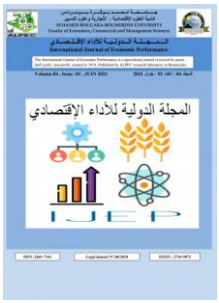
Big data, Data mining and Behavioral tracking against modern Money-Laundering

Rabia Bouarioua, Mohand Si, Si Mohand Mounir

المـجـلـة الـدولـيـة للأداء الاقـتـصـادي
International journal of economic performance
ISSN: 2661-7161 EISSN:2716-9073
Publications are Open Access in this journal



Big data, Data mining and Behavioral tracking against modern Money-Laundering

BOUARIOUA Rabia	SI MOHAND Mounir*
r.bouarioua@univ-boumerdes.dz	Simohand.mounir@univ-alger3.dz
University of Boumerdes (Algeria)	University of d'Algiers 3 (Algeria)

Submitted:29/06/2022 Accepted:25/07/2022 Published:04/12/2022

Abstract:

Our research aims to highlight the different modern programming techniques and methods used against money laundering. We will propose solutions within the literature of programming conceptualization that rely on the ability to analyze information and profile the individual to initiate a tracking process in order to allow the competent cells to intervene. Our study will also show that adequate conditions are necessary for the installation of such process on the Algerian national territory.

Key words: Money-laundering, Tracking, Programming, Behavior

JEL Classification Codes: C61, K42, E59.

ملخص

هدف بحثنا تسليط الضوء على التقنيات والأساليب الجديدة المختلفة من التقنيات المستخدمة ضد غسل الأموال. سنقترح حلولًا ضمن اليات البرمجة التي تعتمد على القدرة على تحليل المعلومات والملف الشخصي للافراد لبدء عملية تتبع من أجل السماح للهيئات المختصة بالتدخل. ستظهر دراستنا الظروف اللازمة و الضرورية لتطبيق هذه التقنيات على مستوى الاقتصاد الوطني الجزائري.

كلمات مفتاحية : تبييض الاموال؛ تتبع الالي؛ برمجة؛ السلوك

تصنيف JEL : C61, K42, E59

* Corresponding Author

Introduction:

One of the scourges experienced by all the economies and all modern societies is money laundering. Regardless of the development of society, money laundering will always have a share in increased crime. Its "popularity" comes back to its simplicity: transferring the fraudulent gains from the criminal circuit to the legal monetary circuit. At first glance, the solution against this activity seems just as simple: preventing the cash from the criminal circuit to transfer to the legal circuit; but it is to be blind on the different facets and the complexity of money laundering. It is somehow wrong to compare money laundering to other types of crime, in our opinion, money laundering is positioned in a centrality on which other facets of crime depends, because what good is a fortune sourced from criminalities of all kinds, if the money remains in the laundry? Interestingly, money-laundering progresses at the same rate as innovation, the more the technology of a society is developed, the more sophisticated money laundering techniques get; it is unlikely to find money-laundering mechanisms through bitcoins in Algeria. Internationally (especially in highly developed countries) the appearance of crypto-currency makes strategies against money laundering a major challenge. Of course, there are exceptions, certain poor countries or in crisis whose currency is extremely low, use crypto-currencies in their most basic purchases, which means that technology is easily transferable. Everything comes down to culture and geopolitical matters.

The structure of anti money-laundering splits into three simple parts: attacking the criminal circuit; protecting the legal circuit; blocking the transfer between the two. What is not very intuitive is that the criminal circuit is just as financially characterized as the legal circuit; we can even say that like the financial system, the criminal circuit is characterized by stability and volatility, the criminal circuit is worth to be known as the black finance. If at the bottom of the scale, the criminal activity is a basic activity of sale and purchase, violation of laws and rights, it can take unsuspected proportions very quickly.

Money laundering mostly focuses on sectors that absorb extravagant amounts of cash such as real estate, aviation, or the art trade for the simple reason that it allows the injection of substantial sums of cash more rapidly. This is why one of the classic techniques against money laundering is setting alert thresholds for money transfers. Nevertheless, even in this case, techniques like *"smurfing"* can allow criminals to launder their money without exceeding the alert limits in unsecured or unsophisticated banks. However, with new technologies, blocking smurfing became a reachable goal.

