the type of operations, products, etc. used by a group;
- ✓ Activity analysis: identified weaknesses of a sector or economic activity.

To estimate the scope of the phenomenon under study and to communicate findings to reporting entities and institutional partners, **statistical analysis** uses aggregated data from the Office's databases, which are organized according to a variety of criteria, including the types of reporting entities, natural persons, and legal persons.

By the end of mid-2023, ONPCSB aims to put into use the Integrated Information Analysis System, which has the following key features:

- ✓ A complete solution for managing the processes of data acquisition (reports, information and requests) - processing - analysis - dissemination - statistics - archiving;
- ✓ Capabilities to retrieve data transmitted by reporting entities' IT systems efficiently, securely and consistently through web services and API (Application Programming Interface) with data translation, firewall and access control functionalities;
- ✓ Capabilities for automatic electronic recording of all reports submitted by reporting entities in special electronic registers;
- ✓ Implementation of electronic distribution/authorisation/signature workflows to eliminate the circulation of paper documents within the organisation;
- ✓ Extract-Transform-Load (ETL) capabilities to ensure that data is extracted, processed, validated and loaded into a data warehouse;
- ✓ Capabilities to connect to national databases or registries held by public institutions in Romania through web services and API (Application Programming Interface) with data translation, firewall and access control functionalities;
- ✓ Search capabilities in data sources that do not have APIs or other standard connectors; - Search capabilities in social networks;
- ✓ Capabilities to monitor transactions reported by legally obliged entities to identify suspicions of money laundering and terrorist financing in accordance with defined detection scenarios;
- ✓ Generate a single alert based on the aggregation of results for an individual/legal entity by combining detection scenarios. This will provide an overview of the individual/legal entity by aggregating scenarios and risk factors, thus allowing analysts to make decisions based on the identified risk;
- ✓ Capabilities that provide analysts with the ability to conduct targeted searches in relation to money laundering/terrorist financing;
- ✓ Equipped with fuzzy search algorithms to allow analysts to identify in a browser interface all potential matches (including transliterations, misspellings, typos and phonetic transcriptions) or to configure detection scenarios for data monitoring;

- ✓ Full text indexing capabilities in documents attached to suspicious transactions; - Network charting capabilities to display entities and financial flows, including geospatial information (overlaid on a map);
- ✓ Enabling the elimination of manual operations required to process the reports taken daily from the reporting entities and enter them into the Office's databases;
- ✓ electronic management of control and supervision processes.

TO CONCLUDE

It is becoming increasingly clear that new technologies need to advance and improve ID verification, collect a large volume of information, distribute it and thereby improve the financial services consumer's experience of AMLCFT procedures and regulation.

It is increasingly clear that the risk-based ML/FT approach as well as risk management in this area is not possible without accurate and complete information and technology that allows the information to be used to benefit the mission and role of this activity. The accumulation and dissemination of financial market information must be well coordinated and transparent. In this way, the goal of strengthening the confidence of clients and institutions, of society as a whole, in the financial system and in the policies and instruments used is achieved.

Financial education is also called upon to play its part in the fight against money laundering, as there is still a significant gap between the public's desire to step up the fight against money laundering and terrorist financing, on the one hand, and its willingness to comply with the rules imposed to monitor it, on the other.

In conclusion, we believe that a more efficient and effective use of technology can be a valuable support in the fight against money laundering and terrorist financing operations, increasing the performance of this regulatory and supervisory activity. Digitisation must be implemented on the basis of an open architecture, with a high capacity for interoperability, in a context marked essentially by the creation and strengthening of sustainable partnerships between all the actors of the AML/CFT ecosystem.