Money laundering literature divides the laundering process into three stages: first, dirty money enters the legal circuit. The second step consists in using this money in

different transactions in order to conceal its origin. Finally, money laundering involves investing the funds in legal activities. The main point of this process is to hide the source and origin of the dirty money. The main difficulty therefore becomes the identification of criminal flows, because if we know their origin, the entire chain of money laundering would be destroyed. The problem becomes even more complex if we take into account the fact that financial flows, resulting from money laundering are not only national, but also international. With new technologies, money laundering seems to reach new levels in its development.

Attacking the criminal circuit is a work of investigation and action that plays out simultaneously on the financial framework and on a "manual" or "physical" framework, which requires elite intervention bodies. In addition, the protection of the legal circuit is not as easy as we think; it requires specific work of control and audit on several levels of intervention. What intrigues us as finance scholars (without even being an expert on money laundering/crime) is that in principle, all cash flows have a direct and indirect source points, and circulate according to specific channels towards points of allocations. In money laundering, even if the criminal source points remain unknown, we do know the intermediaries points that are around those points, those points include all users and different interactions including purchases and transfers. Entry points and exit points are rarely contingent, especially if we apply strict regulations regarding the use of these channels. As private as personal data are, bank records and big data flows allow us to map the flow of cash flows. When we talk about big data the first image that comes to mind is social networks, but in truth, the term is very broad, it refers to the assembly of many different sets of data in a data warehouse to allow analyzes and control to discover new patterns, relationships and correlations.

Keeping in mind that strong intervention on the field will always be necessary, identifying financial flows and blocking them directly will dry up the criminal circuit. Our basic thought is that the triangulation of sources through known patterns and schematizations can allow us to anticipate and detect the source points of criminals; we discover that a large part of literature is dedicated to concretize such thought. In addition, the detection of flows, then of point sources will even give the geographical location of criminals, as long as the necessary technology is used. Our investigation shows that it is on this same principle that the process of financial tracking is based, the basis of solutions resulting from new technologies.

How data tracking enhances the ability to detect criminal cash flows from the criminal circuit to the legal circuit in Algeria in order to prevent money laundering?

In our paper, we will first take a look at money laundering and its definition, and the means adopted by Algeria to prevent it. Then, we will dive directly into the different

techniques and technologies currently used, finally we will talk about the determinants of the application of such technologies, we will also talk about *smurfing* as a reference in criminal techniques to better understand the role of data tracking.

Characteristics of money laundering in Algeria

Damages caused by money laundering and crime on the economy is very well known and documented. Money laundering represents a great nuisance for economic balance. The transfer of value in a criminal way from one country to another is one of the largest destabilization factors that a country can experience. Through laundering, criminals anonymously transfer a substantial amount of funds through financing channels in the legal circuit in order to whiten the revenues of their traffic. Again, money laundering is not a criminal activity like the others strictly speaking; it represents a center of convergence of criminal financial flows.

According to (Mokhefi, 2011), the best-known repercussions are:

- Slowed economic growth: illegal capital is used to finance so-called sterile activities, that is to say activities that are not optimal from an economic point of view.
- Monetary instability: the behavior of dirty money does not meet the logics of economic theory because the aim is not the performance but rather the protection and concealment of the laundering process. This is the reason why this money is subject to transfer from one financial center to another. This situation can negatively influence certain economic variables such as exchange rates and interest rates.
- Decrease in foreign direct investments: foreign investors are not encouraged to invest in countries known for their involvement in laundering acts or suspected of maintaining links with criminal or terrorist organizations.
- Inexplicable variations in the request for money, prudential risks with regard to banks' financial health, contamination effects on legal financial operations or even strengthening the instability of international capital movements and courses in changes due to transnational transfers of unexpected assets.

It is extremely difficult to statistically estimate money laundering because all facets of crime are involved and does not disclose any information, the estimates we found are extremely low or unreliable. According to a press release from El-Watan, for the only public investment sector, it is estimated that fraudulent practices in the management of major projects have generated around $ 50 billion over 15 years, $ 7 billion between 2000-2009 and $ 10 billion since 2010 to 2019. According to the (UNODC, 2012) report, it is estimated that between 1970 and 2008, Algeria lost around $ 25.7 billion in revenue due to illicit financial flows. This very high number is explained by the fact that countries which are very dependent on natural resources are among those which are most affected by the problem of illicit financial flows. Egypt and

Algeria together represent 66% of illicit financial flows from North Africa. In total, crime in the formal sector generates $ 10.8 billion on average annually. By adding, the smuggling product ($ 8 billion) and the informal sector ($ 53 billion), a total of $ 71.8 billion are to be considered as illicit cash flows.

Algeria is part of the GAFI, the financial action group (or Financial Action Task Force) which represents an intergovernmental body against money laundering and the financing of terrorism, and which brings together thirty five (35) countries and two (02) regional organizations (EU and CCG). The institution in charge of the fight against money laundering in Algeria is the CTRF, which is the equivalent of the American *Fincen*, the British *UKFIU* and the French *TRACFIN*. Such institutions are called FIU, Financial Intelligence Units. Their function is the analysis and transmitting reports of suspicions identified and filed by the private sector, for (Penna, 2017), "The main rationale of an FIU is to be a 'buffer' between the financial sector and law enforcement and judicial authorities in charge of financial crime investigations and prosecutions". The CTRF's functions as cited in their chart are:

1. To investigate declarations and reports of suspicious operations and other data concerning capital laundering and financing of terrorism,
3. To transmit the result of investigations to qualified bodies efficiently;
4. The collection of all information and indices to establish the origin of funds and the real nature of the financial operations.
5. The ability to freeze assets and accounts for 72H.
6. The CTRF proposes legislative or regulatory texts to prevent and fight money laundering and the financing of terrorism.

According to the CTRF report, Algeria set up a device, which integrates international commitments such as:

- International conventions
- Relevant provisions of the Security Council resolutions, based on chapter VII of the Charter of United Nations,
- GAFI recommendations

According to statistics, the number of declarations between 2016 and 2017 is stable but low compared to the immensity and the reality of the traffic:

Table 1 : declarations of suspicion

year	2016	2017
#	1240	1239

Source : official CTRF reports

Table 2 : Criminal repports

year	2016	2017
#	168	184

Source : official CTRF reports

According to the latest GAFI report, gaps and weaknesses have been reported with regard to the application of the 49 GAFI recommendations for the Algerian banks. What we particularly note is the weakness and lack of statistical and advanced computer engineering techniques. Knowing that the degree of confidentiality differs from country to country, for Algeria, this confidentiality is not absolute insofar as it is not enforceable against certain third parties.

Understanding behavioral tracking in programming against money-laundering

To better understand the importance of tracking, which represents the constant and dynamic monitoring and control of all the financial interactions specific to the legal circuit and the various financial transfer between individuals and institutions, it must be remembered that the criminal circuit needs the intervention of innumerable individuals who interact with each other using common and very redundant procedures. If we can detect a flow that does not justify the conditions of legality, or is suspected to be from a non-legal or suspect source, using a computer program and an ICT structure, we can detect and anticipate the allocation of the cash through the channel by anticipating the next stages of the flow movement. According to (Böszörmenyi & Schweighofer, 2014) "There are often similarities between the behaviors of criminals. To avoid the iteration of criminal activities with similar patterns, one can learn from previous cases and establish scenarios (rule sets) for the detection of similar *modus operandi*. For this purpose indicators can be derived from known money laundering cases ", which requires experience and expertise in money laundering and solid Databases. It also means that a joint work between anti-criminal groups and investigative cells are required.

A plethora of articles such as (Luo, 2014), (Gao & Ye, 2007) and (Krishnapriya, Phil, & Prabakaran, 2014), propose exactly what we describe in early parts, through the process of data mining. Data mining is the process of extraction of useful information from a voluminous data set. These data exploration techniques can be used to identify the suspicious accounts from which the funds were transferred and so on. The fact that real human beings and not computers with random steps apply criminal operations, allows us to anticipate and analyze their behavior. The program of the previous article makes it possible to monitor and track down transactions according to behavioral rules through data mining. If we have information on the flow, quantity, location, etc., the program can locate and anticipate the destination or the source of the cash flow. The article by (Ahmad, Ghazanfari, & Fathian, 2017) offers several methods:

- Clustering: Clustering is a process that classifies data from transactions and bank accounts in different groups according to their similarities. The algorithms work according to a scheme, which allows associations between key accounts that interact continuously in a suspicious manner.
- Method based on logical rules: use a set of rules expressed in logical language to classify the crime factor and extract possible correlations.
- Neural networks: The neural network is a method that uses a set of connected nodes and imitates human brain function. This method is based on computer models of organic neurons. A network of multilayer neurons contains a large number of units (neurons) linked together in a communication model that permits high efficiency.
- Decision tree programs and processes.
- Social media: Decisions regarding data mining exploitation is called "links analysis".

The articles that deal with behavioral patterns are mainly based on the quantity factor: we can separate between common accounts, that is to say accounts used by the average workers, i.e the basic employee, and the suspect accounts. Employees or households have specific characteristics compared to the quantity of accessible funds, to their class and to the transactions they carry out in their daily lives, we can easily characterize a classic behavior compared to their income. For example, if the basic salary or the average salary in Algeria is 35000 DZA, the number of options concerning consumption and savings are limited, that is to say, the numbers of behavioral patterns become lower. The program becomes even more efficient if we take into account macro-economic and micro-economic data such as purchasing power to anticipate savings. Economic and macroeconomic theories have a great potential application for anti money-laundering techs because they can directly feed computer programs with robust behavioral patterns. The average transaction curves of ordinary citizens have distributions that can be characterized according to classic behavioral patterns and are very close, unlike suspicious accounts, which are characterized by statistical curves with different and volatile frequencies compared to the classic pattern curves. If savings exceeds a specific threshold, the account becomes suspicious.

As we have already specified, one of the mechanisms against money laundering is to set alert thresholds, but if the criminals are aware of these thresholds, they will divide the flows and distribute it on several accounts; this is what we call smurfing. The statistical and technological approach is not to put a fixed threshold according to classic descriptive statistics, but to identify the dynamical and statistical thresholds common to the curves of financial activities or transfer of financial flows, any deviation or exceeding of threshold will be considered as suspect. This is exactly the principle of the

article by (KRISHNAPRIYA, PHIL, & PRABAKARAN, 2014): If the amount received or transferred is greater than the average value of the transfer of funds, it will be selected as a suspicious transaction and will be added to monitoring.

In France, for example, on average, a single adult sets aside 4,800 euros per year (Insee 2017 data), or 16% of their income. This can be used to identify and classify individuals according to a degree of suspicion through a method based on logical rules. Unlike France, the Algerian banking system is not as advanced, and citizens do not necessarily have the motivation to save or use the banking system regularly, which requires a different pattern assessing. (Chadha & Kaur, 2018) follows the same logic and uses big data to be able to flush out smurfing. Smurfing is very simple, which means that it is very likely that this technique is very widespread in Algeria. This article directly uses our principle mentioned in the introduction: The program of the article makes it possible to sort transaction data, which groups together several information and meta-information and then defines the individuals according to their IP addresses, so that those users who perform multiple transactions from a single machine could be detected. One method we can propose is to use a transaction timeline process that clusters accounts by time correlation of withdraws and deposits on a long-term timeline that requires a deep data identification of accounts and profiles of users.

The logic is that if an individual maintains an activity characterized as suspicious (according to the amount of funds or the frequency of transactions for example) throughout a period, he will be classified as suspicious and a report will be systematically sent to the cells of investigation. According to the article, there is a high probability that such malicious individuals have their accounts in different banks and different branches in different countries. This makes it difficult for anti-money laundering authorities to keep track of all their transactions manually; this is where program and institutional synchronization must come into play.

The article by (Xiong, 2017) uses the same approach: the trading statistics of the electronic accounts are set within the program, and then define the transaction limit that is mainly based on the identity of users. For such approach to work, a multitude of databases must be active simultaneously and contain enough information, supported by a sufficient technological infrastructure. Once the status of the individual is established, the patterns can identified and chosen and from there we can anticipate and initiate computer tracking. Several articles use data mining that describe the following methodology: Associated data is selected for the data-mining program, where the data-mining algorithm is applied. After that, the discovered knowledge is then

databased again and used for correlation visualization. Xiong's article uses the methodology to perform the approach of behavior patterns: In a stream of financial transaction data, the discovery of patterns that appear as sufficient anomalies arising from specific behavioral characteristics, that diverge from the regular behaviors will be identified as suspicious transaction patterns, controlled, tracked and reported.

The program used does not need to discover with absolute certainty the criminality of an individual; the purpose is to transmit continuous reports to specialized cells and entities, in order to feed them with data and clues. Nevertheless, we must keep in mind that Banks must categorically refuse non-justifiable money flows and interaction with other institution or corporations that do not take into account the absolute banishment of money laundering; otherwise, the results will be compromised. It means that we are working with the assumption that the bank itself has ethical, or that an outside auditing prevents it from degrading into something that holds no ethical management of its finance. The problem being that in the legal circuit, there are institutions and entities that open doors for money laundering because this activity is extremely lucrative; if the legal circuit is itself corrupt, it will be difficult to make any program efficient. The best legal weapon is to impose extremely strict source and information disclosure rules. Good tracking needs the coordination of all institutions at national and international level; it is not a mere computing system, but a matter of global financial security and governance. We can cite a sample of articles that uses different programming approaches against money laundering. Each article adds up a specific technique that enhances the ability to detect criminal cash flows but rely on behavioral patterns:

Table 3: list of different approaches

(Kingdon, 2004)	The proposed program monitors customer activity to identify unusual behavior and detect potential money laundering situations using artificial intelligence.
(Cheong & Si, 2010) (Miers, Garman, Green, & Rubin, 2013)	Both articles use the Event Based Approach to data analysis and visualization of money laundering data.
(Flores, Angelopoulou, & Self*, 2012)	By combining digital forensics practices along with database tools and database analysis methodologies, the program tracks and detects potential suspects.
(Singh & Best, 2019)	This study explores the use of visualization techniques that can help to effectively identify patterns of money laundering activity. It demonstrates how link analysis can be

	applied to detect suspicious banking transactions
(Kumar & Das, 2020)	This study explores the use of visualization techniques that can help classify a transaction as illegal or not. To achieve this, they used a Big-data analysis technique to identify money-laundering activities through a Naïve Bayes classifier program. The Naive Bayes program provides pragmatic learning algorithms that provide insight in understanding and evaluating many suspicious behavior patterns in money laundering activities. It demonstrates how link analysis can be applied to detect suspicious banking transactions
(KRISHNAPRIYA, PHIL, & PRABAKARAN, 2014)	They proposed a program-based money laundering identification framework that generates transactional behavior patterns based on different time windows. Based on the generated patterns, a money laundering identification is performed. The main objective was to detect behavioral patterns to track suspicious individuals and money flows.

Source: grouped by the authors

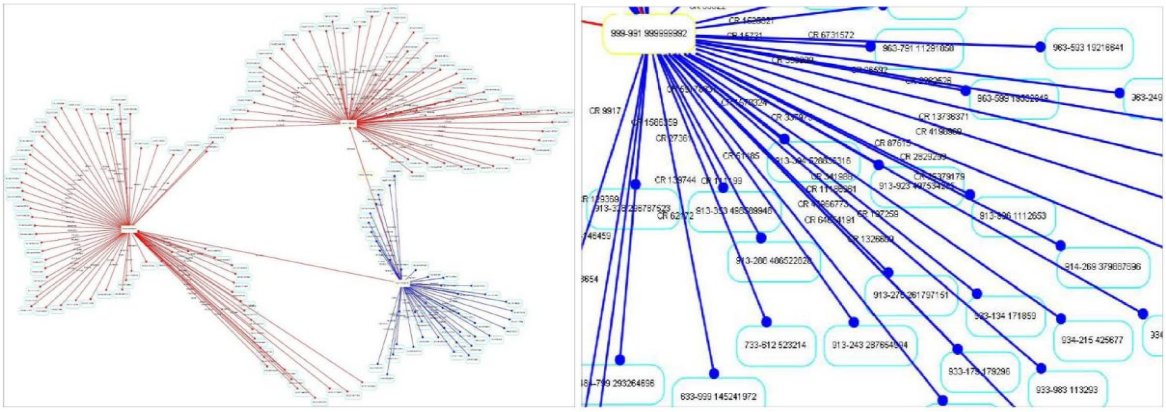
The articles cited experiment with real data, sufficient to prove the effectiveness of the programs they offer, and all show a high degree of effectiveness. In our opinion, the best solution is the use of dynamic programs that are not selective or static, but continuously scan any newcomer throughout its existence and its activity. The CTRF works mainly through the declarations of suspicions and the reports of certain Administrations, which are all targeted procedures and not broad field scanning processes. Computer programs are tools that work on a larger scale, faster and more efficiently.

The article by (Kannan & M.V.Srinath, 2018) takes up word for word the principle that we mentioned previously and integrates it into an extremely sophisticated program: The analysis of important informations assists in the detection of different values between transactions in forms of clusters. Therefore, the abnormal behavior of a particular person is detected from a set of global inputs. The paper uses two complementary algorithmic methodologies: First, a triangular boundary-based imperative detection (TBOD) algorithm segments the dataset into a group based on financial transfers and transactions, and risk of criminality. A triangular matrix is constructed to organize these transactional records and identify abnormal behavior. In order to reduce time and computational complexity, the article uses an independent autoregressive anti-money laundering program "AROMLD" (Autoregressive-based Outlier Algorithm for Money Laundering Detection). An autoregressive process is a

regression model for time series in which the series is explained by its past values rather than by other variables. The algorithm deals with interquartile range that gives information on the dispersion of the series around the most frequent values taken by this series. This offers a method that isolates suspicious transactions in financial systems in real time, and anticipates the evolution of a phenomenon.

The incalculable number of accounts and interactions, and the non-intuitive format of accounts and transactions leave very little room for human investigation and make it very difficult to identify suspicious flows. To be able to effectively analyze and track financial flows, there are several technologies, for example (El-Banna, Khafagy, & El-Kadi, 2020) and (Singh & Best, 2019) cited above use intuitive visualization in the tracking of the suspicious account activity. This visualization uses a graph database. A graph database is a database that uses graphic representation entities as nodes and relationships between those entities such as edges between properties describing a given entity as a node. The diagram below shows how accounts can be viewed.

Figure 1 : graph database



Source: (Singh & Best, Anti-Money Laundering: Using data visualization to identify suspicious activity, 2019)

Many articles use graph database technology against smurfing. What is extremely interesting is that the article claims that the algorithmic visualization program of graph databases allows mitigating the circumvention ability of smurfing, but above all the program has the ability to detect their complete network and to detect the final destination of cash flows. The article of (Suresh, Reddy, & Sweta, 2016) uses the graph database approach with Hash based Association technique in their *apriori* algorithm to successfully identify agents and integrators in the layering stage of Money Laundering, thus identifying the traversal path of the laundered money. The main purpose of the Hash based association approach is to reduce the number of pertinent candidate from the vast pool of possible classes that would render the task much more difficult if taken

as it is. Using the Hash association will sort the data in an array format with unique index value. Access to valuable data becomes easier and reduces research time. According to the AUSTRAC (Australian Transaction Reports and Analysis Centre), the Australian equivalent of the CRTF, there are several clues and indicators that can help identify suspicious transactions, and be included in the programs:

1. The transaction was incompatible with the client's profile.
2. Savings deposited domestically then withdrawn through offshore ATM.
3. Deposit several large amounts of money and receive several checks drawn on this account.
4. Movement of funds through different accounts. Transfers are sent or received from the same person to or from different accounts.
5. Early and frequent loan repayments.
6. Funds transferred to a charity fund or a sudden increase in client account activity.
7. High volume of transactions in a short period.
8. Investment funds sent to countries considered dangerous or risky.
9. Transfers large amounts of money from unexplained sources.
10. Multiple transactions of a similar nature on the same day at different locations.
11. Transfers from Corporate Accounts to Unlisted or Suspicious Individual Accounts.
12. Unexplained income incompatible with the economic situation.
13. The price of the products or services is manifestly excessive or insufficient.
14. Cash deposits contain high value banknotes, in installments or at the counter.

Moreover, banking transactions are carried out through human interactions. If, for example, the client (Monroy, 2021):

- Does not want to provide documentation of a specific transaction he/she is carrying out.
- Insists on paying a tip.
- A broker, lawyer or financial advisor is acting on someone else's behalf without proper documentation, such as an attorney.
- Client provides unusual or suspicious identification documents or refuses to produce originals for verification.
- Customer does not want to provide personal information when opening an account.
- Client tries to open an account without identification, references or full local address
- A student or unemployed person deposits large sums of money.
- Customer frequently exchanges high denomination notes for low denomination notes.

All of the above points can be part of one large-magnitude and very sophisticated data mining computer program.

Determinants that allow the adoption of tracking programs

One of the most well known anti-money laundering entities is the *FinCEN* "The Financial Crimes Enforcement Network", the equivalent of the Algerian CTRF, it represents an office of the United States Treasury Department that collects and analyzes information on financial transactions in order to fight domestic and international money laundering, the financing of terrorism and other crimes. Compared to the CTRF, FinCEN is in a completely new level of expertise and a whole new class of sophistication. It employed approximately 340 people mostly intelligence professionals with expertise in the financial industry, illicit finance, financial intelligence, money laundering, terrorism financing, regulatory regime, computer technology. This institution operates according to a very precise legal framework and allows it to expand and improve the traceability of financial flows. It employs an immense number of programs and detection techniques in order to protect the legal circuit, weaken the criminal circuit, and block all possible transfers between the two. FINCEN is in a constant dynamic of innovation, whether in the use of the most recent technologies such as the latest advances in artificial intelligence or the policies of the financial system. The information and technology used to facilitate analysis is central to FinCEN's mission, which is to deter and detect criminal activity and protect financial systems from fraud by promoting transparency in U.S. and international financial systems.

However, if we first take a look at the internal structure of FinCEN, we realize that the degree of specialization required in order to be able to launch the programs and the various ICTs is gargantuan. It is not a simple structure, but a complex anthill of interconnected machines and programs. As said before, it is not just applying programs to a compilation of data, but a heavy expertise that requires several years of experimentation, and Algeria has not yet started to establish this technological base. It was only recently that Minister Aymen Abderrahmane took the initiative to launch the project to provide databases on a larger scale. Algeria's greatest defect, not only at the economic and financial level, but also socially, is the lack of a reliable base and the serious lack of transparency and legal certification of information. Financial information must comply with various regulations and follow strict protocols and guidelines that allow tracking and control procedures to be effective.

Even if we apply the best programs, without the existence of the information itself, nothing can be done. Algeria must master database and information management on a

very large scale before even embarking on the implementation of statistical programs and new technologies. Institutions must follow several steps to be able to launch the statistical program:

1. Sufficient data collection: Firstly, through cooperation with social credit system, electronic financial institutions and internet, relevant data is obtained directly via data interface and stored in massive database. The data must be much diversified, regulated and in sufficient quantity.
2. Data integration: Data integration is a necessary part of data preprocessing for large data mining. According to the factors involved in the electronic financial risk, it is necessary to identify the risk involved in the data, in order to verify their robustness. In addition, this data is converted to make it more suitable for quantitative processing of early warning model, model algorithm requirements and correlation analysis.
3. Relevant data mining analysis: Database analysis is implemented through processing and evaluation systems. Database mining analysis methods include risk index system, statistical models and artificial intelligence.
4. Data application: finally, launch of the various programs available in the search for correlation and variations, the identification of crime risks, alert and monitoring, and the automatic report function

The biggest problem is the strategic approach to information, without a real understanding of the type of information; the extracted correlations can be noisy and meaningless because they do not reflect the reality of events. Computer biases and serious deviations can occur in the primary data collection process and in the modeling. A deep knowledge regarding the theory of information and data is required. Most papers use an approach that minimizes information that has low correlation potential or that generates dissonance in the computer program. However, as the article by (LaValle, Lesser, Shockley, Hopkins, & Kruschwitz, 2011) points out, despite popular opinion, obtaining data is not a primary challenge that organizations face when adopting Data-mining processes. Barriers to adoption related to culture rather than data and technology. Algeria must follow the example of the *FinCEN* and promote skills and the use of new technologies. Over the past few years, *FinCEN* has deployed several recruitment and talent support programs; even today, it continues to improve and modify its internal structure in order to achieve its objectives.

According to (Akkarene, Bouda, & Ameziane, 2020) “the introduction of IT remains very average, IT is only disseminated in a relatively average way in banking structures”. One of the most advantageous elements of ICT is the considerable

reduction in cost and investigation time. Criminal activities aim to launder their resources as quickly as possible; without equally fast techniques, identification will be useless, because the accounts will be closed before an effective intervention could takes place. The Algerian government needs to release a sufficient budget in order to invest in innovation and technologies within a broad and continuous plan. There is a profound stagnation in the culture and development of the technology-finance couple. Unlike several other countries, Algeria does not have the technological capacity to take over data mining techniques at the economic level.

Conclusion:

We briefly described the money-laundering situation in Algeria, and then we mentioned several techniques that use original approaches such as data mining and big data. The proposed techniques are very effective solutions against laundering methods such as smurfing. Today, worldwide, different means are used against money laundering, most modern banks use sophisticated banking softwares that includes anti money-laundering modules that scan all deposits/withdrawals looking for patterns and that indicate money laundering. The software generates reports automatically and submits them to law enforcement in a blink of an eye. Some software can detect smurfing if it is done at different branches of the same bank, it will be caught and reports will be sent to competent services. Nevertheless, for such processes to be put in place and launched effectively in Algeria, heavy IT and technological structures must be put in place by the institutions concerned.,

Referrals and references

- Ahmad, S., Ghazanfari, M., & Fathian, M. (2017). Data Mining Techniques for Anti Money Laundering. *International Journal of Applied Engineering Research* .
- Akkarene, R., Bouda, N., & Ameziane, L. (2020). Utilisation des technologies de l'information et de la communication dans le secteur bancaire : cas des banques de la ville de Bejaïa- Algérie. *revue internationale d'économie numerique* , 29.
- Böszörmenyi, J., & Schweighofer, E. (2014). TRACKING OF FINANCIAL MOVEMENTS. *Transparency* , 620.
- Chadha, A., & Kaur, P. (2018). Handling Smurfing Through Big Data. *Advances in Intelligent Systems and Computing* .
- Cheong, T.-M., & Si, Y.-W. (2010). Event-based Approach to Money Laundering Data Analysis and Visualization. *Proceedings of the 3rd International Symposium on Visual Information Communication* , 10-15.
- El-Banna, M. M., Khafagy, M. H., & El-Kadi, H. M. (2020). Smurf Detector: a Detection technique of criminal entities involved in Money. *international conference on innovative trends in communication and computer engeneering* .
- Flores, D., Angelopoulou, O., & Self*, R. J. (2012). Combining Digital Forensic Practices and Database Analysis as an Anti-Money . *Third International Conference on Emerging Intelligent Data and Web Technologies* , 1-7.

- Gao, Z., & Ye, M. (2007). A framework for data mining-based anti-money laundering research. *Journal of Money Laundering Control* .
- Kannan, S., & M.V.Srinath. (2018). Autoregressive --based Outlier Algorithm to Detect Money Laundering Activities. *International Journal of Research and Analytical Reviews* , 1-10.
- Kingdon, J. (2004). AI fights money laundering. *Intelligent Systems* , 87-89.
- KRISHNAPRIYA, G., PHIL, M., & PRABAKARAN, M. (2014). MONEY LAUNDERING ANALYSIS BASED ON TIME VARIANT BEHAVIORAL TRANSACTION PATTERNS USING DATA MINING. *Journal of Theoretical and Applied Information Technology* .
- Kumar, A., & Das, S. (2020). Anti Money Laundering detection using Naıve Bayes Classifier. *International Conference on Computing, Power and Communication Technologies* , 1-10.
- LaValle, S., Lesser, E., Shockley, R., Hopkins, M. S., & Kruschwitz, N. (2011). Big Data, Analytics and the Path From Insights to Value. *MIT Sloan* , 21-31.
- Luo, X. (2014). Suspicious Transaction Detection for Anti-Money Laundering. *International Journal of Security and Its Applications* , 620.
- Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. *IEEE Symposium on Security and Privacy* , 1-15.
- MOKHEFI, A. (2011). LA DIFFICILE LUTTE CONTRE LE BLANCHIMENT D'ARGENT: L'ALGERIE AU-DEVANT DE LA SCENE. *مجلة الإستراتيجية والتنمية*, 7.
- Monroy, S. (2021, 04 25). *Comment détecter le blanchiment d'argent*. Consulté le 12 2021, 28, sur atalayar: https://atalayar.com/fr/blog/comment-détecter-le-blanchiment-dargent
- Penna, M. (2017). The 'Pre-investigative' Role of Financial Intelligence Units in Recovering Assets. *Criminal Money: Challenges and Perspectives* , 271.
- Singh, K., & Best, P. (2019). Anti-Money Laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information systems* , 8.
- Suresh, C., Reddy, T., & Sweta, N. (2016). A Hybrid Approach for Detecting Suspicious Accounts in Money Laundering Using Data Mining Techniques. *Information Technology and Computer Science* , 3-7.
- UNODC. (2012). Illicit Financial Flows :. *Commissioned by the AU/ECA Conference of Ministers of Finance, Planning and Economic Development* , 95.
- Xiong, J. (2017). An Early Risk Warning Model for Electronic Financial Crime Based on Big Data. *Advances in Social Science, Education and Humanities Research* .